한국정보전자통신기술학회논문지(jkiiect)'22-4, Vol.15 No.2
논문 22-15-02-134 http://dx.doi.org/10.17661/jkiiect.2022.15.2.134

디지털 헬스케어 서비스의 데이터 컴플라이언스 방안에 관한 연구 - 개인정보 라이프사이클을 중심으로

정재은, 양진홍*

A Study on Data Compliance Measures of Digital Healthcare Service - Focusing on Personal Information Lifecycle

Jaeeun Jung, Jinhong Yang*

요 약 디지털 헬스케어를 이끄는 핵심 요소는 '데이터'이다. 헬스케어 데이터는 대부분 정보주체의 개인정보이며, 데이터 특성상 민감정보를 포함한다. 기업은 데이터 수집 및 이용, 제공, 파기되는 라이프사이클 동안 데이터를 준법하고 안전하게 활용하는 것이 매우 중요하지만, 헬스케어 서비스 산업의 78%를 차지하는 중소·벤처·스타트업은 개인정보보호 관련 업무를 수행하는데 어려움을 겪고 있었다. 개인정보를 이용하는 목적에 따라 개인정보보호법에서 요구하는 사항이 다르고, 개인정보 라이프사이클 시점마다 요구하는 사항들도 다양하므로, 데이터 활용 시 법적·기술적 측면에서 충분히 고려되어야 한다. 이에 본 연구에서는 기업이 헬스케어 데이터를 활용하는 목적을 여섯 가지로 제시하고, 개인정보가 수집되어 파기되는 라이프사이클 동안 고려해야 하는 사항에 대해 제안하고자 한다.

Abstract 'Data' is the key component that leads Digital Healthcare. Most of the Healthcare Data is personal information of data subject and includes Sensitive Information. It is very important for companies to use data lawfully and safely during the lifecycle of data collection, use, provision, and destruction. However, small and medium-sized enterprises(SMEs), ventures, and startups, which account for 78% of the Healthcare Services Industry, have had difficulties in performing tasks related to personal information protection. The personal Information Protection Act's requirements depending on the purpose of using Personal Information are different. Also, the requirements for each personal information lifecycle are varied. Therefore, this study suggests six purposes for companies to use healthcare data. It examines the considerations during the lifecycle in which personal information is collected to be destroyed.

Key Words : Data Compliance, Data Privacy, Digital Healthcare, Personal Information Lifecycle, Personal Information Protection Act

1. 서론

디지털 헬스케어는 헬스케어 산업과 ICT(정보통신기술)가 융합되어 개인 건강과 질환을 관리하는 산업 영역으로, 데이터 기반의 디지털 헬스케어 혁신은 헬스케어 데이터를 측정, 통합, 분석, 활용하는 과정에서 의료와 건강관리 등 헬스케어 전반에 변화를 가져오는 것을 의미한다. 한국은 보건의료정보의 디지털화가 빠르게 이루어져서 디지털 헬스케어가 성장할 수 있는 토대가 마련되어 있으며, 데이터 측정, 분석, 연계 각 단계별 새로운 비즈니스가 나타나고 있다[1].

산업통상자원부가 실시한 '국내 디지털 헬스케어 실

This paper has supported by the Commercializations Promotion Agency for R&D Outcomes grant funded by the Ministry of Science and ICT (2022, Local industry-connected university Open-Lab fostering support project)
Departmet of Healthcare IT Engineering, INJE university
*Corresponding Author: Departmet of Healthcare IT Engineering, INJE university (jinhong@inje.ac.kr)
Received April 11, 2022 Revised April 19, 2022 Accepted April 20, 2022

태조사'에 따르면, 2020년 국내 디지털 헬스케어 산업의 매출 규모는 약 1조 3,500억 원이며, 그중 지능형 건강관리 서비스(홈&모바일 헬스케어 서비스, 의료정보 플랫폼 등)가 55.6%로 가장 높은 비중을 차지하였다[2].

디지털 헬스케어를 이끄는 핵심 요소는 '데이터'이다. 헬스케어 데이터는 전통적으로는 병원 내에서 생성되고 축적되었지만, 발전된 기술의 접목과 다양한 공급자의 생태계 진입으로 산업 간 융합이 빠르게 일어나고 있으며, 라이프로그(lifelog) 데이터와 같은 병원 밖에서도 새로운 헬스케어 데이터들이 생성되고 맞춤형 서비스로 확장되고 있다[3][그림1].

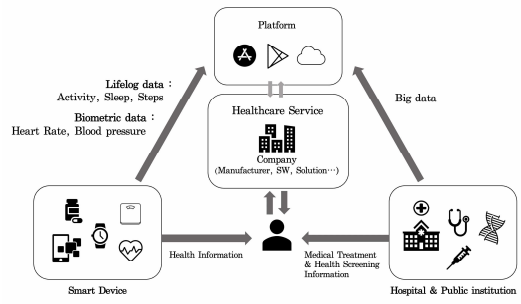

그림 1. 헬스케어 서비스 구조
Fig. 1. Architecture of Healthcare service

웨어러블 시장이 성장하고, AI가 질병을 예측하는 등의 변화가 일어난 것은 모두 헬스케어 데이터를 수집하고 이를 활용하는 것에서 비롯되었다고 할 수 있다. 이렇게 디지털 헬스케어 시장에서 중요한 역할을 하는 헬스케어 데이터는 대부분 정보주체의 개인정보이며, 데이터 특성상 건강정보를 포함한다. 개인정보보호법 제23조에 따르면, 민감정보는 '사상·신념, 노동조합·정당의 가입 탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖의 정보 주체의 사생활을 현저히 침해할 우려가 있는 개인정보'로써, 헬스케어 데이터의 기반이 되는 개인 건강정보는 민감정보에 해당한다. 민감정보는 일반 개인정보보다 더 강력한 보호를 받으므로 유의하여 다뤄야 한다. 개인정보는 법률에 따라 개인정보 주체로부터 동의를 받고 수집 시점부터 엄격한 통제를 받으며, 목적이 달성되면 보유한 개인정보를 파기해야 한다[4]. 따라서, 기업은 데이터 수집 및 이용, 제공, 파기되는 데이터 라이프사이클(Lifecycle) 동안 데이터를 준법하고 안전하게 활용하는 것이 매우 중요하다.

국내 디지털 헬스케어 산업은 중소·벤처, 스타트업이 72%로 대부분을 차지하는데[2], 개인정보보호위원회가 실시한, 2021년 개인정보보호 실태조사에 따르면, 기업의 규모와 상관없이 개인정보 보호에 대한 중요성은 높게 나타났으나 기업의 규모가 작아질수록 '관련 법률의 내용 이해가 어렵다'는 응답 비율이 높아지는 특징을 보였다[5][표 1].

표 1. 개인정보보호 업무 관련 애로사항(%)
Table 1. Difficulties related to Personal Information Protection(%)

Number of employees	~5	5~49	50~299	300~
Complexity of processing personal information	47.4	42.8	42.6	51.0
Difficulty in understanding the relevant laws	35.8	33.7	30.2	26.6
Lack of professional personnel	29.1	32.1	30.5	24.0
Lack of privacy-related skills	25.1	29.6	34.4	24.4
Budgetary deficit	25.6	18.6	11.7	5.5
Operation of personal information protection education program	11.7	15.5	18.8	23.4
etc.	9.5	10.3	10.6	18.2

특히, 서비스를 운영하면서 수집한 헬스케어 데이터를 서비스의 개발과 비즈니스의 확장 등의 새로운 목적으로 활용하고자 할 때, 그 목적에 따라 법에서 요구하는 준수 사항이 다르다. 때문에 '목적'에 따른 요구사항을 구분할 수 있어야 준법한 개인정보 활용이 가능하다.

병원 등 의료기관의 경우, 데이터 라이프사이클을 기반으로 데이터가 사용되지만, 수집하는 개인정보의 종류도 영상 정보(X-Ray, MRI, HRV 등), 단층촬영 이미지, 유전자 정보 등으로 다양하며 의료기관에서 수집되는 정보는 의료법의 적용을 받기 때문에 개인정보보호법뿐 아니라 유관 법령 간의 우선순위를 파악해

야 한다. 다만 아직 헬스케어 데이터 활용과 관련해서 많은 개별 법령들이 산재되어 있으며 법령 간의 해석이 모호한 부분이 있어 논란이 되고 있다.

따라서, 본 논문에서는 병원을 제외한 헬스케어 기업이 헬스케어 서비스 상에서 개인정보가 포함된 데이터를 활용하고자 할 때, 그 목적을 분류할 수 있는 여섯 가지의 세부 기준을 제시하고, 개인정보 보호법(이하 '법')을 준수하기 위해 고려해야 하는 사항들을 데이터 라이프사이클의 4단계-수집, 이용, 제공, 파기-에 따라 살펴보고자 한다.

2. 문헌 연구

헬스케어 데이터는 개인의 건강정보, 성생활, 유전정보 등을 포함하는데 이는 개인정보 중에서도 민감한 정보이기 때문에, 오래전부터 데이터의 보호와 연구 및 활용 측면에서 여러 법적, 윤리적, 사회적 논의가 진행되어 왔다.

디지털 헬스케어와 보건의료 데이터의 활용 및 보호에 관한 연구는 크게 두 가지로 구분할 수 있다. 첫 번째는 보건의료 데이터를 활용함에 있어 법적 측면에서 연구한 것이고, 두 번째는 기술적인 방안에 대해 연구한 것이다.

2.1 법적 측면을 고려한 헬스케어 데이터 연구

헬스케어 데이터 활용에 있어 법적 측면을 고려하지 않을 수 없다. 기술의 발전 속도에 비해 법이 개정되는 절차도 많고 여러 이해관계자들의 논의가 필요하기 때문에 충분히 고려되지 않은 부분이 다소 존재한다. 그래서 국내 현 개인정보 보호 정책의 문제점을 제안하고, 이를 국내 다른 법률과 비교하거나, EU GDPR과 같은 해외 법안과의 비교를 통해[6][7][8][9] 국내 법제도의 개선 방안을 제시한다. 또한 디지털 헬스케어 사례를 연구[10]나 헬스케어 데이터와 특정 분야에 대한 연구[11]로 그 분야에서 앞으로 해결해야 할 과제에 대해 고민하고 제안하는 연구도 이루어지고 있다.

2.2 기술적 측면을 고려한 헬스케어 데이터 연구

개인정보를 더 안전하게 활용하기 위한 기술적 방안 연구도 활발히 이루어지고 있다.

헬스케어 데이터 수집 시에는 서로 다른 타입의 데이터가 수집될 수 있는데, 이기종 센서 장치에서 수집된 다양한 형태의 센서 데이터를 제안된 모델을 통해서 일관되게 수집하는 데이터 수집 모델을 제안[12]하였고, 각 병원에 저장된 서로 다른 형태의 헬스케어 데이터를 더 효율적으로 수집하기 위한 병원 간의 데이터 통합 모델을 제안[13]하였다.

헬스케어 데이터를 활용하는 방법은 무궁무진한데, 보다 안전한 활용을 하기 위해 비식별 처리된 개인정보가 가지는 위험도를 데이터 활용방법, 데이터 이용환경, 데이터 3가지로 나누어 각 상황별 위험도에 기반하여 정량적으로 측정함으로써 개인정보처리자가 위험도를 확인할 수 있게 하였다[14]. 또한 빅데이터 분석을 위해 여러 기업에서 수집된 방대한 양의 데이터를 한 기업이 모두 보유하게 되면 정보 간의 결합을 통해 개인식별성이 증가할 수 있는 위험이 존재하는데, 이를 해결하기 위한 연계 프로세스도 제안되었다[15]. 이외에도 의료분야에 인공지능을 활용한 연구[16]도 활발히 이루어지고 있다.

민감정보인 헬스케어 데이터는 저장 시에도 유의해야 하는데, 안전하게 저장하는 방법으로 의료 이미지 데이터를 블록체인을 통하여 이미지 데이터 접근 권한을 설정하고, 데이터의 무결성을 검증하는 방식[17]에 대한 연구가 수행되었다. 또한 의료 데이터가 클라우드 환경에서 처리될 때에 헬스케어 데이터를 전체 암호화가 아닌 일부 암호화 방식으로 보안의 측면과 처리 효율을 향상시키는 방안을 제안[18]하였다.

헬스케어 데이터 제공에 관한 연구를 살펴보면, 각기 다른 헬스케어 기기에서 수집된 데이터들은 표준을 준용하지 않기 때문에 플랫폼 간의 데이터 공유가 어렵다. 따라서 헬스케어 플랫폼 개인 건강 데이터를 공유할 때 사용할 수 있는 표준 기반 모바일 프레임워크를 제안[19]하였다. 또한 사물인터넷 기반의 헬스케어 서비스에서 일어날 수 있는보안 취약점을 개선한 사용자 프라이버시 보호 모델을 제안한 연구[20]도 있었다.

그러나, 기존의 연구들은 법의 문제점을 살펴보고 이를 개선하는 방안을 제안하는 것에서 그쳤으며, 안전한 개인정보 활용을 위한 기술적인 방안은 제시하였으나, 개인정보가 수집되어 이용, 제공, 파기되는 라이

프사이클 전반에 거친 기술적·제도적 방안에 대한 고려가 부족했다. 그리고 활용 목적에 따라 달라지는 고려사항에 대한 논의가 충분치 못하였다. 따라서, 본 논문에서는 헬스케어 데이터를 수집 및 이용하는 헬스케어 서비스 기업이 사용자의 개인정보를 활용할 때 고려해야 하는 사항을 활용 목적과 데이터 라이프사이클 단계별로 살펴보고자 한다.

3. 기업의 헬스케어 데이터 활용 목적 분류

의료영역에서 디지털 헬스케어로 확장되면서 수집·이용되는 데이터가 변화하였다. 기존에는 개인의료 정보에 대한 접근과 이용이 의료진과 의료관계자 중심이었다면 디지털 헬스케어에서는 플랫폼 사업자 및 플랫폼에서 수집된 데이터를 분석·가공하여 새로운 정보를 생성하려는 기업 등까지 정보의 접근 및 이용이 확장되었다[10].

법 제3조 개인정보 보호 원칙에 따르면, 1) 개인정보처리자는 개인정보의 '처리 목적을 명확하게' 하여야 하고 그 목적에 필요한 범위에서 '최소한의 개인정보만'을 적법하고 정당하게 수집하여야 하며, 2) 처리 목적에 필요한 범위에서 처리하며, '그 목적 외의 용도로 활용해서는 안 되고', 3) 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 해야 한다. 기업이 당초 수집한 목적 외에 개인정보를 사용하는 것은 금지되어 있다. 하지만 기업에서 제공하고자 하는 원 서비스의 운영의 목적이 아니더라도 사용자에게 적법한 동의를 받았다면 사용 가능하다. 다만 원 서비스의 범위를 벗어나서 사용하는 경우에 사용되는 개인정보의 수집·이용 동의는 필수로 받을 수 없으며, 이를 거부하였다고 서비스를 제공하지 않는 것은 불법이라는 점을 유의하여야 한다. 이렇듯 사용하는 목적에 따라 법에서 요구하는 준수 사항이 달라지기 때문에 기업이 헬스케어 데이터를 활용하는 목적을 6가지로 제시하여 '목적'에 따라 달라지는 요구사항을 분류하고자 한다[표2].

기업이 헬스케어 데이터, 즉 개인정보를 이용하는 목적은 먼저 크게 두 가지의 경우로 나눌 수 있다. 첫 번째는 정보주체가 가장 사용하고자 하는 '원 서비스 운영 등의 목적'으로 사용되는 경우고, 두 번째는 '원 서비스의 범위를 벗어나서 사용하는 경우'이다. 예를 들어, 당뇨 환자를 위한 서비스라면 '혈당정보를 기록하고 관리'하는 것이 원 서비스 운영 등의 목적으로 사용되는 것이고, '사용자 커뮤니티 기능, 당뇨 환자를 위한 간식·의료기기 구매 쇼핑몰' 등은 원 서비스의 범위를 벗어나서 사용하는 경우라 할 수 있다.

표 2. 개인정보 활용 목적 분류
Table 2. Classification of Purposes of Personal Information Use

Classification	Purpose
Used for the purpose of operation of the original service, etc.	the provision of original service
	the advancement of original service
	the expension of original service
Used for purposes other than original service	new service development
	provision of pseudonymized data
	providing and selling data to other companies

3.1 원 서비스 운영 등의 목적으로 사용되는 경우

원 서비스 운영 등의 목적으로 사용되는 경우는 다시 3가지로 나눌 수 있는데, 1)원 서비스의 제공에 사용되는 경우, 2)원 서비스의 고도화를 위해 사용하는 경우, 3)원 서비스의 확장을 위해 사용하는 경우이다.

당뇨 환자를 위한 서비스라면, 혈당 정보를 기록·관리하는 것은 1번 원 서비스 제공이고, 당뇨 기록을 다른 환자와 비교하여 통계 등을 알려주는 것은 2번 원 서비스 고도화이며, 기록을 기반으로 개인 맞춤형 관리법을 제안해 주는 것이 3번 원 서비스의 확장을 위해 사용하는 경우라 할 수 있다.

원 서비스 제공을 위해 사용자에게 필수로 받아야 하는 개인정보의 경우, 필수 동의 항목으로 반드시 사용자가 동의하여야만 서비스를 사용할 수 있도록 정할 수 있으며, 이에 동의하지 않을 시 기업은 서비스 제공을 거부할 수 있다.

3.2 원 서비스의 범위를 벗어나서 사용하는 경우

원 서비스의 범위를 벗어나서 사용하는 경우도 3가지로 분류할 수 있는데, 1)신규 서비스 개발을 위한 목적, 2)가명처리를 통한 데이터 제공, 3)타사로 데이터

제공 및 판매하는 경우이다.

회사 내에서 자체 연구 및 실험을 하거나, 신규 콘텐츠를 개발하는 것이 1번, 제약 회사와 공동 연구를 위해 수집한 정보를 가명처리하여 제공하는 경우가 2번, 제약회사에 데이터를 판매하는 것이 3번에 해당한다. 2,3번 모두 제 3자에게 데이터를 제공한다는 사실은 동일하지만 가명처리의 여부에 따라 구분하여 볼 수 있다. 가명처리란, '개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보 없이는 특정 개인을 알아볼 수 없도록 처리하는 것(법 제2조제1항)'을 말한다. 개인정보처리자는 통계 작성, 과학적 연구, 공익적 기록 보존 등을 위한 경우 정보주체의 동의 없이 가명정보를 처리할 수 있기 때문에, 가명처리하여 사용하는 경우(2번) 별도의 동의를 받지 않아도 된다. 하지만 가명처리하지 않은 정보를 타사에게 제공하는 경우(3번), 제공받는 자인 제약회사의 목적에 따라 데이터가 사용되므로 정보주체에게 제3자 제공 동의를 획득하여야 한다.

원 서비스의 범위를 벗어나서 개인정보를 사용할 때에는 서비스 제공을 위해 반드시 수집해야 하는 정보가 아니므로 사용자에게 필수 동의 항목으로 받을 수 없으며 사용자에게 선택권을 주어야 한다. 필요한 최소한 외의 개인정보 처리에 동의하지 않는다는 이유로 사용자에게 서비스 제공 자체를 거부하는 것은 금지되어 있다[21].

4. 개인정보 라이프사이클에 따른 개인정보 활용시 고려사항

기업이 개인정보를 효과적으로 보호하기 위해서는 개인정보 및 개인정보 보호에 대한 체계적이고 종합적인 분석이 선행되어야 한다. 복잡한 개인정보를 가장 효율적으로 이해하는 방법 중 하나는 기업에 의해 개인정보가 수집되어 저장·이용·파기되는 전체 프로세스를 분석하는 것이다[22].

기업은 사용자로부터 개인정보를 수집하여 DB에 저장하며, 서비스 제공 및 확장, 신규 서비스 개발, 서비스 고도화, 홍보 및 마케팅 등의 목적으로 사용한다. 제3자에게 제공하는 경우는 개인정보 처리와 관련된 특정 업무를 타 기업에게 위탁하는 것과 개인정보의 지배·관리권이 모두 타 기업에게 이전되는 '개인정보 제공'이 있다. 수집된 개인정보를 목적 달성, 기간 만료 등의 이유로 더 이상 필요없게 되면, DB를 삭제하거나 파쇄하는 등 복구할 수 없는 영구적인 방법으로 파기하여야 한다.

앞서 3장에서 살펴보았듯이, 사용자의 개인정보를 처리하는 목적을 원 서비스 운영 등의 목적으로 사용하는지, 아니면 원 서비스의 범위를 벗어나서 사용하는 지로 분류할 수 있었다. 이 외에도 개인정보를 처리하는 주체에 따라 분류할 수 있는데, 수집한 개인정보를 개인정보처리자(기업)가 직접 사용하는 것인지, 제3자에게 제공하는지, 개인정보 처리업무를 위탁하는지, 개인정보를 제공·위탁받는 업체가 국내에 있는지 해외에 있는지에 따라 고려해야 하는 사항이 다르다. 따라서, 개인정보의 수집부터 파기까지 적법한 데이터 활용을 위해 기업이 고려해야 하는 사항을 단계별로 살펴보고자 한다.

4.1 개인정보 수집 시 고려사항

사용자의 개인정보를 수집하기에 앞서, 기업의 개인정보 보호책임자를 정하고 담당 부서와 담당자를 지정하여야 한다. 이때, 개인정보 보호책임자는 사업주 또는 대표, 임원의 지위에 있는 사람이 해야하기 때문에(법 시행령 제32조제2항) 중소·벤처 및 스타트업은 규모가 크지 않기 때문에 대표가 개인정보보호책임자인 경우가 많다.

4.1.1 개인정보 항목별 고려사항

서비스 제공을 위해 수집할 개인정보의 항목을 설정할 때에는 각 항목마다 세 가지를 확인하여야 한다.

첫 번째, 서비스 운영에 필요한 개인정보를 파악한다. 서비스를 제공할 때 수집하려는 개인정보가 반드시 필요한지를 따져 최소한의 개인정보만 수집해야 한다.

두 번째, 수집하고자 하는 개인정보가 사용자의 동의가 필요한지 파악한다. 사용자가 동의하지 않아도 법 제15조(제2-6항)에서 규정한 경우, 사용자 동의 없이 개인정보를 수집·이용할 수 있다. 특히 법 제15조

4항에 '정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우'를 주의해서 볼 필요가 있다. 예를 들어, 고혈압 환자를 위한 서비스를 제공하는 기업이라면 '혈압 데이터'는 서비스의 제공을 위해 필수불가결한 것으로 제15조 4항에 해당하기 때문에 사용자의 동의 없이 사용할 수 있다고 생각할 수 있다. 하지만, 혈압 데이터는 개인의 건강정보로 '민감정보'에도 해당하므로, 법 제23조에 따라 사용자로부터 동의를 받아야 한다. 이렇듯 수집하는 개인정보가 필수불가결한 것임에도 다른 조항에 영향을 받아 사용자의 동의를 받아야 하는 경우나 혹은 제15조(제2-6항)에 해당하지 않아 사용자의 동의를 받아야 한다면 개인정보 활용 목적에 따라 필수 동의 항목과 선택 동의 항목으로 나누어진다. 원 서비스 목적 내 원 서비스 제공을 위해 '불가피하게' 필요한 정보가 아닌 필요한 최소한의 개인정보는 필수 항목으로 동의를 받아야 하고, 그 외 다른 목적으로 사용되는 경우 선택 항목으로 동의를 받아야 한다. 사용자가 선택 항목에 동의하지 않았다고 해서 원 서비스 제공을 거부해서는 안 된다.

세 번째, 수집하고자 하는 개인정보에 고유식별정보, 민감정보가 포함되어 있는지 확인해야 한다. 특히, 고유식별정보의 경우 사용자의 동의가 있더라도 법적 근거가 있어야만 처리할 수 있는데, 만약, 법적 근거에 해당하지 않는다면 고유식별정보를 대체할 수 있는 수단(휴대폰 인증, 공인인증서, 아이핀 등)을 사용하여야 한다.

4.1.2 개인정보 처리를 위한 필수 문서 구비

수집할 개인정보에 대해 항목과 목적을 정하였다면 개인정보 처리를 위한 필수문서인 동의서, 개인정보처리방침을 작성하여야 한다.

동의는 다른 개인정보 처리 요건과 달리 정보주체가 자신의 개인정보 처리 여부에 대한 통제권을 행사할 수 있는 수단으로, 개인정보처리자인 기업이 정보주체의 동의권을 보장할 수 있도록 동의서를 작성한다[12]. 동의서에는 처리하려는 개인정보에 대한 동의 내용을 기재하고, 필요시 제3자 제공, 위탁, 국외 이전 등에 내용을 작성한다. 헬스케어 서비스 특성상, 수집하는 개인정보에 건강정보, 즉 민감정보가 포함될 가능성이 크다. 만약 고유식별정보와 민감정보를 수집한다면 다른 수집항목과 구분하여 별도의 동의서로 작성하여 동의를 받아야 한다.

개인정보처리자인 기업은 개인정보 처리 현황을 구체적으로 수립하여 투명하게 공개해야 하는 의무가 있다. 따라서 개인정보처리자는 법 제30조에서 요구하는 내용을 수립하고 개인정보 처리방침에 반드시 기재하여 정보주체가 쉽게 확인할 수 있도록 공개하여야 하는 의무가 있다. 개인정보 처리방침에는 개인정보의 처리 목적, 처리 및 보유기간, 처리하는 개인정보 항목, 파기, 정보주체의 권리 의무 행사방법, 안전성 확보조치에 관한 사항, 개인정보 보호책임자, 열람청구부서, 권익 침해 구제방법 등에 대해 반드시 기재하여야 하며, 해당 시 개인정보의 제3자 제공, 위탁, 국외 이전, 행태정보 수집 및 이용 등에 관한 정보도 함께 작성해야 한다[23].

4.2 개인정보 이용 시 고려사항

이용 단계에서 가장 중요한 첫 번째는, 동의서와 개인정보 처리방침에 작성한 목적 내에서만 사용자의 개인정보를 이용하는 것이다. 사용자에게 동의받은 목적 외로 사용해서는 안 된다. 만약 개인정보를 사용하고자 하는 목적이 추가되거나 변경하고자 한다면 사용자에게 알리고 별도의 동의를 추가로 받아야 하며, 개인정보 처리방침의 내용도 변경되어야 한다.

두 번째, 사용자의 개인정보가 분실·도난·유출·변조 또는 훼손되지 않도록 내부관리계획을 수립해야 한다. 개인정보 데이터에 대해 접근 통제, 권한 관리, 암호화, 접근기록의 위변조 방지, 보안 프로그램 설치 및 운영해야 하며, 월 1회 이상 접속기록 관리, 연 1회 이상 시스템 취약점 점검을 하고 직원들을 대상으로 개인정보보호 교육을 실시하여야 한다.

세 번째, 사용자의 권리를 보장해야 한다. 법 제4조에 따르면, 정보주체는 자신의 개인정보에 대해 열람·처리정지·정정·삭제·파기를 요구할 권리를 가지기 때문에 기업은 사용자가 권리를 행사할 수 있는 방법을 제공하여야 한다. 사용자가 개인정보의 열람을 요청한 경우, 10일 이내(법 시행령 제41조 제4항)에 정보주체가 해당 개인정보를 열람할 수 있도록 하여야 한다. 정

정·삭제·처리정지를 요청한 경우, 다른 법령에 특별한 절차가 규정되어 있지 않다면 지체 없이 필요한 조치를 한 후 그 결과를 정보주체에게 알려야 한다.

4.3 개인정보 제공·위탁 시 고려사항

개인정보의 제공과 위탁은 다른 회사에 제공하는 행위는 동일하나 각기 다른 업무이다. 법 제17조에 따르면 '개인정보의 제공'은 개인정보처리자 외의 제3자에게 개인정보의 지배·관리권이 이전되는 것을 말하며, 개인정보를 저장한 매체나 수기문서를 전달하는 경우뿐만 아니라 DB 시스템에 대한 접속 권한을 허용하여 열람·복사가 가능하게 하여 개인정보를 공유하는 경우도 포함한다. '개인정보 처리업무 위탁'이란 개인정보처리자의 목적을 위하여 개인정보를 외부의 제3자에게 맡겨 업무를 처리하는 것으로, 콜센터나 A/S센터, 클라우드 서비스 업체 등이 위탁에 해당된다[21].

4.3.1 개인정보 제공 시 고려사항

개인정보를 제3자에게 제공하기 전, 무분별하게 여러 곳으로 제공되는 것을 막기 위해 제공하고자 하는 개인정보가 정말로 제공이 필요한지에 대해 먼저 점검해야 한다.

개인정보를 제3자에게 제공하는 경우, 개인정보를 제공받는 자, 제공받는 자의 목적, 제공 항목, 제공받는 자의 보유 및 이용 기간에 대해 사용자에게 알리고 동의를 받아야만 제공할 수 있다. 만약 타 사로부터 개인정보를 제공받은 경우, 전달받은 개인정보가 사용자로부터 적법한 동의를 받았는지 확인하여야 한다.

정보통신망을 통해 사용자의 개인정보를 송·수신할 때는 안전한 보안서버 구축(SSL, 암호화 응용프로그램 등) 등의 조치를 통해 데이터를 암호화해야 한다.

4.3.2 개인정보 위탁 시 고려사항

개인정보를 제3자에게 위탁하는 경우, 사용자의 동의를 받을 필요는 없으나 개인정보 처리방침에 위탁받은 자(수탁자), 위탁하는 업무 내용에 대해 각각 기재하여 고지하여야 한다. 또한 위탁 업무의 내용이나 수탁자가 변경되는 경우에는 개인정보 처리방침에 지체 없이 변경 사항을 공개하여야 한다.

개인정보처리자는 위탁계약 체결 시, 법 제26조에 따라, 수탁자가 안전하게 개인정보를 처리할 수 있게 교육하고, 안전하게 처리하는지 감독해야하는 의무가 있다. 현행법상에서는 위탁사에게 관리·감독의 의무만 규정하고 있고, 제재 대상에서는 제외되어 있다. 하지만 개인정보보호법 2차 개정안에는 개인정보 처리 위탁자도 과태료·과징금·형벌 등의 제재 대상에 포함되므로 더더욱 수탁사의 관리에 주의를 기울여야 한다.

4.4 개인정보 파기 시 고려사항

처리하고 있는 개인정보가 사용자에게 동의 받았던 보유 기간이 경과하였거나 개인정보의 처리 목적을 달성하는 등 더 이상 개인정보가 불필요하게 되었을 때에는 지체 없이 해당 개인정보를 파기하여야 한다. 개인정보를 파기할 때에는 복구 또는 재생되지 않도록 소각, 파쇄, 전용 소자장비를 이용하거나 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 해야 한다. 개인정보를 파기했다면, 개인정보보호책임자의 책임하에 파기 결과를 확인하여야 하며, 파기에 관한 사항을 기록·관리하여야 한다.

사용자로부터 동의를 받은 기간이 경과하였더라도 다른 법령에 따라 개인정보를 계속 보존하여야 하는 경우가 있다. 예를 들어, '전자상거래 등에서의 소비자보호에 관한 법률'에 따르면 표시·광고에 관한 기록은 6개월, 계약 또는 청약철회·대금 결제·재화 등의 공급 기록은 5년, 소비자 불만 또는 분쟁처리에 관한 기록은 3년 동안 보관해야 하는 의무가 있다. 이와 같이 개인정보를 계속 보관해야 하는 경우에는, 해당 개인정보를 별도의 데이터베이스(DB)로 옮기거나 보관장소를 달리하여 보존해야 한다.

정보통신서비스 제공자등은 개인정보 유효기간제에 따라, 1년 동안 서비스를 이용하지 않은 사용자의 개인정보를 보호하기 위해 개인정보를 파기하여야 한다. 하지만, 이 또한 다른 법령에 의거하거나 사용자의 별도 요청이 있는 경우 변경될 수 있다. 기간이 만료되기 30일 전까지 개인정보가 파기되는 사실과 기간 만료일, 파기되는 개인정보 항목 등에 대해 사용자에게 알려야 한다.

표 3. 개인정보 활용 시 고려사항
Table 3. Considerations of Personal Information use

Step	Action	
Collection	Have privacy officer and related department	
	Determine particulars to be collected	Identify minimum of personal information
		Verify whether user consent is required
		Verify personally identifiable information and sensitive information
	Draw the required document up	Consent form for collection, use, and provision
		Privacy Policy
Use	Use for purposes of consent and notification	
	Establish an internal management plan	
	Guarantee rights of user	
Provision · Outsourcing	Provision	Verify whether provision is necessary
		Obtain user consent
		Encrypt data when transmitting
	Outsourcing	Notify outsourcing personal information processing
		Manage and supervise the outsourcee
Destruction	Destroy to the extent is not recoverable or revivable	
	Verify related statutes	
	Personal information validity period plan	

5. 결론

디지털 헬스케어를 필두로 의료와 ICT의 융합은 가속화되고 있으며, 개인 건강관리 서비스 관련 시장은 계속해서 커질 전망이다. 또한 보건의료 마이데이터가 시행된다면, 디지털 헬스케어 서비스가 지금보다 더 활발히 이루어질 것으로 예상되는데, 디지털 헬스케어의 핵심요소인 데이터에는 민감정보가 많이 포함되어 있기 때문에 적극적인 활용과 동시에 안전한 보호 방안에 대해서도 함께 고려되어야 한다.

본 연구에서는 헬스케어 데이터를 사용하는 기업들이 헬스케어 데이터를 활용하는 목적을 총 6가지, 1)원 서비스의 제공, 2)원 서비스의 고도화, 3)원 서비스의 확장을 위해 사용되는 경우와 4)신규 서비스 개발, 5)가명 처리를 통한 데이터 제공, 6)타사로 데이터 제공 및 판매하는 경우로 제시하였다. 그리고 개인정보가 수집, 이용, 제공, 위탁, 파기되는 라이프사이클에 맞춰 개인정보보호법 준수를 위해 고려해야 하는 사항을 각각 살펴보았다.

만약 기업이 개인정보보호법이 규정하는 의무를 위반했을 때에는 과징금, 과태료가 부과되는데, 이때, 개인정보보호위원회는 법령에서 정한 안전조치를 기업이 이행했는지를 확인하고 이를 감안하여 과태료를 부과한다. 사용자의 동의를 올바르게 수집했는지, 사용자에게 동의하는 내용을 올바르게 알렸는지, 처리 목적에 맞게 사용했는지, 정보주체의 권리를 보장하고 개인정보를 올바르게 파기했는지, 기술적·관리적 보호조치 수행 등의 여부를 확인한다.

따라서, 기업들이 헬스케어 서비스에서 데이터를 활용하고자 할 때, 활용하고자 하는 목적이 본 연구에서 제시한 여섯 가지의 목적 중 어느 것에 해당하는지 확인하고, 그 목적의 분류에 대한 법적 요구사항을 이해하여 개인정보 라이프사이클 동안 고려해야 하는 사항들을 준수한다면, 기업이 적법하고 안전하게 개인정보를 활용할 수 있을 것이라 기대한다.

REFERENCES

[1] Da-eun Lee, Seok-kwan Kim, Digital Healthcare Innovation Trends and Policy Implications, Science & Technology Policy, Vol. 48, pp.1-32, Jun. 2018.

[2] A Survey of the Domestic Digital Healthcare Industry, Ministry of Trade, Industry and Energy, Feb. 2022.

[3] Gi-Jeong Han, The 4th industrial revolution and vitalization of the healthcare industry. Korea Insurance Research. p.12, May, 2017.

[4] Jae-young Jang, Tae-hwan Park, Beomsoo Kim. The Life Cycle Model Considering Legal and Technical Characteristics of Personal Data, Proceedings of the Society for E-Business Studies, p.2 Apr. 2012.

[5] Survey on Personal Information Protection, Personal Information Protection Commission, p.183, Feb. 2022.

[6] Oseong Kwon, Yunhui Choi, Current status

and implications of related laws·systems to promote the use of healthcare, KIET, pp.1-99, Oct. 2021.

[7] Park, Mi-Jeong. A Study on Legislative and Policy Measures for Big Health Care Data. Korean Journal of Medicine and Law. Vol. 26, No. 1, June. 2018.

[8] Geun Ryeong Kim, Dae-Hee Lee. Review on Healthcare Big Data Analysis - Focusing on Privacy Protection -, Institute for Law of Science & Technology, Vol.24, No.3. Oct. 2018

[9] Dohwi Park, Min-young Kang, The Three Revised Bills which Ease Regulations on the Use of Personal Information Passed : Medical Data, beyond Openness to Utilization, Samjong KPMG ERI, Vol. 124, Mar. 2020.

[10] Soo-young Kim, Hyunkyung Kim, Study on the Reasonable Regulation and Use of Personal Information on Digital Healthcare Environment, IT&LAW REVIEW, Vol., No. 12, Feb. 2016.

[11] Yeongguk Kim, Revision data 3 law and Issues of insurance business - Focusing on the activation of digital healthcare services -, Korean Insurance Law Association, Vol. 14, No.1, pp.1-30, Feb. 2020.

[12] Yoosang Park, Jongsun Choi, Jaeyoung Choi, Heterogeneous Sensor Data Acquisitin Model for Providing Healthcare Services in IoT Environments, Korea Information Processing Society, Vol.6, No.2, pp.77-84, Dec. 2016.

[13] Yoon-su Jeong, Kun-hee Han, Design of data integration model between hospitals for healthcare information collection, Journal of the Korea Convergence Society, Vol.9, No.6, pp.1-7, June, 2018.

[14] Dong-hyun Kim, Soon-seok Kim. A New Scheme for Risk Assessment Based on Data Context for De-Identification of Personal Information, Journal of The Korea Institute of Information Security & Cryptology, Vol. 30, No. 4, Aug. 2020.

[15] Hyun-joon Kim, Seung-hyun Jung, Kyung-hee Lee, Wan-sup Cho, Healthcare Bigdata Linkage and Standardization Process with Privacy Protection, Proceedings of the Korea Contents Association Conference. May. 2017.

[16] Seong-ho Park, Artificial Intelligence in Medicine : Beginner's Guide, Journal of the Korean Society of Radiology, , Vol.78, No.5, pp.301-308, May. 2018.

[17] Hyeong-won Yu, Eunsol Lee, Wookyun Kho, Ho-seong Han, Hyun-wook Han, Blockchain Technology for Healthcare Big Data Sharing, The Journal of Bigdata, Vol.3, No.1, pp.73-82, Aug, 2018.

[18] Sung-nam Cho, Yoon-su Jeong, ChungShick Oh, An Efficient cryptography for healthcare data in the cloud environment, Journal of Convergence for Information Technology, Vol.8, No.3, pp.63-69, June. 2018.

[19] Habin Im, Hee-joung Hwang, Mobile Framework Designed for Sharing Personal Health Data in Standards-Based Healthcare Platform, Journal of KIIT, Vol.14, No.10, pp.113-122, Oct. 2016.

[20] Yoon-su Jeong, An Efficiency Management Scheme using Big Data of Healthcare Patients using Puzzy AHP, Journal of Digital Convergence, Vol.13, No.4, pp.227-233, Apr. 2015.

[21] Easy-to-understand Personal Information Processing Consent Guide, Personal Information Protection Commission, p.26, Feb. 2022.

[22] Jaeyoung Jang, Taehwan Park, Beomsoo Kim. The life cycle model considering legal and technical characteristics of personal data, Proceedings of the Society for E-Business Studies, p.2 Apr. 2012.

[23] Guidelines for Writing a Privacy Policy, Personal Information Protection Commission, pp.13-39, Feb. 2022.

[24] Guidlines for Using Health Data, Personal Information Protection Commission & Ministry of Health and Welfare, pp.1-74,

Jan. 2021.
[25] Explanation of Standards for Technical·Administrative Protection Measures for Personal Information, Personal Information Protection Commission & KISA, pp.1-104, Dec. 2020.
[26] Biometric Information Protection Guideilnes, Personal Information Protection Commission, pp.1-58, Sep. 2021.
[27] Guidelines for the processing of pseudonymous data, Personal Information Protection Commission, , pp.1-72, Oct. 2021.

저자약력

정 재 은 (Jaeeun Jung)

- 2021년 2월: 인제대학교 헬스케어IT학 학사
- 2021년 3월~현재: 인제대학교 헬스케어IT공학 정보보안 석사과정

〈관심분야〉 개인정보, 헬스케어 데이터, 데이터 컴플라이언스

양 진 홍 (Jinhong Yang)

- 2017년 2월: KAIST 정보통신공학 박사
- 2017년 2월~2018년 1월: HECAS 기술책임(CTO)
- 2017년 10월~현재: 한국과학기술원 IT융합연구소 겸직교수
- 2018년 3월~현재: 인제대학교 헬스케어IT공학과 조교수

〈관심분야〉 데이터 컴플라이언스, 마이데이터, 헬스케어 데이터 활용