디지털헬스케어환경에서 개인정보의 활용과 규제의 합리적 조화방안 연구

김수영*, 김현경**

≪ 목 차 ≫

■ 투고일 : 2016. 1. 15 심사일 : 2016. 2. 15, 게재확정일 : 2016. 2. 25.

Ⅰ. 서론

2013년 LG유플러스와 의사협회가 클라우드컴퓨팅 기반의 의원급 전자의무기록시스템(Electronic Medical Record)의 공동개발을 시도하였으나, 현행법상 전자의무기록의 외부보관은 금지되어 있기 때문에 서비스 자체가 상용화 될 수 없었다. 반면 미국의 ‘프랙티스 퓨전(Practice Fusion)’이라는 기업은 클라우드컴퓨팅을 통해 실시간으로 수집되는 미국 전역의 익명화된 전자의무기록을 활용한 빅데이터를 분석한 결과 미국 전역에서 어떤 질병

* 서울과학기술대학교, IT정책전문대학원 박사과정.
** 서울과학기술대학교 IT정책전문대학원 조교수, 법학박사. 교신저자.

이 어떻게 관리되고 있는지, 특정 약이 특정 인구에 대해서 얼마나 어떻게 처방되고 있는지에 대한 데이터를 실시간으로 볼 수 있는 “Insight”라는 서비스를 2014년 5월 개시하였다.

스마트폰을 통해 쉽게 몸 상태를 측정하는 “웰니스 제품”과 “웨어러블 헬스기기”, 개인의 신체정보 및 의료정보를 모아 데이터분석을 통해 건강관리를 가능케 하는 “헬스킷” 등 ICT 기술의 발달은 최근 질병예방 및 치료, 건강관리의 새로운 방안으로 기대를 모으고 있다. 이러한 기대에 부응하듯 애플, 구글, 삼성 등 ICT분야의 선두 기업들은 차세대 산업으로서 디지털헬스케어를 지목하고 과감한 투자를 감행하고 있다.[1] 그러나 디지털헬스케어산업은 인간의 생명 혹은 건강과 직결되므로 다른 디지털산업보다 더욱 규제에 민감할 수밖에 없다. 규제가 이러한 기술 및 산업의 발전에 걸림돌이 된다는 의견과, 무분별한 기술의 발전이 오히려 인간생명의 위협을 야기할 수 있다는 의견이 공존한다.

이러한 논의의 핵심이슈는 결국 ‘개인의료정보’의 활용이다. 모든 디지털헬스케어서비스는 축척·분석된 ‘개인의료정보’의 활용을 통해서만 가능하다. 특히 이러한 정보는 대부분 개인의 신체상태와 직결되므로 ‘민감한’ 개인정보에 해당될 여지가 높다. 그럼에도 불구하고 이미 구글, 애플 등은 빅데이터·클라우드컴퓨팅 기반의 디지털헬스케어서비스 플랫폼을 구축하여 의료기관과의 연계 및 서비스 고도화에 박차를 가하고 있다. 그러나 현재 우리나라는 이러한 개인의료정보의 활용을 「의료법」 및 「개인정보 보호법」에서 규정하고 있으나 실질적 서비스 상용화를 위한 제도적 기반은 미흡하다. 따라서 본 고에서는 인간 삶의 질 향상이라는 기본적 명제를 바탕으로 디지털헬스케어서비스의 합리적 구현을 위한 ‘개인의료정보’의 규제방안을 모색해 보고자 한다. 이를 위해 실질적으로 ‘개인정보’가 활용되는 디지털헬스케어서비스 사례연구를 통해 불합리한 규제의 문제점을 명확히 하

1) IDC는 전 세계 헬스케어 IT 시장 규모가 2011년 840억 달러에서 2016년 1,150억 달러까지 성장할 것이라고 전망했으며, BBC 리서치는 향후 원격의료 기술의 도입 증가와 전자의무기록(EHR, Electronic Health Records)의 활성화가 헬스케어 IT 시장을 견인할 것으로 예상했다(IDC, KT경제경영연구소(2013), 스마트 헬스케어 시장의 성장과 기회 재인용).

고 이를 해결하기 위한 제도적 개선방안을 제시하고자 한다.

Ⅱ. 디지털헬스케어산업과 개인의료정보

1. 헬스케어산업 패러다임의 변화

의료서비스는 질병 치료에서 예방과 관리를 통해 건강한 삶을 유지하는 것으로 변화하고 있다. 이러한 변화는 첫째, 인구의 고령화, 생활수준의 향상, 의료비 부담 증가에 따라 질병의 예방 및 일상 관리의 중요성이 증대되고 있어 건강 수명 연장을 위한 개인 맞춤형 헬스케어에 대한 수요가 확대된다는 것이고, 둘째, 미래의 보건의료 서비스 시장은 치료 분야의 비중은 감소하고 진단, 사후 관리, 예방 부분의 시장 비중이 향상함을 의미한다.[2] ICT는 이러한 변화의 주요 촉매로 작용해 왔다. 의료분야에 대한 정보화는 일찌감치 1977년 의료보험 제도 시작 시 진료비 청구를 위한 행정업무 처리에 활용되면서부터 급격하게 발전하기 시작하였으며 이후 이헬스(e-Health), 유헬스(u-Health), 스마트 헬스(smart-Health), 웰니스(Wellness) 등과 같은 새로운 패러다임을 형성하게 되었다.[3] 특히 스마트 디바이스의 보급 확대는 개인별 건강 데이터를 끊임없이(continuously) 측정할 수 있게 해주었고, 무선 인터넷의 발달은 신속하고 안전하게 건강 데이터를 이동할 수 있게 해주었다. 뿐만 아니라 클라우드컴퓨팅은 수많은 비정형 데이터를 외부에서 저장 및 관리하도록 함으로서 개인 및 의료기관이 개인의료정보 공통플랫폼을 통해 다양한 의료서비스를 누릴 수 있게 되었다. 이러한 건강·의료관리서비스를 통상 '디지털 헬스케어' 또는 'IT헬스케어'라 칭한다.[4]

---

2) 이진수, "디지털 헬스케어 플랫폼과 주요기업 동향", 보건산업브리프 vol. 140, 한국보건산업진흥원, 2014. 9, 1면.

3) 이태희·정영철, "의료분야에서의 정보기술 융합연구 동향과 시사점". 보건복지포럼(209), 2014, 36-49면.

[그림 1]의료+IT 융합 트렌드의 변화

	e-헬스	u-헬스케어	Smart 헬스케어	IT헬스
주요 서비스	디지털병원, 의료정보화	e-헬스+원격진료, 만성질환관리	u-헬스+운동, 식사량 등 건강관리	Smart 헬스케어+개인 맞춤형관리, 근거중심의학, 예방의학, 자기관리
주요 Player	병원	병원, IT기업	병원, IT기업, 서비스업체	보험사, 서비스업체 등 모든 이해관계자
주요 이용자	의료인	의료인, 환자	의료인, 환자, 일반인	의료인, 환자, 일반인, 정부, 기업
주요 시스템	병원운영시스템	의무기록(EMR) 건강기록(EHR)	개인건강기록	IoT 기반 PHR,클라우드, 빅데이터, 인공지능

출처: 한국보건산업진흥원, 2014 보건산업백서, 359면

이러한 디지털헬스케어 패러다임의 주요 특징은 '예방중심', '맞춤의학', '환자중심', '자가건강중심'이라고 할 수 있다. 즉 과거 '치료 중심'에서 스마트 기기를 통해 스스로 건강을 관리하는 예방주의로 진화하고 있다. 또한 지금까지의 의학은 일반적으로 환자 개개인의 지속적인 건강관리 점검이 불가능했기 때문에 통계학적으로 전체 환자에 대한 유병율(prevalence)을

4) IT 헬스(health IT)란 착용 컴퓨터(wearable device), 건강앱, 빅데이터, 사물 인터넷 등 IT기술을 활용하여 건강관리 및 질환관리 등 헬스케어 서비스의 효과를 높이고 비용을 절감하는 융합형 미래성장산업이다. e-health, u-health, m-health, smart healthcare, digital healthcare, health IT 등 다양한 이름으로 불리고 있으며 아직 정확한 산업 분류나 기준이 있는 것은 아니나 IT 기술을 헬스케어산업에 접목하는 관련 기술 및 산업을 아우르는 것으로 통상 이해되고 있다. 세계보건기구(WHO)에서 정의한 용어는 e-health, m-health, tele-health 정도이고 m-health와 tele-health는 e-health의 하위요소로 정의한다. 백승수 외, "의료산업 패러다임 변화에 따른 IT헬스 발전방향", 「2014 보건산업백서」, 2015, 359면.

기반으로 단편적인 질환에 대한 진단을 통해 치료가 이루어져 왔다. 이는 전체 인구의 질환별 통계수치를 통한 추측 데이터로서 의료인은 진단 데이터를 기반으로 환자의 병력과 가족력을 종합적으로 판단하여 의료서비스를 제공하였다. 그러나 사람의 인체 구조는 동일하나 모두 다른 특성을 가진 유기체이기 때문에 이러한 일반적 통계치로는 한계가 있다고 할 것이다. 빅데이터에 기반한 데이터분석기술은 이러한 일반적 통계를 극복하여 개별 환자를 토대로 한 맞춤의학 및 근거중심의학으로의 발전을 가능하게 하고 있다. 한편 기존의 의료산업은 소비자가 주체가 될 수 없는 전문분야였다. 소비자인 환자들은 의사가 작성한 자신의 진료내역을 제공받기도 어려운 구조이며, 제공받는다 해도 의학적 지식의 부족으로 그 의미를 정확히 파악하기 어렵다. 따라서 의료인과 환자의 관계는 일종의 권력관계를 형성하게 되는데 의료 정보의 일방적 생산과 해석은 소비주체인 환자가 능동적인 의료소비행위를 할 수 없게 하는 구조로 작용해 왔고 이는 각종 의료사고 시 환자가 정보에 접근할 수 없게 하는 요인이 되었다. 하지만 건강정보를 측정할 수 있는 손쉬운 어플리케이션 서비스들과 전자의무기록장치의 접근은 소비자가 건강 및 의료서비스의 중심으로 이동할 수 있게 하는 기제로 작용할 수 있게 해주었다. 즉 기존의 의료진 중심에서 환자중심으로, 병원중심에서 다양한 스마트 헬스케어기기를 활용한 자가건강 중심으로 의료서비스와 산업이 변화, 발전하고 있다.

2. ‘디지털헬스케어서비스’와 ‘정보’의 흐름

ICT를 기반으로 한 디지털헬스케어서비스를 가능하게 하는 것은 결국 이용자 개인에 대한 “정보”이다. 특히 이러한 정보는 기기의 이용과정에서 수집, 관리, 활용되면서 서비스 제공을 가능하게 한다. 이러한 디지털헬스케어서비스에서 정보의 흐름은 정보가 수집되는 영역과 보관, 활용되는 영역으로 구분하여 볼 수 있다.

우선 개인의 건강 정보는 개인건강기기(Personal Health Device)를 통해 수집된다. 이러한 개인건강기기는 가정용 또는 휴대용기기에 센서를 내장

하여 언제 어디서나 개인의 건강상태를 측정할 수 있는 웨어러블 디바이스 등을 말한다. 주요 제품으로는 Fitbit Flex(핏비트), Fuel Band(나이키), Shine(미스핏), Gear Series(삼성전자) 등이 있다.[5] 최근 미국 식품의약국(Food and Drug Administration, FDA) 및 한국 식약처에서 의료기기로서의 규제를 받지 않아도 된다고 정의한 건강관리용 제품들, 일명 "웰니스" 제품들도 이에 해당된다. "웰니스"제품의 경우에는 건강관리용으로서 맥박, 수면 장애 등을 점검하여 사용자에게 정보를 알려줄 수는 있으나 본 데이터는 질병 진단의 목적을 가질 수 없기 때문에 의료용으로 사용할 수 없다. 또한 의료기기로서 규제를 받으나 ICT의 기술을 활용하는 심전도 측정 제품, 유전자 분석 제품들 또한 이에 해당한다. 이렇게 수집된 정보들은 스마트기기에 내장된 카메라 센서 및 앱세서리(앱과 연결된 악세서리를 이용하여 개인의 건강상태를 측정·관리할 수 있는 어플리케이션)인 PHA(Personal Health Application)를 통해 전송된다. 주요 PHA 제품으로는 Nike Move(나이키), S-헬스 (삼성전자), RunKeeper(피트니스키퍼) 등이 있다.[6]

두 번째로는 각 기기들로부터 측정된 결과가 집결되는 데이터 관리의 영역이다. 개인건강정보들은 각각의 정보를 통합하여 저장·관리할 수 있는 데이터 플랫폼이 필요하며, 이를 '개인건강정보 플랫폼(PHI Platform)' 또는 '디지털헬스케어 플랫폼'이라 한다. 외부사업자들이 개발한 헬스케어 제품들로부터 수집된 개인건강정보들은 이러한 하나의 플랫폼에서 통합·관리함으로서 개인의 건강상태를 종합적으로 분석할 수 있다. 개인건강정보(PHI)를 효율적으로 관리할 수 있는 플랫폼을 중심으로, 개인의 건강정보를 수집하는 제품공급자(PHD, PHA)와 건강관리·의료서비스 제공자가 참여함으로써 디지털헬스케어 생태계의 구현이 가능하다.[7] 클라우드컴퓨팅을 이용하여 개인용 의료 히스토리(PHR, EMR)를 모으는 형태와, SNS서비스

5) 이진수, "디지털 헬스케어 플랫폼과 주요기업 동향", 보건산업브리프 vol 140, 한국보건산업진흥원, 2014. 9, 4면.
6) 이진수, 전게논문, 4면.
7) 이진수, 전게논문, 4~5면.

로 구성되어 이용자들이 자발적으로 자신들의 의료 기록 및 정보를 공유하는 형태가 있다.[8] 개인건강정보 플랫폼 서비스의 특성상 다양한 공급자와 참여자(소비자)를 수용할 수 있는 사업자가 유의미한 개인건강정보 플랫폼 사업자로서 참여할 수 있어 애플, 구글과 같이 많은 이용자의 트래픽을 유도할 수 있는 플랫폼 사업자들이 이 영역에서 성과를 낼 수 있을 것으로 생각된다.

마지막으로는 이 데이터를 활용한 질병 진단 및 예측, 예방, 그리고 치료의 영역이다. 환자의 상태는 단편적인 결과 검사만으로 판단을 내릴 수 없고 종합적으로 개인의 의료히스토리(병력), 가족 내력(유전적 요인) 등 모든 정보를 복합적으로 판단하여 진단 및 치료를 하여야 하기 때문에 개인 의료히스토리 데이터 관리는 기존의 단편적인 검사체계를 보완할 수 있는 주요한 수단이며, 의료기관 및 의료인이 바뀌더라도 적합하고 신속한 의료서비스를 받을 수 있는 수단이기도 하다. 또한 개인별로 지속적인 데이터를 기반으로 한 의료히스토리는 개인의 질병 발병률을 객관적으로 예측할 수 있게 해주어 평소에 개개인이 건강을 관리하도록 해줄 수 있다. 또한 이는 관련 산업으로의 연계가 가능한데, 예를 들어 보험산업의 경우 기존에는 전체적인 유병율에 따라 책정되던 보험금액이 개인별로 세분화하여 측정할 수 있게 되어 합리적인 보험금 산정과 보험사기까지 줄일 수 있는 효과가 나타날 수 있다.

이처럼 디지털헬스케어서비스를 가능하게 하는 핵심 키워드는 바로 '개인의료정보'라고 할 수 있다.

---

8) SNS를 통해 의료정보를 공유하는 대표적 케이스로 'PatientsLikeMe'가 있다. 'PatientsLikeMe'는 2004년 29살의 젊은 나이로 희귀 질환인 루게릭병에 걸린 형제를 위해 3명의 MIT출신 엔지니어가 모여서 만든 환자들의 SNS로 2011년까지 루게릭병, 파킨슨씨병 등 22가지 만성 질환에만 제한적으로 새로운 멤버들을 받아들이다가, 이후로는 완전히 공개하여 암이나 당뇨병등 여타 다른 질병에 대한 환자들의 가입도 허용하고 있다. 이렇게 환자들을 통해 쌓인 데이터를 바탕으로 기존의 의학계 연구를 정면으로 반박하는 논문을 Nature Biotechnology 에 출판하기도 하였으며 매우 희귀한 질병을 가진 환자들을 서로 이어줌으로써, 학계와 제약업계에서 아직 연구가 되지 않은 해당 질병을 파악하기 위한 방도로도 많이 이용되고 있다.

3. 디지털헬스케어와 의료영역에서의 '개인정보'의 특성

「개인정보보호법」 제2조 제1호에서 "개인정보란 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."라 하였고, 「정보통신망 이용촉진 및 정보보호등에 관한 법률」에서도 개인정보를 유사하게 정의하고 있다.[9] 또한 「개인정보보호법」은 건강, 성생활 등에 관한 정보를 포함하여 '민감정보'를 별도로 규정하고 있다.[10] 한편 헌법재판소에서는 개인정보를 "개인의 신체, 신념, 사회적 지위, 신분 등과 같이 개인의 인격주체성을 특징짓는 사항으로서 그 개인의 동일성을 식별할 수 있게 하는 일체의 정보라고 할 수 있고, 반드시 개인의 내밀한 영역이나 사사(私事)의 영역에 속하는 정보에 국한되지 않고 공적 생활에서 형성되었거나 이미 공개된 정보까지 포함"하는 것으로 판시하였다.[11] 이러한 개념들을 종합해보면 개인정보는 생존하는 개인을 직접 식별하거나 다른 정보와 결합하여 식별할 수 있는 일체의 정보로 이해할 수 있다.

이러한 개인정보의 개념을 바탕으로 할 때 통상 의료영역에서의 개인정보는 일반적인 모든 영역을 보호대상으로 하는 개인정보와 유사하면서도 다음과 같은 개별적인 특징을 갖고 있다.[12]

---

9) 「정보통신망 이용촉진 및 정보보호등에 관한 법률」 제2조(정의) 6. 개인정보란 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말한다.

10) 「개인정보보호법」 제23조 개인정보처리자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 "민감정보"라 한다)를 처리하여서는 아니 된다.

11) 헌재 2005.05.26, 99헌마513, 판례집 제17권 제1집, 668, 682.

12) 이한주, "개인의료정보보호법 제정의 필요성과 입법방향", 「한국의료법학회지」 제22권 제1호, 2014, 180-181면.

우선 기본적으로 정보주체인 환자가 의료기관을 방문하여 의사 등 의료제공자 간의 신뢰를 통하여 생성되므로,[13] 관련자에 의한 다양한 접근과 이용이 가능하다. 따라서 의료기관에서 의료행위를 하는 담당 의사, 간호사, 의료기사 등 직접적으로 환자와 접촉하는 의료기관 종사자뿐만 아니라 수납·보험·입원관리 등 의료행정 담당자, 심지어 전산 담당자도 환자와의 직접적인 관련성은 없다 하더라도 본인의 업무범위 내에서 개인의 의료정보에 대한 접근이 가능하다. 그 외에도 의료기관이 관리하는 개인정보는 공공기관이 소관업무를 수행하기 위하여 불가피하거나, 국민건강보험공단에게 급여비용 심사·지급·대상여부 확인 등을 위한 경우거나, 의료기관으로부터 자동차보험진료수가를 청구 받은 보험회사 등이 의료기관에 대하여 관련 기록을 청구하는 등의 경우에는 정보주체의 동의와 관계없이 법률의 규정에 의해 제3자에게 제공할 수 있게 되어 제공 받은 기관(제3자)은 이러한 개인정보를 제공 받은 목적의 범위 내에서 이용할 수 있다.[14]

다음으로, 민감정보로서의 성격을 갖는다. 의료영역에서의 개인정보는 대체적으로 정보주체인 환자의 건강, 질병 및 유전정보와 관련된 정보로서, 만약 이러한 정보가 환자의 동의 없이 타인에게 공개될 경우 일반 개인정보와 비교하여 심각한 사생활의 침해를 가져올 수 있다. 특히 성병, 유전적 질환과 같이 의료기관에서 진료를 필요로 하는 의료정보뿐만 아니라, 성생활이나 신체적 비밀과 같은 정보도 타인에게 공개될 경우 개인의 사회생활에 치명적인 영향을 줄 수 있다. 게다가 한번 공개된 정보는 원상회복을 하는 것이 현실적으로 불가능하다는 점에서 보호의 필요성이 더 크다고 할 수 있다.[15]

그밖에 전문적 지식·경험·기술과의 결합이다. 의료영역에서의 개인정보는 정보주체인 환자의 일반 신상정보, 문진·검사 등을 통한 증상정보 등과 의

13) 장석천, “의료정보보호에 관한 입법방향”, 「법학연구」 제24권 제2호, 충북대학교 법학연구소, 2013. 12, 431면.
14) 정부균, “환자 의료정보 보호의 문제”, 「의료법학」 제9권 제2호, 대한의료법학회, 2008, 356면.
15) 조홍석, “위험사회에 있어 개인의 의료정보 보호방안”, 「한양법학」 제24권 제4집, 한양법학회, 2013. 11., 175면.

료인의 전문적인 지식과 경험이 결합하여 생성된다. 따라서 이러한 개인정보는 정보주체성의 문제를 가져올 수 있다. 환자에게 정보주체성이 인정된다는 점에서는 의견이 일치되지만, 의사 등 의료인 또는 의료기관에 대해서 정보주체성을 인정할 수 있는지의 문제를 검토해야 한다.

이러한 통상적인 의료영역에서의 개인정보의 특성은 디지털헬스케어서비스 환경에서 또 다른 특성을 보이게 된다. 우선 정보에 대한 접근과 이용의 범위가 더욱 확장된다. 기존 개인의료정보에 대한 접근과 이용이 의료진과 의료행정인을 포함한 의료관계자, 공공기관, 보험회사 중심이었다면 디지털헬스케어서비스 환경에서는 플랫폼사업자, 또는 이러한 플랫폼을 통해 데이터를 분석·가공하여 새로운 정보를 생성하려는 자 등까지 정보의 접근 및 이용이 확장된다. 다음으로 민감정보로서의 성격은 감소된다. 디지털헬스케어서비스의 수집대상 정보는 통상 의료진의 진단으로 이루어진 특정 질병에 대한 정보가 아니라 신체의 현재 상태를 측정하는 측정정보이므로 통상의 개인의료정보가 가지고 있는 민감성은 약화된다. 마지막으로 개인의료정보의 범위가 확대되며, 정보의 전문성은 낮아진다. 기존의 개인의료정보는 진료기록부 작성 중심의 개인의료정보였으나, 디지털헬스케어기기를 통해 수집되는 개인의료정보는 실시간 신체상태를 측정하는 측정정보 중심이므로 그 범위와 정보의 수(數)는 무한 증가할 수밖에 없다. 또한 기존의 개인의료정보가 이미 수집단계에서 의사·간호사 등의 전문적 소견이 부가된 즉 전문적인 지식과 경험이 결합하여 생성된 정보 중심이라면, 디지털헬스케어서비스 환경에서의 개인의료정보는 추후 가공·분석되는 것은 별론으로 하더라도 수집단계에서는 기기에 의한 실시간 측정·진단 중심의, 즉 가공되지 않은 데이터(raw data)가 상당부분 차지한다.

한편 현행 법령은 이러한 환경을 반영하여 의료·진료·보건·건강 등과 관련된 정보인 '개인의료정보'를 규정하고 있지는 않다. 다만 학자에 따라 (개인)의료정보를 다양하게 정의하고 있다. 의료현장에서 작성되는 모든 형태의 자료,[16] 의료제공의 필요성 여부를 판단하기 위하여 또는 의료제공을

16) 류화신, "전자의무기록의 운용 및 그에 대한 민·형사상 문제점", 「인터넷법률」 제32호, 2005. 11, 32~33면.

행하기 위하여 진료 등을 통해서 얻은 환자의 건강상태 등에 관한 정보,[17] 의무기록이나 진료카드 등에 기록되는 내용(진료기록),[18] 국민의 건강을 보호·증진하기 위하여 국가·지방자치단체·보건의료기관 또는 보건의료인 등이 행하는 모든 활동과 관련해서 의료현장에서 환자를 통해서 취득·작성되는 모든 종류의 보건의료 자료[19] 라는 견해 등이 있다. 또한 '의료정보'를 정보의 용도에 따라 환자의 기본인적정보, 건강보험정보, 진료정보, 진료관리정보, 요약정보, 사망기록정보 등으로, 생성시점에 따라 환자가 직접작성 혹은 객관적 사실에 의한 1차 의료정보와 이러한 1차 의료정보를 기초로 생성된 2차 의료정보(가공의료정보)로 구분하기도 한다.[20] 그밖에 '의료정보'를 환자에 의해 작성되는 주관정보, 검사 및 진료 등에 의한 객관정보, 그리고 의료인의 전문성에 기초하여 작성된 가치판단정보로 분류하기도 한다.[21] 한편 일반적으로 의료정보는 개인정보 중에서 국민의 건강을 보호·증진하기 위하여 의료인과 의료기관 등이 행하는 의료행위와 관련된 정보를 의미하여, 의료행위 전 과정에서 수집된 자료들과 이를 기초로 하여 연구·분석된 정보를 총괄하는 것으로 이해하는 견해도 있다.[22] 현행 「보건의료기본법」 제3조 제6호에서 '보건의료정보'의 개념을 "보건의료와 관련한 지식 또는 부호·숫자·문자·음성·음향·영상 등으로 표현된 모든 종류의 자료"라고 규정하고 있는데, 이는 보건의료라는 특정한 분야라는 것을 제외하고는 앞에서 기술한 개인정보의 개념과 유사하다. 또한 18대 국회에서 발의되었던 3건의 「건강정보보호법(안)」에서 규정되었던 '건강정보'[23]와

17) 백윤철, "우리나라에서 의료정보와 개인정보보호", 「헌법학연구」 제11권 제1호, 한국헌법학회, 2005, 417~418면.
18) 이부하, "환자의 의료정보권", 「한양법학」 제17집, 2005, 178면 이하 ; 이인영, "개정 의료법의 환자의 개인정보 보호규정에 관한 법리적 고찰", 「한림법학 Forum」 제11권, 2002, 137~138면.
19) 장석천, "의료정보보호에 관한 입법방향", 「법학연구」 제24권 제2호, 충북대학교 법학연구소, 2013. 12, 428면.
20) 백윤철, "우리나라에서 의료정보와 개인정보보호", 「헌법학연구」 11(1), 한국헌법학회. 2005. 395~442면.
21) 전영주, "의료정보와 개인정보보호", 「법학연구」 23, 한국법학회. 2006, 521~540면
22) 정규원, "의료정보의 활용 및 보호", 「정보법학」 제6권 제1호, 2002. 7, 3~4면.

도 유사한 측면이 있으나, 건강정보는 미래에 예측할 수 있는 정보와 가족병력도 포함하고 있다는 점에서 보호범위가 훨씬 크다고 해석할 수 있다.[24]

그러나 이러한 개념은 대부분 정보와 관련된 행위의 주체를 의료인·의료기관으로 제한함으로서 스마트기기에 의해 수집되는 개인의료정보는 제외된다. 본 고에서는 이러한 환경변화에 대한 법률적 쟁점을 제기, 분석하고자 하므로 '개인의료정보'의 행위관련자를 '의료인·의료기관'으로 제한하지 않고 '질병·부상에 대한 예방·진단·치료·재활과 출산·사망 및 건강증진에 관한 지식 또는 부호·숫자·문자·음성·음향·영상 등으로 표현된 모든 종류의 자료 중 개인을 직접 식별하거나 다른 정보와 결합하여 식별할 수 있는 일체의 정보'를 의미하는 것으로 '개인의료정보'를 정의하고자 한다.

Ⅲ. '개인의료정보' 규제법과 디지털헬스케어서비스 사례연구

1. 개인의료정보 규제법 현황

1) 개인의료정보의 수집·이용

「의료법」상 개인정보의 수집과 이용은 '진료기록부등의 작성을 위한

---

23) 유일호 의원안 제2조(정의) 1. "개인건강정보"란 보건의료인이 보건의료서비스의 제공 과정에서 지득한 환자 개인의 신체상황, 상병·치료, 과거병력, 가족병력 등의 개인건강기록과 이와 함께 포함되어 있는 환자의 성명·성별·주소 또는 주민등록번호 등 개인을 식별하는 것이 가능한 정보를 말한다.
전현희 의원안 제2조(정의) 1. "건강정보"란 보건의료인이 진료과정(건강검진 포함에서 얻은 개인의 과거·현재·미래의 신체적이거나 정신적인 건강상태, 상병·치료 및 과거병력, 가족병력 등의 진료정보를 말한다.
백원우 의원안 제2조(정의) 1. "건강정보"란 질병·부상에 대한 예방·진단·치료·재활과 출산·사망 및 건강증진에 관한 지식 또는 부호·숫자·문자·음성·음향·영상 등으로 표현된 모든 종류의 자료를 말한다.

24) 이한주, "의료영역에서의 개인정보보호의 문제점과 해결방안", 「한국의료법학회지」 제20권 제2호, 한국의료법학회, 2012, 269~272면 참고.

개인정보'와 '그 외의 의료서비스 제공을 위한 개인정보'로 나뉘어 그 적용법이 다르다.

의료인은 「의료법」에 따라서 진료기록부, 조산기록부, 간호기록부, 처방전 그 밖의 진료에 관한 기록(이하 "진료기록부등"이라 한다)의 작성을 위해 환자의 성명, 주민등록번호, 주소, 질병정보 등을 정보주체의 별도의 사전 동의 없이 수집하여 관리할 수 있다(「의료법」 제22조, 동법 시행규칙 제14조). 법령에 의해 수집하는 이러한 진료목적의 개인정보는 정보주체의 의사에 관계없이 개인정보를 수집할 수 있는 경우로서 「개인정보 보호법」상 '다른 법률과의 관계' 규정에 의해(「개인정보 보호법」 제6조)[25] 또는 개인정보 보호법 제15조제1항제2호에 의거 '법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우'에 해당되므로 동의절차가 불필요하다.[26] 다만 진료의 예약, 진단결과 통보, 진료비 청구, 증명서 발급, 진단결과 통보를 위한 연락처 정보 등의 업무와 관련된 개인정보의 사전동의 면제에 대한 특칙이 규정되어 있지 않은 바 이와 관련하여서는 정보주체의 이익에 반하지 않으며 진료업무의 연장선상으로 보아야 하므로 이에 대한 사전 동의 없이도 수집할 수 있는 근거 규정이 필요하다.[27]

'그 외의 의료서비스 제공을 위한 개인정보'의 수집, 이용에 대하여는 「의료법」상 특별한 규정이 없으므로 「개인정보 보호법」이 적용된다. 의료기관에서 진료정보, 학술정보, 병원소식 등의 안내 및 환자의 의견수렴을 위해 휴대전화 문자, 이메일 등을 통해 추가 서비스를 제공하는 경우

25) 제6조(다른 법률과의 관계) 개인정보 보호에 관하여는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따른다.

26) 제15조(개인정보의 수집·이용) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.
2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우

27) 2012년 9월 행정안전부에서 작성한 "개인정보보호법 적용 사례(의료기관)"에 의하면 진료의 예약, 진단, 진단결과 통보, 진료비 청구, 증명서 발급 등은 진료목적으로 보며 진단결과 통보를 위한 연락처 정보까지는 동의 없이 수집 가능하다고 기술하고 있으나(2페이지) 이는 명백히 법령에 규정이 없는바 자의적 해석의 여지가 있다.

이에 필요한 개인정보는 그 수집 및 이용에 법령에 별도의 근거가 없으므로 「개인정보 보호법」에 의해 정보주체에게 별도의 동의를 받아야 한다. 이러한 서비스를 위한 개인정보는 가급적 진료정보와 별도로 관리하여야 하며 동의하지 않아도 진료에 지장이 없음을 고지하고 동의를 강요하지 않아야 한다. 의료기관에서 운영하는 홈페이지를 통해 진료정보, 학술정보, 병원소식 등의 안내 및 환자의 의견수렴을 목적으로 회원가입을 받는 경우에도 동의절차가 필요하다. 홈페이지 회원 가입시 필수정보, 선택정보를 구분하여 동의를 받아야 한다. 이러한 경우 홈페이지 회원 가입정보는 의료법에서 수집하도록 한 진료목적의 개인정보로 볼 수 없으므로 주민등록번호의 수집은 원칙적으로 금지된다.

다만 감염병의 예방 및 관리를 위한 개인정보 수집의 경우에는 사전동의의 예외가 인정된다. 예방접종을 하는 경우 또는 역학조사를 실시하여야 하는 경우 필연적으로 개인정보의 수집이 일어나게 된다(「감염병의 예방 및 관리에 관한 법률」 제18조부터 제18조의4).[28] 이는 「개인정보 보호법」상 “법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우(제17조제1항제2호)”에 해당된다고 볼 수 있다.

개인정보의 이용과 관련하여서는 ‘의료법’에서 특별히 규정하고 있는 바가 없으므로 ‘개인정보 보호법’이 적용된다. 따라서 그 수집 목적의 범위에서 이용하여야 하며, ①정보주체로부터 별도의 동의를 받은 경우, ②다른 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

28) 「감염병 예방 및 관리에 관한 법률」 제2조제17호 : 감염병환자, 감염병의사환자 또는 병원체보유자(이하 "감염병환자등"이라 한다)가 발생한 경우 감염병의 차단과 확산 방지 등을 위하여 감염병환자등의 발생 규모를 파악하고 감염원을 추적하는 등의 활동과 감염병 예방접종 후 이상반응 사례가 발생한 경우 그 원인을 규명하기 위하여 하는 활동을 말한다.

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 경우 에만 그 수집목적 범위 외에 이용할 수 있다.

또한 수집 후 개인정보가 분실·도난·유출·변조·훼손되지 않도록 안전성 확보에 필요한 기술적·관리적·물리적 조치 이행하여야 한다(법 제29조). 개인정보보호책임자 지정, 개인정보보호책임자와 개인정보취급자의 역할 및 책임, 안전성 확보를 위한 조치사항(보안장비 설치, 암호화, 열람기록 보관 등), 개인정보취급자의 교육에 관한 사항이 기재된 내부관리계획을 수립하여야 하며 그밖에 인터넷에 연결된 경우 방화벽 등 보안장비 설치, 개인정보 취급자 지정, 열람제한 및 열람기록 저장 등의 기술적 조치 등을 이행하여야 한다.

2) 개인의료정보의 제3자 제공

개인의료정보와 관련된 대표적인 개인정보 제3자 제공은 환자에 관한 기록을 열람하게 하거나 그 사본을 내주는 등 정보주체인 환자 이외의 자에게 환자에 대한 정보를 알려주는 것이라고 할 수 있다. 이에 대하여 「의료법」은 '의료인이나 의료기관 종사자는 환자가 아닌 다른 사람에게 환자에 관한 기록을 열람하게 하거나 그 사본을 내주는 등 내용을 확인할 수 있게 하여서는 아니 된다(「의료법」 제21조 제1항)'고 규정함으로써 원칙적으로 제3자 제공을 금지하고 있다. 다만 환자 본인의 동의서와 친족관계임을 증명한 경우, 건강보험료 지급을 위해 필요한 경우, 의료급여 지급을 위해 필요한 경우, 자동차보험진료수가를 청구 받은 보험회사등의 경우, 산업재해 보험급여의 경우, 징병검사의 경우, 민형사 재판을 위해 필요한 경우 등에 있어서 예외적으로 그 내용 열람 등이 가능하다(「의료법」 제21

조제2항). 또한 약사는 환자, 환자의 배우자, 환자의 직계존비속, 배우자의 직계존속(배우자·직계 존비속 및 배우자의 직계존속이 없으면 환자가 지정하는 대리인)이 제1항에 따른 조제기록부의 열람·사본 교부 등 그 내용 확인을 요구하면 이에 따라야 한다(「약사법」 제30조 제2항).

「의료법」상 제3자 제공이 가능한 경우가 아닌 한 「개인정보 보호법」에 따라 'i) 정보주체에게 별도의 동의를 받은 경우 그밖에 ii) 법률에 특별한 규정이 있거나 법령상 의무를 수행하기 위하여 불가피한 경우, iii) 사전동의를 받을 수 없는 경우로서 명백히 정보주체등의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우' 에 제3자 제공이 가능하다. 다만 사전동의의 예외로 역학조사, 전염병관리 등 감염병 예방 및 감염 전파의 차단을 위하여 필요한 경우에는 관련 개인정보를 보건복지부장관, 관련 중앙행정기관의 장, 지방자치단체의 장, 국민건강보험공단 이사장, 건강보험심사평가원 원장 및 감염병 관련 업무를 수행 중인 의료인, 의료기관, 그 밖의 단체 등이 서로 제공하면서 공동활용 할 수 있다. 의사나 한의사 또는 감염병병원체 확인기관의 소속 직원은 감염병환자를 발견한 경우 소속 기관의 장에게 보고하고 이러한 보고를 받은 소속관의 장은 이러한 사실을 보건복지부장관 또는 관할보건소장에게 신고하여야 한다(「감염병 예방 및 관리에 관한 법률」 제11조 및 제12조). 이러한 과정에서 필연적으로 환자정보의 제공이 이루어지게 된다. 이는 개인정보의 제3자 제공으로 「개인정보 보호법」상 "법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우(제17조제1항제2호)"에 해당된다. 이때 제공되는 개인정보는 i) 성명, 「주민등록법」 제7조제3항에 따른 주민등록번호, 주소 및 전화번호(휴대전화번호를 포함한다) 등 인적사항, ii) 「의료법」 제17조에 따른 처방전 및 같은 법 제22조에 따른 진료기록부등 iii) 보건복지부장관이 정하는 기간의 출입국관리기록, iv) 그 밖에 이동경로를 파악하기 위하여 대통령령으로 정하는 정보 등이다. 보건복지부장관은 이렇게 수집한 정보를 관련 중앙행정기관의 장, 지방자치단체의 장, 국민건강보험공단 이사장, 건강보험심사평가원 원장 및 감염병 관련 업무를 수행 중인 의료인, 의료기관, 그 밖의 단체 등에게 제공할 수 있다. 이 경우 감염병 예방

및 감염 전파의 차단을 위하여 해당 기관의 업무에 관련된 정보로 한정한다(「감염병 예방 및 관리에 관한 법률」 제76조의2제2항).

3) 개인의료정보의 보관·파기

의료인이나 의료기관 개설자는 전자의무기록을 안전하게 관리・보존하는 데에 필요한 시설과 장비를 갖추어야 하며(「의료법」 제23조제2항), 누구든지 정당한 사유 없이 이러한 의무기록에 저장된 개인정보를 탐지하거나 누출・변조 또는 훼손하여서는 아니 된다(「의료법」제23조제3항). 의료인이나 의료기관의 개설자가 전자의무기록을 안전하게 관리·보존하기 위하여 갖추어야 할 장비의 요건으로 'i)전자의무기록의 생성과 전자서명을 검증할 수 있는 장비, ii)전자서명이 있은 후 전자의무기록의 변경 여부를 확인할 수 있는 장비, iii)네트워크에 연결되지 아니한 백업저장시스템'을 규정하고 있다(「의료법 시행규칙」제16조). 따라서 네트워크에 연결되지 아니한 별도의 백업저장시스템을 갖추어야 하는 설비요건에 의하여 현행 클라우드컴퓨팅을 통한 전자의무기록의 보관은 곤란하다.

「의료법」에 의하면 의료인이나 의료기관 개설자는 진료기록부 등을 일정기간 보존하여야 한다(「의료법」 제22조). 다만 계속적 진료를 위하여 필요한 경우에는 1회에 한정하여 그 일정기간의 범위에서 그 기간을 연장하여 보존할 수 있다(「의료법 시행규칙」 제15조제1항). 또한 「감염병의 예방 및 관리에 관한 법률」에 의할 경우 예방접종에 관한 기록을 작성·보관하도록 규정하고 있다(제28조). 이러한 보고서에는 성명, 주민번호, 생년월일, 전화번호 등의 개인정보가 기록된다. 「약사법」 역시 처방전의 보존에 대하여 규정하고 있다. 즉 약사 또는 한약사가 약국에서 조제한 처방전은 조제한 날부터 2년 동안 보존하여야 한다(「약사법」 제29조). 뿐만 아니라 약사는 약국에서 의약품을 조제하면 환자의 인적 사항, 조제 연월일, 처방 약품명과 일수, 조제 내용 및 복약지도 내용, 그 밖에 보건복지부령으로 정하는 사항을 조제기록부(전자문서로 작성한 것을 포함한다)에 적어 5년 동안 보존하여야 한다(「약사법」 제30조 제1항).

다만 「의료법」과 「약사법」, 「감염병의 예방 및 관리에 관한 법률」에는 보존의무에 대한 규정만 있을 뿐 그러한 기간이 경과했을 때 어떻게 해야 하는지, 즉시 파기하여야 하는지 등 파기에 대한 규정은 없다. 따라서 파기와 관련하여서는 「개인정보 보호법」이 적용된다. 「개인정보 보호법」은 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하도록 규정하고 있다(제21조제1항). 개인정보를 폐기할 때에는 복구·재생되지 않도록 전자적 파일은 복원이 불가능한 방법으로 영구 삭제하고, 종이 등 기록매체는 파쇄 또는 소각하여야 한다.

2. '디지털헬스케어서비스'와 의료정보 활용 사례

1) 전자의무기록(EMR)의 활용 - 얼라이브코(AliveCor)

전자의무기록(Electronic Medical Record, 이하 "EMR"이라 한다)이란 기존의 종이차트로 관리되던 의무기록 관리 방식에 IT를 접목하여 병원에서 발생하는 의료정보를 일체의 수정 없이 모두 전산화하는 의료서비스시스템이다.[29] EMR보급은 2000년 21.6%[30]에서 2011년 70%미만이었다가 2014년 92.1%까지 높아진 가장 대표적인 의료정보 시스템이다.[31]

ICT기술의 발달은 이러한 EMR을 활용한 다양한 디지털헬스케어서비스의 출시를 가능하게 하고 있다. 미국의 경우 클라우드컴퓨팅 기반의 의료정보를 활용한 서비스 및 생태계가 빠르게 구축되고 있다. 당뇨병 환자를

---

29) EMR은 EHR(전자건강기록, Electronic Health Record)보다는 하위의 개념으로서 의미로서 EMR이 한 의료기관 내의 의료정보 시스템인데 비해, EHR은 의료정보의 전송과 교류를 통해 활용하는 원내뿐만 아니라 모든 웹 기반의 전자환자진료시스템까지 포함하는 개념이다. 이호용, "전자의무기록의 보관과 신뢰할 수 있는 제3의 기관의 활용", 「한양법학」 제24권 제4집(통권 제44집), 2013.11, 126면.

30) 서정욱, "전자건강기록(EHR)의 현황과 전망", 보건산업기술동향, 한국보건산업진흥원, 2005, 17면.

31) 보건복지부, '의료법 시행규칙' 일부개정령안 규제영향분석서', 2015. 11.

위한 서비스 '웰덱'은 미국 식품의약국(FDA)의 승인을 받아 수가체계를 인정받은 의료-헬스케어 서비스이다. '웰덱'은 환자 본인의 동의하에 의료기관에서 민간 보험회사와 연계하여 환자의 의료정보 및 건강정보를 클라우드컴퓨팅에 저장하고 이를 민간 보험사가 분석하여 병원에 전송한다. 전송된 데이터를 받은 의료기관은 데이터에 따라 환자에게 처방을 내려 건강을 관리할 수 있다.

'얼라이브코(AliveCor)'가 제공하는 '얼라이브 인사이트(Alive insight)'서비스는 사용자가 자신이 측정한 데이터를 미국 내 의사 면허를 갖고 있는 심혈관계 전문의(cardiologist) 및 심장 관련 테크니션(cardiac technician)에게 전송 하는 원격 진단 서비스라고 할 수 있다. 사용자가 스마트폰으로 측정한 ECG(심전도)데이터를 일정한 금액을 지불하고 원격으로 의료 전문가에게 전송하면, 일정 시간 후 그 데이터에 대한 해석 및 진단을 받아볼 수 있다.[32] 심장 기기 테크니션에게 데이터를 보내는 서비스는 지불하는 금액에 따라 30분 내, 혹은 24시간 내에 결과를 받아볼 수 있으며[33] 심혈관계 전문의에게 데이터를 보내면 24시간 내에 상태가 얼마나 심각한지를 나타내어주는 결과 및 권고 사항을 받아볼 수 있다. '얼라이브코(AliveCor)'는 미국 내 가장 큰 전자건강기록(EHR)[34] 기업 중 하나인 '프랙티스 퓨전(Practice Fusion)'과 연동하여 측정된 데이터를 의료기관의 의료진이 진료에 활용할 수 있도록 제공하고 있다. '프랙티스 퓨전(Practice Fusion)'의 EMR에 '얼라이브코(AliveCor)'가 연동되면서, 환자들이 측정한 ECG 데이

32) 최윤섭, "이미 시작된 미래 헬스케어 이노베이션", 클라우드 나인, 2014, 98면
33) 각각 서비스의 가격은 5달러, 2달러이다.
34) 모든 의료 기관의 전자 의료 기록(EMR)을 네트워크로 통합하여 공유하는 첨단 의료 정보화. 현재 각 의료 기관별로 개별 관리되고 있는 환자의 진료 관련 자료들을 통일 또는 호환성을 향상시키고, 시스템 및 서비스 표준화를 통해 중복 투자와 낭비를 줄이며, 임상 진료의 효과를 향상시킨다는 것이 주 목적이다. 전자 건강 기록(EHR)은 환자에 대한 처방 및 임상 실험, 진료 의사 결정뿐만 아니라 환자의 의료 정보에 대한 장기적 관리를 가능하게 해 주는 장점을 가지고 있으며, 네트워크화된 시스템은 진료 정보에 대한 저장뿐만 아니라 원격 진료, 치료, 처방, 건강 관리 및 분석과 기록을 가능하게 함으로써 의료의 질을 향상시킬 수 있는 기회를 제공한다. (IT용어사전, 한국정보통신기술협회)

터를 실시간으로 전송하여 EMR에 저장할 수 있고, 이 결과를 의사들이 일상적인 진료에 활용할 수 있다. 이제 의사들은 기존의 다른 일반적인 의료 테스트 결과와 함께, 환자들이 매일 측정한 ECG 데이터 또한 진료실에서 EMR을 통해 간편하게 확인하고 진료에 이용할 수 있다. '프렉티스 퓨전'은 미국에서 매달 10만 명의 의사가 사용하는 대규모 EHR이기 때문에 그 파급효과는 더욱 클 것으로 예상 된다. 의사들은 비용대비 효과적인 방법으로 환자들의 심장을 언제, 어디서나 측정하고, 이 데이터를 즉시 EMR로 받아들일 수 있으며, 환자들의 ECG(심전도)데이터를 '얼라이브코(AliveCor)'와 AliveInsight를 통해서 무선으로 기록 및 저장, 열람하고 이를 해석하여 전송하는 것이 가능하다. 또한 측정한 데이터는 클라우드컴퓨터 내에서 언제 어디서나 안전하게 저장할 수 있으며, 환자의 측정 결과 및 분석 레포트, 전문가 리뷰를 EMR과 함께 동기화 할 수 있다.

현재 우리나라 의료법에 의할 경우 전자의무기록(EMR)을 이러한 디지털헬스케어 사업자가 활용하는 것은 불가능하다. '의료법'은 '의료인이나 의료기관 종사자는 환자가 아닌 다른 사람에게 환자에 관한 기록을 열람하게 하거나 그 사본을 주는 등 내용을 확인할 수 있게 하여서는 아니 된다(의료법 제21조제1항)'고 규정함으로써 원칙적으로 제3자 제공을 금지하고 있다. 다만 건강보험료, 의료급여, 산업재해, 보험지급을 위해 필요한 경우 또는 역학조사, 전염병관리 등 감염병 예방 및 감염 전파의 차단을 위하여 필요한 경우에만 예외적으로 그 내용 열람 등이 가능하다. 그 밖의 경우에는 '개인정보 보호법'에 따라 'i) 정보주체에게 별도의 동의를 받은 경우 그밖에 ii) 법률에 특별한 규정이 있거나 법령상 의무를 수행을 위하여 불가피한 경우, iii) 사전 동의를 받을 수 없는 경우로서 명백히 정보주체등의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우' 에만 제3자 제공이 가능하다. 따라서 우리나라에서 '얼라이브코(AliveCor)'나 '웰덱'이 제공하는 서비스 출시는 일일이 구체적으로 서비스 내용에 대한 정보주체의 동의를 득하지 않는 한 현행법 위반이다. 또한 '얼라이브코(AliveCor)'의 '얼라이브 인사이트'서비스는 의사와 환자간의 원격진료를 허용하고 있는 미국에서나 가능하며 우리 의료법(제34조)은[35] 의료인과 의료

인간의 원격의료만을 허용하고 있는바 서비스 자체가 불가능하다.

2) 클라우드 EMR- 프랙티스 퓨전(Practice Fusion)

‘프랙티스 퓨전(Practice Fusion)’ 은 클라우드 컴퓨팅 모델을 통해 의료진들이 자유자재로 이용할 수 있는 웹 기반의 EMR제공 업체이다. ‘프랙티스 퓨전(Practice Fusion)’은 112,000 명 이상의 의사들이 사용하고 있으며, 8천1백 만 명 이상의 환자 기록을 가지고 있다.[36] 특히, 이 회사는 클라우드컴퓨팅에 실시간으로 수집되는 미국 전역의 의료 기록 빅데이터 및 관련 통계를 무료로 공개하는 Insight 라는 서비스를 2014년 5월 개시하였다. 이 데이터베이스를 기반으로 미국 전역에서 어떠한 질병이 어떻게 관리되고 있는지, 특정 약이 특정 인구에 대해서 얼마나 어떻게 처방되고 있는지에 대한 데이터를 실시간으로 볼 수 있다. 우리나라도 2013년 ‘LG유플러스’와 의사협회가 의원급 클라우드EMR을 개발하였으나 현행 「의료법 시행규칙」에 의하면 의료기관의 개설자가 전자의무기록을 안전하게 관리·보존하기 위하여 갖추어야 할 장비로 네트워크에 연결되지 아니한 백업저장시스템을 포함하고 있는 바,[37] 현행법규에 부합하지 않아 서비스가 상용화되지 못하였다. 당시 복지부는 클라우드컴퓨팅 방식의 의료정보 솔루션에 대해 “의료인이나 의료기관 개설자가 진료기록을 외부 클라우드 컴퓨팅 시스템에 보존하는 것은 의료법에 저촉될 것으로 판단된다"는 유권 해석을 한 바 있다.[38] 이후 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」이

35) 「의료법」 제34조(원격의료) ① 의료인(의료업에 종사하는 의사·치과의사·한의사만 해당한다)은 제33조제1항에도 불구하고 컴퓨터·화상통신 등 정보통신기술을 활용하여 먼 곳에 있는 의료인에게 의료지식이나 기술을 지원하는 원격의료(이하 "원격의료"라 한다)를 할 수 있다.

36) http://www.practicefusion.com/(2015.12.21.확인)

37) 「의료법 시행규칙」 제16조(전자의무기록의 관리·보존에 필요한 장비) 법 제23조제2항에 따라 의료인이나 의료기관의 개설자가 전자의무기록(電子醫務記錄)을 안전하게 관리·보존하기 위하여 갖추어야 할 장비는 다음 각 호와 같다.
1. 전자의무기록의 생성과 전자서명을 검증할 수 있는 장비
2. 전자서명이 있은 후 전자의무기록의 변경 여부를 확인할 수 있는 장비
3. 네트워크에 연결되지 아니한 백업저장시스템

2015년 9월 시행되어 '다른 법령에서 인가·허가·등록·지정 등의 요건으로 전산 시설·장비·설비 등을 규정한 경우 해당 전산시설등에 클라우드컴퓨팅 서비스가 포함되는 것으로 간주'하는 규정을 마련하였다.[39] 그러나 여전히 「의료법 시행규칙」에 의하면 의료기관은 네트워크에 연결되지 않은 백업 저장 시스템을 갖추고 있어야 한다고 규정하므로 클라우드컴퓨팅의 활용은 곤란하다. 의료산업 주무부처인 복지부도 여전히 "의료인이나 의료기관 개설자는 전자의무기록을 안전하게 관리-보존하는 데에 필요한 시설과 장비를 갖추고 외부보관을 금지 한다"는 유권 해석을 하고 있는 바[40] 의료기관 입장에서 클라우드컴퓨팅의 활용은 더욱 불안할 수밖에 없다.

3) 디지털 헬스케어 플랫폼

'애플'은 클라우드컴퓨팅을 기반으로 헬스앱을 통해 수집한 개인건강정보와 EMR정보의 통합을 통해 새로운 디지털헬스케어서비스를 제공하고자 종합적인 개인건강정보 통합 플랫폼 구축을 시도하고 있다. 애플의 HealthKit은 외부의 다양한 디바이스 어플리케이션을 통해 개인건강정보를 수집하고 이를 통합 저장·관리하는 시스템이다.[41] 이를 위해 애플은 헬스

---

38) 최윤섭, "디지털 헬스케어와 제도 개선 방향", 2015, 『디지털 시대의 기술융합 정책 무엇을 바꾸어야 하는가?』, 한국경제연구원 대외세미나, 3~5면. 재인용, 디지털 타임즈, "의료법에 발목 잡힌 클라우드 병원"(2013년 5월 27일)

39) 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제21조(전산시설등의 구비) 다른 법령에서 인가·허가·등록·지정 등의 요건으로 전산 시설·장비·설비 등(이하 "전산시설등"이라 한다)을 규정한 경우 해당 전산시설등에 클라우드컴퓨팅서비스가 포함되는 것으로 본다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.
1. 해당 법령에서 클라우드컴퓨팅서비스의 이용을 명시적으로 금지한 경우
2. 해당 법령에서 회선 또는 설비의 물리적 분리구축 등을 요구하여 사실상 클라우드컴퓨팅서비스 이용을 제한한 경우
3. 해당 법령에서 요구하는 전산시설등의 요건을 충족하지 못하는 클라우드컴퓨팅서비스를 이용하는 경우

40) http://www.ittoday.co.kr/news/articleView.html?idxno=66569(2015.12.21 확인)

41) 애플은 2014년 6월 3일, 자사의 개발자 행사인 WWDC 2014를 통해 모바일 운영체제 차기 버전 iOS8를 발표하고 디지털 헬스케어 플랫폼 HealthKit과 어플리

케어 시장에 다양한 외부사업자(Third party service)들을 끌어들여 개방형 헬스케어 생태계를 구축할 계획을 추진하고 있으며, 이와 동시에 iOS 어플리케이션을 개발하기 위한 iOS SDK(Software Development Kit)의 프레임워크로 HealthKit을 제공, 외부사업자는 애플의 앱스토어에 입점한 iOS 어플리케이션으로 한정함으로써 통제권을 발휘하고자 한다. 아울러 헬스어플리케이션을 통해 의료기관, EHR 시스템과 연계 및 의료서비스와 접목을 시도하고 있는데 지난 5년간 미국 의료기관인 Mayo Clinic과 협력을 통해 헬스어플리케이션을 공동으로 개발함으로써 단순한 건강데이터의 관리뿐 아니라 기존의 의료시스템과 통합까지 사업영역을 확대하고 있다. 또한 미국 최대 EHR 회사인 Epic과의 제휴를 통해 다양한 대형의료기관 환자들의 의료기록을 HealthKit과 통합함으로써 플랫폼 활용도를 극대화 하고자 하는 움직임을 보이고 있다.

앞서 살펴보았듯이 이러한 개인건강정보 통합 플랫폼은 우선 클라우드컴퓨팅을 기반으로 하는 한, 그리고 EMR정보와 다른 건강정보의 통합을 전제로 하는 한 현행 의료법 위반으로 우리나라에서는 서비스 상용화가 불가능하다.

3. 소결

현행법상 개인의료정보의 규제는 다음과 같이 요약될 수 있다. 첫째, 진료기록 중심의 개인의료정보 수집 규제이다. 「의료법」은 의료인·의료기관 등이 진료기록부 등의 작성을 위해 개인의료정보를 수집하는 것과 관련된 사항만 규정하고 있으므로 그 이외의 디지털헬스케어기기를 통한 개인의료정보에 대한 사항은 「개인정보 보호법」상의 정보주체 사전동의 중심의 규제를 따라야 한다. 둘째, 개인의료정보의 활용에 대한 엄격한 제한이다. 국내·외 진료정보 교류현황으로만 살펴봤을 때, EMR(전자진료기록), EHR(전자건강기록) 등의 구축률은 우리나라가 92%로 해외 81%보다 상당

케이션 Health를 탑재함으로써 디지털헬스분야 진출을 본격화하였다.

히 높은 수치를 기록한다. 그러나 의료기관간 진료정보교류 현황을 보면 해외가 39%인데 반해 우리는 1%미만에 그쳐 현저히 차이가 난다. 그 이유로 현재 구축된 전자의무기록시스템이 진료정보교류 기능을 위해서가 아닌 심평원에 수가청구를 위해 구축돼 있기 때문이라는 지적이 있으며, 각 의료기관별로 사용되는 용어가 표준화가 돼 있지 않아 시스템에서 제대로 인식을 하지 못하기 때문이라는 이유도 제기된다.[42] 그러나 무엇보다도 「의료법」이나 「개인정보 보호법」이 EMR의 활용 및 제3자 제공을 진료목적 등으로 엄격히 제한하고 있기 때문이다. 그리고 셋째, 디지털헬스케어기술의 불수용이다. 현행 「의료법」상 앞서 검토한 바와 같이 클라우드컴퓨팅서비스나 개인의료정보를 활용한 빅데이터 분석은 불가능하다. 의사와 환자간의 원격진료 역시 불가능하다.

통상적 의료절차에 의할 경우 의사는 환자의 진료를 위해 개인정보를 수집하게 된다. 이러한 개인의료정보를 기반으로 진료기록부 등을 작성한 후 의사는 처방전을 발행하고 환자는 처방전을 가지고 약국에 가서 약의 조제를 받게 된다. 현재의 개인의료정보의 규제는 단순히 이러한 면대면 의료행위 상황만을 가정하여 규율하고 있다. 그러나 ICT기술과 융합된 의료서비스는 환자의 정보수집이 이렇게 의사와의 대면을 통하여만 이루어지지 않는다. 앞서 사례에서 살펴본 바와 같이 각종 디지털헬스케어기기를 통해 개인의료정보가 수집될 수 있다. 또한 기존의 수집된 개인의료정보가 EMR 형태로 병원내의 시설과 장비안에만 머물러 있었다면 이제 클라우드컴퓨팅을 통해 보관·관리되는 개인의료정보는 다양한 방식으로 다른 정보와 융합되고 분석·처리되어 더 업데이트된 형태로 새로운 개인의료정보를 생성하게 된다. 이러한 서비스가 가능하기 위해서는 개인의료정보의 수집주체 및 제3자 제공의 범위가 확대 되어야 한다. 그러나 현재의 '의료 관련 법령'은 개인의료정보의 규제와 관련하여 이와 같이 진화된 기술적 상황을 반영하지 못하고 있다.

---

42) http://medipana.com/news/news_viewer.asp?NewsNum=172574&MainKind=A&NewsKind=5&vCount=12&vKind=1, 2015.12.21.확인

Ⅳ. 디지털헬스케어와 개인의료정보의 규제 합리화 방안

1. 규제방향

1) 신기술의 합리적 수용을 위한 규제의 수정

규제의 근본 이유는 '공익의 추구'이다. 규제는 공익이라는 규범적 계기에 의해 만들어지는 것이며 다만 이러한 공익적 계기가 사인이 자신의 이익을 위해 활용하려는 이익집단활동에 의해 왜곡될 수 있으나 이는 역관계인 규제완화에서도 마찬가지이다. 따라서 공익추구 결과 나타날 수 있는 사익의 추구는 그것이 규제의 주된 효과라기보다는 반사적 효과로서 나타나는 것이며 공익의 주된 본질은 "공공의 이익, 즉 공익"의 추구라고 하는 것이 타당하다.[43] 이러한 공익 추구라는 근본목표를 향한 규제원리는 여럿 있을 수 있으나 규제의 집행과 관련하여서는 집행대상자에 대한 차별 금지의 원칙, 어떻게 집행될지 수범자가 예측할 수 있는 집행예측성 원칙 등이 담보되어야 그러한 집행이 국민에게 명확히 인식되고 준수될 것이다. 이것이 바로 규제형평성[44]의 문제이다. 형평성과 관련한 중요한 원칙중의 하나가 동일한 범주의 대상을 동일하게 대우하는 것과 함께 동일하지 않은 것들에 대해서는 차등의 가능성을 의미하는 '동일범주 동일대우의 원칙'이다.[45]

그렇다면 '디지털헬스케어기술'을 둘러싼 규제환경이 기존 '의료환경'을 둘러싼 규제환경과 동일범주라고 할 수 있는가? 앞서 언급하였듯이 기존의

43) 김현경, "ICT규제원칙에 기반한 온라인서비스 비대칭규제의 개선방안에 관한 연구", 「성균관법학」 제26권제3호(2014.09), 490면.

44) 형평성은 그 어원에서 동등(equality), 일치(conformity), 균형(symmetry), 공평(fairness)을 의미하는 라틴어 aequitas에서 유래하였으며, 그 어원의 전개과정에서 볼 수 있는 것처럼 "규칙들의 기계적인 적용과는 다른 공평성에 따른 정의(justice)"를 의미한다(임의영, 사회적 형평성의 정의론적 논거 모색: R. Dworkin의 자원평등론을 중심으로. 「행정논총」,45(3), 2007, 1-21면.

45) 임의영, 행정이념의 이해. 이민호·윤수재·채종헌(편). 「한국의 행정이념과 실용행정」. 한국행정연구원, 공공성과 행정이념 연구총서(2). 2010.

‘의료환경’이 의사와 환자의 치료에 중점을 두었다면 현재는 클라우드컴퓨팅, 빅데이터, 각종 디지털헬스케어앱 등을 통한 예방·맞춤·자가건강 중심이라고 할 수 있다. 기존의 의료정보의 생성이 주로 의사와 환자의 진료를 통해서만 이루어졌다면, 이제는 각종 디지털헬스케어기기를 통해 생성된 의료정보가 추가되게 된다. 기존의 진료기록의 역할은 의사와 환자간의 치료 활용이 주된 기능이었다면, 이제 빅데이터 분석 기술을 통해 예방, 예측, 새로운 의료정보의 생성 등 그 역할·기능이 다변화 되고 있다. 또한 사후 분쟁의 대비 또는 의료인들 간의 협업 차원에서 의료기관에만 보관되어 있던 진료기록들은 각종 플랫폼을 통해 다양한 목적으로 활용이 용이해 진다. 이처럼 규제환경은 변화하였다. 그렇다면 기존의 의료환경에 맞추어져 있었던 규제는 규제형평성 측면에서 변화된 규제환경에 부응해야 한다. 즉 기술의 발전에 따른 규제의 방향은 규제원칙의 변경이 아니라, 변화된 환경에 부합하는 규제내용의 수정이다. 과거 종이의무기록만 그 유효성을 인정하였던 규제가 의무기록의 전자적 처리가 가능해 지면서 ‘전자의무기록’의 법적 효력을 인정한 것과 같이 ‘공익’이라는 ‘원칙’의 준수가 보장되는 한 당연히 변화된 환경에 부합하도록 규제의 합리적 ‘수정’이 이루어져야 한다. 이러한 합리적 수정의 기본적 방향은 당연히 정보주체에게 유익한 신규서비스의 수용이라고 할 수 있다.

2) 개인의료정보의 부가가치 극대화

개인의료정보는 보호되어야 할 프라이버시로서의 가치와 활용되어야 할 정보로서의 가치를 모두 지니고 있으며 일정한 상황에서는 이것을 형량하지 않을 수 없다. 물론 이들 양자 중 어느 하나를 반드시 선택하는 것이 아니라 각자의 가치만으로 의미를 가지는 경우가 더 많을 것이다.[46] 개인의료정보는 지극히 개인적인 건강정보, 생활습성, 신체적 특징 등과 같은 내용들을 담고 있어서 개인정보 중에서도 가장 프라이버시가 강조되는 민

46) 이호용, “전자의무기록의 보관과 신뢰할 수 있는 제3의 기관의 활용”, 「한양법학」 제24권 제4집(통권 제44집) 2013.11, 124면

감한 정보라고 할 수 있다. 반면, 축적된 정보를 이용하여 희귀한 질병에 대한 학술 연구・통계자료 작성 등의 2차적 목적으로의 활용 등 보건정책 또는 의학의 연구라는 공익적 목적 역시 간과될 수 없다. 이러한 활용은 생명의학산업이라는 고부가가치산업을 창출할 수 있는 중요한 기반이 되기 때문에 최근에는 그 필요성이 더욱 증대되고 있다.[47] 이러한 필요성의 증대는 결국 디지털헬스케어기술의 발달과 관련된다. 과거 데이터 분석기술이 요원한 시대에는 개인의료정보의 가치가 개인의 질병치료를 위한 제한적 활용에 한정되었다. 그러나 빅데이터, 클라우드컴퓨팅, 디지털헬스케어 기기의 발달은 더 이상 개인의료정보가 개인적 진료와 관련된 활용대상으로 제한되지 않고 국민 건강, 질병 예방, 의학 연구에 있어서 더욱 유의미한 자료로 활용되는 것을 가능하게 하였다. 미국에서는 의료(Health care) 분야에서 연간 3,000억 달러(스페인 연간 의료비의 2배) 이상의 새로운 가치창출을 전망한 바 있으며[48] 빅데이터 도입, 활용이 매우 기대되는 영역의 하나로 의료분야를 꼽고 있다.[49]

기존의 기술적 한계로 인해 개인의료정보의 활용이 개인의 질병치료적 사용에 제한되었다면, 그 규율 역시 개인의 프라이버시적 관점에서 규제되는 것이 타당하다. 그러나 기술의 발달은 개인의료정보의 활용가치를 획기적으로 변화시키고 있으며 이제는 건강연구·보건정책적 차원에서 공익적 요구에 부응하는 가치도 함께 고려되어야 한다. 즉 개인의 프라이버시 보호와 보건정책·건강연구의 공익적 가치가 조화를 이루도록 규율되어야 한다.

3) 의료의 공익적 가치 준수

47) 이한주, “의료영역에서의 개인정보보호의 문제점과 해결방안”, 「한국의료법학회지」 제20권 제2호, 한국의료법학회, 2012, 273면.
48) McKinsey Global Institute, Big data: The next frontier for innovation, competition, and productivity. 2011.06.
49) 안창원, 황승구. “빅 데이터 기술과 주요이슈”, 「정보과학회지」 30권6호, 한국정보과학회, 2012.6, 10~17면.

의료영역은 국민의 건강 및 보건과 직결되는 영역이므로 그 시장을 완전히 민간의 자율에 맡겨둘 수 없는 공익성이 높이 요구되는 영역이라고 할 수 있다. 최근 약학정보원[50]의 개인의료정보 무단 수집, 판매 사건에서도 볼 수 있듯이 개인의료정보가 유출 될 경우 그 여파는 단순히 경제적 피해뿐만 아니라 국민적 신뢰저하를 초래하게 된다.[51] 따라서 신기술의 수용에 양보되어져서는 안 되는 것이 공익적 가치의 존중이다.

미국의 신용도용범죄정보센터(Identity Theft Resource Center)[52] 통계분석 보고서에 의하면 자체적으로 수집한 약 9백만 개에 달하는 노출된 정보에 대해 총 데이터 침해 건수는 783건이며 이 중 보건의료 관련 정보는 333건으로 전체의 42.5%에 달하는 수치이고, 2005년 이후 약 300% 가량 증가했다고 하였다.[53] 또한 미국의 IT보안 연구소 SANS Institute(SysAmin, Audit, Network and Security)가 발표한 '의료산업에 대한 해킹위협 진단(SANS Health Care Cyber Threat Report-Widespread

---

50) 약학정보원은 대한 약사회 · 한국제약협회 · 한국의약품도매협회가 출연해 설립한 비영리 공익재단이다. 약학정보원은 국내 유통되는 의약품 관련 데이터베이스를 구축하고 보험청구 프로그램 등 약국 소프트웨어를 보급하는 등의 일을 하는 곳이다. 대한 약사회와 한국제약협회, 한국의약품도매협회 등 3개 단체가 자산을 출연해 설립 ·운영하는 약학정보원은 전국 병 ·의원과 약국에서 처방 ·조제되는 의약품의 종류와 수량 등을 암호화해 데이터베이스를 구축하고 관리한다("약학정보원서도 환자정보 유출 정황", 중앙일보 2013. 12. 12.).

51) 대한약사회 산하 기관인 약학정보원이 2011년 1월부터 2014년 11월까지 가맹 약국에 경영관리 프로그램 PM2000을 배부해 약 1만 800개 약국으로부터 환자 조제정보 43억3593만 건을 약국측에 설명하지 않고 환자들의 동의없이 수집·저장·보유한 후 판매한 혐의로 약학정보원과 IMS 헬스코리아 등 관련자 24명이 검찰에 기소된 사건이다. 특히 이들은 16억원을 받고 IMS사에 수집한 조제정보들을 판매했다는 것이 검찰측의 주장이다. 이와 관련 IMS 헬스코리아는 매입한 자료를 해외 본사에 임의 제공해 우리나라 국민들의 건강정보를 해외로 유출한 것은 물론, 이 자료를 통계처리해 제약사들에게 다시 판매해 총 70억원의 수익을 얻었다는 주장도 제기되고 있다(http://hnews.kr/n_news/news/view.html?no=30667.현대건강신문, 2015.11.9. 확인)

52) 미국의 신용도용범죄정보센터는 2005년부터 경영, 교육, 정부/군, 보건의료, 금융 등 각 분야별 데이터 침해 사고에 대해서 통계를 내고 있다.

53) ITRC Breach Statistics 2005-2014 http://www.idtheftcenter.org/images/breach/MultiYearStatistics.pdf (2016.1.8.확인)

Compromises Detected, Compliance Nightmare on Horizon) 연구보고서(2014년 2월 19일)에 의하면 2012년 9월부터 2013년 10월까지 의료서비스 제공기관과 건강관리사업단체, 의료보험업계, 보건의료정보센터, 제약업계, 기타 관련 보건의료 단체들 등 375개의 연관 업계의 보안악성 이벤트(security malicious events) 약 5만 건을 가지고 데이터 보안성을 점검한 결과 의료서비스 제공기관이 전체 악성 트래픽의 72%를, 건강관리사업단체가 9.9%를 차지해 가장 심각한 해킹 위험에 노출되어 있다고 진단하였다.[54]

따라서 개인의료정보의 규제를 전적으로 '정보주체의 의사' 혹은 '시장의 자율'에 맡기어서는 안 되며 국민건강, 보건이라는 공익적 목적을 위해 정보주체의 이익에 반하지 않는 한 개인의료정보의 수집 및 활용과 관련된 공익적 규제가 마련될 필요가 있다. 또한 개인의료정보는 대부분 질병과 관련되는 민감한 사항이므로 새로운 서비스의 수용과 더불어 이용과정에서 기술적·관리적 안전성이 확보되어야 한다.

2. 개선방안

1) '클라우드컴퓨팅서비스'의 명시적 허용

현행 「의료법 시행규칙」에 의하면 의료기관은 네트워크에 연결되지 않은 백업 저장 시스템을 갖추고 있어야 하므로 원칙적으로 전자의무기록의 보관과 관련하여 '클라우드컴퓨팅 '의 도입이 곤란하다. 이와 관련하여 보건복지부는 의료기관 내부보관으로 제한되던 현행 규제를 개선하여 의료기관 개설자에게 보관장소(내부, 외부)의 선택권을 명시적으로 부여하도록 「의료법 시행규칙」 개정을 시도하고 있다. 개정안에 의하면 전자의무기록

54) SANS, 2014 Health Care Cyberthreat Report: Widespread Compromises Detected, Compliance Nightmare on Horizon(http://www.sans.org/reading-room/whitepapers/firewalls/health-care-cyberthreat-report-widespread-compromises-detected-compliance-nightmare-horizon-34735).

의 관리・보존을 위한 시설・장비 기준을 내부・외부로 분리 규정하고, 환자진료기록의 보호를 위해 전자의무기록의 외부보관시 안전한 관리・보존을 위한 시설・장비를 갖추도록 세부기준을 마련하였다.[55] 그러나 전자의무기록의 외부 보관 시, 즉 클라우드컴퓨팅 이용 시 의료인이나 의료기관은 'i)전자의무기록의 생성 및 보관을 위하여 필요한 기능을 갖춘 장비, ii) 전자의무기록의 이력관리를 위하여 필요한 장비, iii) 전자의무기록의 복제・저장에 필요한 백업 장비, iv) 네트워크 및 시스템 보안에 관한 설비 및 장비, v) 전자시스템 운영에 필요한 장비, vi) 별도의 출입통제구역의 설치와 그 장소의 통제 및 감시를 위한 설비, vii) 재해예방에 관한 설비'를 갖추어야 하는 바, 현실적으로 보안 관점이나 시스템 장애에 따른 혼란이 적은 의원급 의료기관에게는 과도한 의무로 작용할 수 있다는 비판이 있다.[56] 뿐만 아니라 개정안 문구를 '외부'라고만 표현해 '외부'가 의미하는 것이 의료기관이 아닌 '외부장소'를 뜻하는 것인지, 제3 '외부기관'에 위탁을 하는 것인지 불명확하다는 지적과 함께, "제3자인 외부기관에 위탁하는 개념이라면, 상위법인 의료법 제21조[57]와 충돌한다."고 주장하는 등[58] 개정안에 대한 이해관계자의 반대 또한 첨예하다. 그러나 자료를 외부기관에

---

55) 의료법 시행규칙 일부개정령(안) 입법예고(2015.11.17.) 제16조(전자의무기록의 관리・보존에 필요한 시설・장비) ①<생략>
② 제1항에도 불구하고 의료인이나 의료기관의 개설자가 사용권한을 보유하고 있는 의료기관 외부의 전자시스템에서 전자의무기록을 관리・보존하고자 할 때에는 다음 각 호에서 정하는 시설・장비를 갖추어야 한다.
1. 전자의무기록의 생성 및 보관을 위하여 필요한 기능을 갖춘 장비
2. 전자의무기록의 이력관리를 위하여 필요한 장비
3. 전자의무기록의 복제・저장에 필요한 백업 장비
4. 네트워크 및 시스템 보안에 관한 설비 및 장비
5. 전자시스템 운영에 필요한 장비
6. 별도의 출입통제구역의 설치와 그 장소의 통제 및 감시를 위한 설비
7. 재해예방에 관한 설비
③- ④<생략>

56) http://www.ittoday.co.kr/news/articleView.html?idxno=66569, 2015,12,21 확인

57) 의료법 제21조(기록 열람 등) 제1항에는 '의료인이나 의료기관 종사자는 환자가 아닌 다른 사람에게 환자에 관한 기록을 열람하게 하거나 그 사본을 내주는 등 내용을 확인할 수 있게 하여서는 아니 된다'라고 명시돼 있다.

58) 헬스조선, '전자의무기록 외부보관 허용 법안은 '엉터리 규제안?', 2015. 11. 24

위탁한다 해도 위탁받은 외부기관이 전자의무기록의 내용을 마음대로 확인할 수 있는 것은 아니므로 이러한 주장은 타당하지 않다. 또한 '환자정보의 외부기관 축적에 따른 정보 악용 가능성'이라는 비판[59] 역시 타당하지 않다. 환자정보의 악용가능성은 내부에 의해서도 가능하며, 외부기관에서 환자정보를 악용하는 것을 막기 위해 각종 모니터링, 관제 시스템, 「개인정보보호법」상의 각종 기술적·관리적 보호조치 등이 마련되어 있기 때문이다. 결국 정보의 악용가능성은 전자의무기록의 관리·점검 및 이에 대한 제도 구비의 문제이지, 외부기관에 보관을 허용하는 것이 근본적인 문제라고 볼 수 없다.

그럼에도 불구하고 법령의 내용이 명확하지 않기 때문에 발생하는 비판은 여전히 의미가 있다. '외부'의 의미 자체가 물리적 공간을 기준으로 하는 것인지, 관리주체를 기준으로 하는 것인지 불명확하며, 외부기관의 시설·장비 기준을 내부와 동일하게 하였고 클라우드컴퓨팅의 기술적 특성에 대한 고려 또한 미흡하다. 법률에서는 '의료인이나 의료기관 개설자는 보건복지부령으로 정하는 바에 따라 전자의무기록을 안전하게 관리·보존하는 데에 필요한 시설과 장비를 갖추어야 한다(「의료법」 제23조제2항)'고 규정하고 있으므로 그 하위법규인 시행규칙에 '전자의무기록의 안전한 관리·보존을 위한 시설과 장비'에 명확히 '클라우드컴퓨팅서비스'를 포함하도록 규정하는 것이 바람직하다. 의료기관의 규모와 성격에 따라 '클라우드컴퓨팅서비스'의 내용도 다를 것이므로 '클라우드컴퓨팅서비스'의 품질이나 성능에 관한 사항을 일률적으로 시행규칙에 나열하기 보다는 고시를 통하여 융통성을 부여하는 것이 타당하다. 따라서 현재의 의료법 시행규칙 일부개정령(2015.11.17.) 제16조 제2항은 다음과 같이 수정될 필요가 있다

"제1항에도 불구하고 의료인이나 의료기관의 개설자는 '클라우드컴퓨팅발전 및 이용자 보호에 관한 법률' 제2조제3호에 따른 '클라우드컴퓨팅서비스'를 통하여 전자의무기록을 관리·보존할 수 있다. 다만 보건복지부장관

59) 헬스조선, '전자의무기록 외부보관 허용 법안은 '엉터리 규제안?', 2015. 11. 24

은 전자의무기록을 관리·보존하는 클라우드컴퓨팅서비스의 품질·성능에 관한 기준 및 정보보호에 관한 기준(관리적·물리적·기술적 보호조치를 포함한다)을 정하여 고시하고, 해당 클라우드컴퓨팅서비스 제공자는 그 기준을 준수하여야 한다."

2) EMR의 합리적 활용범위 확대

EMR은 행정/인구통계학적 자료(administrative/demographic data)와 임상자료(cinical data)로 구분할 수 있다. 행정/인구통계학적 자료는 병원에서 환자에게 처음으로 얻어진 자료로서 환자의 이름, 주소 및 전화번호 등의 개인 인적사항이 기록되며 진료비와 관련한 사항과 치료 및 수술 등의 다양한 동의서가 이에 속한다. 임상자료는 크게 진료기록(medical data), 간호기록(nursing data), 진료지원자료(ancillary data)로 나누어진다. 진료기록은 병력 및 신체검진기록, 수술기록, 경과기록 등 의사에 의해서 기록된 자료들을, 간호기록은 간호사가 기록한 투약기록 등을, 진료지원자료는 물리치료기록, 임상병리기록, 각종 검사기록, 사회사업관련 기록 등을 말하며 모두 진료를 위해 업무상 필요한 자료들을 의미한다.[60]

전자의무기록이 단순히 의료에 관한 정보를 획득하고 그것을 어떤 안전한 방법으로 저장하며, 임상적 필요에 의해 검색이 용이하도록 하는 메커니즘이라고만 한다면 종이문서로 된 의무기록 그 이상의 의미를 부여하기 어렵다. 전자의무기록을 통해 의료서비스의 공급자, 소비자, 비용 부담자 모두가 능률적이며, 삶의 질 향상에 도움이 되는 방향으로 상호 작용이 이루어져야 한다.[61] 이러한 상호작용은 결국 전자의무기록의 정보로서의 새로운 가치를 창출해 내게 되고 이러한 정보는 또다시 순환되어 새로운 유의미한 정보를 생성하게 된다. 미국의학연구소가 전자의무기록을 "완전하

60) 이주연 외, "대형 대학병원의 의무기록관리 현황분석 및 개선방안에 관한 연구", 「한국기록관리학회지」 제13권 제1호, 2013. 4. 20, 111면.
61) 노미진・정경수, "전자의무기록 성과에 관한 연구: 정보신뢰와 기술신뢰를 중심으로", 「경영연구」 제28권 제1호, 한국산업경영학회, 2013, 5면.

고 정확한 자료, 경보, 비망록, 임상적 의사결정 지원체계, 의료지식에 대한 연결망, 다른 보조수단에 대한 접근성을 제공함으로써 사용자를 지원하도록 설계된 체계를 가진 전자환자기록"이라고 정의한 것도[62] 이러한 의미를 부여한 것이라 하지 않을 수 없다. 만성질환과 같이 개인 단위의 건강정보 관리가 필요한 경우 개인별 맞춤형 의료서비스를 제공하는 데 효과적인 근거가 될 뿐만 아니라, 축적된 의료정보데이터는 다양한 조건별 진료나 간호의 가이드라인을 제공할 수 있다. 따라서 EMR이라는 정보가 가지는 부가가치를 극대화하기 위해서는 다음과 같은 규제의 개선이 이루어져야 한다.

우선 EMR의 활용대상과 범위에 대한 조정이 필요하다. EMR을 제한된 범위 내에서 제3자 즉 디지털헬스케어서비스제공자가 활용할 수 있도록 법률적 근거가 마련되어야 한다. 현행법상 EMR은 원칙적으로 병원의 진료를 위해 획득된 정보만으로 제한되어 있으며 그 활용역시 매우 제한적이다. 「의료법」은 원칙적으로 EMR의 제3자 제공을 금지하되, 건강보험료, 의료급여, 산업재해, 보험지급, 전염병관리 등을 위하여 필요한 경우에만 예외적으로 그 내용 열람 등이 가능하다. 다만 내용에 대하여 '열람'이 가능하다는 것이지 정보를 재가공·변환·다른 정보와 결합 등 '활용'할 수 있는 것이 아니다. 따라서 앞서 언급된 '디지털헬스케어서비스'의 제공을 위해 EMR을 활용하는 서비스의 경우에는 '정보주체에게 별도의 동의'를 받아야 한다. 설사 서비스 제공업체가 정보주체의 동의를 받았다 할지라고, 그러한 동의에 근거하여 의료기관은 보유하고 있는 EMR을 디지털헬스케어서비스 제공자에게 제공하여야 할 의무가 있는지는 별도의 문제다. EMR 기록에는 의사의 소견, 진단결과 등 의사의 주관적 진료결과가 담겨 있으므로 이에 대한 처분권이 전적으로 정보주체에게 있다고 볼 수 없기 때문이다. 따라서 정보주체의 의사에 기하여 EMR을 제3자 즉 디지털헬스케어서비스제공자가 활용할 수 있도록 하기 위해서는 법률의 규정이 마련되어야 한다.

다음으로 비식별화된 개인의료정보의 폭넓은 활용에 대한 근거가 마련될

62) 김경호, "전자의무기록(EMR)을 활용한 원무관리 개선" 법과정책연구 제6집 제1호, 한국법정책학회, 2006, 11면.

필요가 있다. EMR 중 법이 정하는 기술적 요건에 부합하는 비식별화 조치를 한 “비식별화 개인의료정보”에 대한 활용 근거 신설하는 방안이 검토되어야 한다. 개인의료정보로 수집된 정보에 비식별화 조치를 한다면 더 이상 ‘개인의료정보’에 해당되지 않는다는 견해도 있을 수 있다. 이러한 견해에 의할 경우 비식별화된 개인의료정보는 특별히 법률에 규정이 없더라도 법률상 ‘개인정보’에 해당되지 않으므로 제3자 제공 등 자유롭게 활용할 수 있다. 그러나 현행법상 개인정보의 개념에는 ‘해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것이 포함된다(「개인정보보호법」 제2조제1호). 따라서 재식별가능성이 존재한다면 현행법상 ‘개인정보’에 해당될 가능성이 농후하다.[63] 아무리 시간과 비용을 들여 비식별화 조치를 한다 할지라도 수집, 활용, 제3자 제공 등에 있어서의 사전동의 등 「개인정보보호법」상의 모든 의무를 준수하여야 한다. 따라서 법령에서 정하는 일정한 요건의 비식별화조치가 수반된 개인정보의 경우 즉 ‘특정 개인의 식별이 불가능하도록 또는 과도한(비합리적인) 시간적·비용적 노력을 통해서만 개인의 식별이 가능하도록 처리된 개인정보’를 ′비식별화된 개인정보‘ 라고 규정하여 「개인정보보호법상」의 개인정보처리자의 의무를 면제시켜 주되, 다만 재식별화 조치를 한 자에 대한 별도의 제재조치를 마련하는 방안으로 개선하는 것이 하나의 방안으로 제

63) 다음과 같은 개인정보 재식별화 사례가 있다. 미국 매사추세츠주의 단체보험위원회에서 공무원들의 병원 진료기록을 연구 목적 차원에서 공개하되, 이름, 주소, 사회보장번호 등 식별정보 제거하고, 기타 속성 정보만 공개(우편번호,생년월일, 성별 포함)하였다. 이 데이터를 이용해 개인을 재식별할 수 있는지 알아보기 위해, 매사추세츠주 케임브리지시의 선거인 명부를 구입 및 비교(L. Sweeny)한 결과 의료데이터와 투표자 명부로부터 특정 개인(주시사)의 개인정보를 재식별 할 수 있었다. 또 다른 사례로 미국의 비디오 대여 및 스트리밍 기업인 Netflix사(40개국 3,300만명)도 영화추천 시스템 개선을 위해 백만 달러에 달하는 Netflix Award를 공표하고, 6년간 50만명의 고객들이 작성한 1억건의 질의 데이터를 공개하였다(2006.10). 그러나 2007년 실명확인이 가능하다는 사실이 일부 연구진에 의해 공개되었다. 인터넷 무비 데이터베이스(IMDb)의 영화 평점 자료와 연계시킬 경우 6개의 영화 평점만을 비교해도 84%의 고객 이름 식별가능하다는 결과가 나오면서 2009년 고객의 집단 소송에 직면하게 되었고 관련 데이터 공개 종료하였다.

시될 수 있다.[64] 다만 비식별화의 기술적 수준은 각 영역별 대상정보의 중요도·민감도에 따라 달라질 수 있으므로 「개인정보 보호법」을 통해 일률적으로 정할 것이 아니라, 보건복지부가 전문가로 구성된 협의체의 논의를 통해 고시 등으로 정하는 방안이 고려될 수 있다. 1996년 제정된 미국의 '건강보험 이전과 책임에 관한 법(HIPAA, Health Insurance Portability and Accountability Act)'은 의료관련 행정 및 금융자료의 전자교환을 표준화하는 법률이다. 이러한 법률에 따라 개인의료정보 보호를 위해 마련된 규칙이 'HIPAA Privacy Rule'로 의료분야 개인정보보호에 대한 상세한 규정을 담고 있다. 'HIPAA Privacy Rule'에서는 해당 법에 의해 보호를 받는 의료정보(PHI, Protected Health Information)를 규정하고 있을 뿐 아니라, 보호대상에서 제외하여 의료정보의 자유로운 이용 및 제공을 허용하는 전면적 규율면제와 부분적인 규율면제에 대해 설정하고 있다. 먼저 보호를 받는 의료정보(PHI)는 '개인을 식별할 수 있는(individually identifiable) 정보' 혹은 '개인을 식별할 수 있는 합리적인 근거가 있는(reasonable basis) 정보'이며 이와 반하여 개인을 식별할 수 없는 즉, 비식별화된 의료정보(de-identified healthinformation)는 전면적 규율면제로 누구나 자유롭게 이용 및 제공할 수 있음을 명시하여 의료정보 이용에 있어 개인정보 비식별화가 중요 수단임을 명확히 하고 있다.[65]

또한 EMR과 결합되지 않은 단순한 건강정보만으로는 제공할 수 있는 서비스가 한정적일 수밖에 없다. 따라서 정보주체가 원할 시 데이터의 신뢰성과 관련된 일정한 요건을 구비한 경우 혹은 정부에 의해서 허가된(또는 인증된) 디지털기기를 통해 수집된 의료(건강)정보의 경우 EMR기재를 허용하고 이를 진료 시 의사 및 의료기관이 참조할 수 있도록 하는 규정을 도입하는 방안이 검토되어야 할 것이다. 다만 부정확한 정보의 EMR 기재는 자칫 EMR의 질적 저하에 따른 신뢰성 상실을 초래할 수 있으므로 그

64) 김현경, "'개인정보'와 '사물정보'의 규제 차별성에 관한 연구 - 사물인터넷 환경 하에서 서비스를 중심으로 -", 「성균관법학」 第27卷 第3號(2015.09), 49-50면.

65) 이인호. "개인정보 보호법 상의 '개인정보' 개념에 대한 해석론", 「정보법학」 19(1), 한국정보법학회. 2015, 59~87면.

요건과 범위를 정함에 있어서 신중을 기할 필요가 있다.

3) 공익적 규제를 통한 안전성·신뢰성 확보

2013년 7월 미국 라스베이거스에서 열린 '블랙햇 2013 컨퍼런스'에서는[66] 의사의 원격조정으로 체내에서 심장박동이나 인슐린 농도를 조절함으로써 생명을 유지시켜주는 체내삽입형 의료장치들의 주파수를 해킹하는 실험이 시연된 바 있다. 무선통신 기능을 지원하는 의료기기(예: 심박기와 같은 삽입형 의료기구)를 15m 떨어진 거리에서 해킹하여 원격 조정하여 고압 전류를 흘려 전기충격을 보내는 실험이, 또한 직접 당뇨 환자의 체내에 심어져 있는 인슐린 주입기기를 해킹하여 인슐린 주입량을 치사량 수준으로 조작해 결국 환자를 사망에 이르도록 하는 실험이 시연되었다.[67] 이처럼 심박조율기나 인슐린 펌프 등 인체에 삽입 가능한 의료기기는 무선통신 네트워크 덕택에 의료진이 환자에 대한 정보를 체내 장치에서 컴퓨터로 내려받거나 수술 없이 장치 조작만으로 실시간 치료 행위를 할 수 있게 된 대신, 해킹 등을 통해 그 취약성이 의도적으로 이용될 수 있다.[68] 즉 느슨한 사이버 보안표준, 암시장에서 높은 값으로 거래되는 의료기록 등은[69] 의료정보에 대한 사이버 침입을 증가시킬 것이며 인터넷에 연결된 디지털 헬스

66) 블랙햇은 악의적 목적의 정보 체계 침입, 컴퓨터 소프트웨어 변조, 컴퓨터 바이러스 유포 등의 행위로 해를 끼치는 해커를 말한다. 일명 크래커라고도 한다. 블랙햇 컨퍼런스는 각 분야의 연구원들에게 네트워크 및 전자기기 보안을 테스트할 수 있는 툴(tool)을 제공한다는 취지로 시작된 행사로, 다양한 해킹방법과 기법, 전략, 그리고 이를 방어할 수 있는 방안에 대해서 논의하는 컨퍼런스이다.

67) 블랙햇 USA 2013 공식 홈페이지(http://www.blackhat.com/us-13/schedule/index.html).

68) N. Paul et al., "A Review of the Security of Insulin Pump Infusion Systems," Journal of Diabetes Science and Technology, 5(6):1557-62 (November 2011).

69) EMC2/RSA 백서에 따르면, 2013년 상반기에 보고된 2백만 건 이상의 건강정보 중 31%가 유출되었다. 사이버 범죄자들이 훔친 사회보장번호나 신용카드 번호는 건당 1~2달러에 거래했지만, 의료 관련 정보는 아직 유통 물량이 적기때문에 최소 50달러에서 1,000달러까지 비싸게 거래되고 있다.

케어 기기와 함께 확장된 EHR의 유입은 사이버 범죄자들이 악용할 수 있는 매우 풍부한 새로운 환경을 생성하게 된다.[70] 디지털헬스케어 기기가 인간에게 완전히 이롭게 작동하기 위해서는 사이버 침입 전술, 기술과 절차(basic cyber intrusion tactics, techniques and procedures, TTPs), 지능형 지속가능위협(APT)과 같은 사이버 범죄에 대항하기 위한 기술적·제도적 기반이 전제되어야 한다.

현재 우리나라는 「의료기기법」에서 의료기기의 사용목적과 사용 시 인체에 미치는 잠재적 위해성(危害性) 등의 차이에 따라 의료기기 등급제를 실시하고 있으며, 의료기기 제조허가, 제조인증에 대한 제도를 두고 있다. 최근 식품의약품안전처는 규제개선의 일환으로 「의료기기법」상의 '의료기기'와 운동·레저 등에 사용되는 '개인용 건강관리제품(웰니스 제품)'을 명확하게 구분할 수 있는 '의료기기와 개인용 건강관리(웰니스) 제품 판단기준'을 마련한 바 있다.[71] 즉 웰니스 제품에 해당될 경우 해당 제품은 의료기기 규제대상에서 제외된다. 그러나 이에 대하여는 「의료기기법」상 의료기기의 개념과 유사한 웰니스제품을 법률을 통해서가 아니라 단순히 행정지침을 통해 규율하려 하는 것은 바람직하지 않다는 비판과 함께, '사용목적'이라는 판단기준 역시 지극히 자의적이라는 비판이 있다.[72] 즉 건강상태 또는 건강한 활동의 유지·향상 목적을 가진 웰니스 제품의 개념은 「의료기기법」상 질병을 진단·치료·경감·처치 또는 예방할 목적으로 사용되는 의료기기와 유사한 개념으로 이를 기준으로 웰니스 제품과 의료기기를 구

70) FBI, 2014 Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain(http://www.inforisktoday.com/fbi-issues-healthcare-cyber-alerts-a-6779 2016.1.8. 확인).

71) 식품의약품안전처, 의료기기와 개인용 건강관리(웰니스)제품 판단기준(지침), 2015.7.

72) 새정치민주연합 김성주 의원(전주덕진/국회보건복지위 간사)은 2015년 9월 국정감사에서 이러한 비판 외에도 식약처가 추진하고 있는 웰니스 제품 도입은 국회 입법권을 무시한 행정입법의 한계를 벗어난 것이며, 산업부에 의료기기 관리권한을 넘겨버리는 처사이자, 비의료인의 무면허 의료행위를 만연시키는 등 국민건강을 심각하게 훼손하는 것이라고 비판했다.http://www.yakup.com/news/index.html?mode=view&cat=11&nid=188867 (2016.1.12.확인)

분하겠다는 것은 타당하지 않으며. '사용목적'의 판단기준을 제조자등에 의해 제공된 규격(specification), 설명서(instruction), 정보(information) 등에 표현된 제품의 사용방법 등에 관한 제조자의 객관적인 의도로 판단토록 하고 있지만, 이러한 기준만으로 웰니스 제품인지 여부를 판단한다는 것은 결국 제조자의 의사에 따라 사용목적이 결정된다는 것에 불과하여 객관적인 기준이 되지 못하는 문제가 있다는 지적이다.

또한 이러한 지침은 기기 등을 통해 전달되는 개인의료정보의 정확성·신뢰성 및 그로 인한 피해 등에 대한 규율내용에 대하여는 담고 있지 않다. 따라서 헬스케어앱과 의료기기로부터 데이터를 전달하는 소프트웨어 일명 '메디컬디바이스 데이터 시스템(MDDS)'에 대한 정부의 적절한 규제와 사후 관리감독체계 마련이 필요하다. 우선 기본적인 건강통계에 대한 정보나 추적기록, 특정 치료 목적이 아닌 조언을 제공하는 질병 및 컨디션 관리 같은 기술정보에 대하여는 의료기기로서가 아니라 단순한 건강보조기구로서 그 규제를 완화할 필요가 있다. 그리고 이러한 기기에 대하여 그 정보의 신뢰도·기기의 오작동에 따른 정보의 부정확성에 대한 경고나 알림이 반드시 필요하다.

아울러 중요한 진단 혹은 치료 플랫폼으로 전환한 모바일앱 또는 모바일 기기에 대하여는 통상의 의료기기에 적용되는 규제가 준용되어야 할 것이며, 첨부파일이나 센서 등 다른 방법을 사용해 모바일 플랫폼을 규제대항이 되는 의료기기로 바꾸는 행위는 철저히 배제되어야 한다. 무엇보다도 향후 EMR과 연동되어 개인의료정보를 제공하는 디지털헬스케어기기, 플랫폼 등은 의료기기에 준하는 안전성·정확성·신뢰성 등에 대한 사전 검증체계의 마련이 필요하다. 현행 「의료기기법」상 의료기기의 등급은 인체에 접촉·침습 등으로 직접적 위해를 가하는 기준으로 작성되어 있는 바,[73] 개인의료정보를 제공하는 디지털헬스케어 기기, 플랫폼 등에 대하여는 이러

73) 의료기기법 시행규칙 제2조에 의한 의료기기의 등급분류 및 지정에 관한 기준과 절차에 의하면 잠재적 위해성에 대한 판단기준은 1) 인체와 접촉하고 있는 기간, 2) 침습의 정도, 3) 약품이나 에너지를 환자에게 전달하는지 여부, 4) 환자에게 생물학적 영향을 미치는지 여부 이다.

한 기준 외에 개인의료정보의 신뢰성·정확성·지속성 등이 확보될 수 있는지 여부도 고려되어야 할 것이다.

Ⅴ. 결론

ICT 기술의 발달은 최근 질병치료, 예방의학 등 의료 영역의 난제를 해결할 수 있는 해결책으로 기대를 모으고 있다. 이러한 기대에 부응하듯 애플, 구글, 삼성 등 ICT분야의 선두 기업들은 차세대 산업으로서 디지털헬스케어를 지목하고 과감한 투자를 감행하고 있다. 이러한 디지털헬스케어 서비스는 축척·분석된 '개인의료정보'의 활용을 통해서만 가능하다. 그러나 현재 우리나라는 이러한 개인의료정보의 활용과 관련하여 「의료법」 및 「개인정보 보호법」에서 그 활용 및 제3자 제공을 진료목적 등으로 엄격히 제한하고 있는 바 클라우드컴퓨팅이나 빅데이터 분석등을 통한 서비스 제공, 그리고 의사와 환자간의 원격진료 등은 불가능하다. 그러므로 앞서 살펴본 바와 같이 이미 미국에서 상용화되고 있는 '얼라이브코(AliveCor)'나 '프랙티스 퓨전(Practice Fusion)'의 서비스의 상용화는 곤란하다.

따라서 본 고에서는 인간 삶의 질 향상 이라는 기본적 공동명제를 바탕으로 디지털헬스케어서비스의 합리적 구현을 위한 "개인의료정보"의 규제방안을 모색해 보았다.

우선 변화된 디지털 헬스케어 환경을 기반으로 개인의료정보의 특성을 도출하였다. 기존 개인의료정보에 대한 접근과 이용이 의료진과 의료행정인을 포함한 의료관계자, 공공기관, 보험회사 중심이었다면 디지털헬스케어 플랫폼사업자 또는 이러한 플랫폼을 통해 데이터를 분석·가공하여 새로운 정보를 생성하려는 자 등에게 까지 정보의 접근 및 이용이 확장된다. 그리고 디지털헬스케어서비스의 수집대상 정보는 통상 의료진의 진단으로 이루어진 특정 질병에 대한 정보가 아니라 신체의 현재 상태를 측정하는 측정정보이므로 기존 의사 등의 진단 하에 이루어지는 전문성은 및 의료정보

고유의 민감성은 약화되나 정보의 범위와 수(數)는 무한 증가하게 된다.

따라서 기존의 의료정보의 특성을 기반으로 한 개인의료정보 규제는 타당하지 않다. 변화된 개인의료정보의 특성이 반영되어야 한다. 이러한 특성을 위한 규제방향으로 신기술의 합리적 수용을 위한 규제의 수정이 필요하며 개인의료정보의 부가가치 극대화시키기 위한 제도가 마련되어야 한다. 그러나 의료영역은 국민의 건강과 보건이 직결되는 공익성이 높이 요구되는 영역이므로 완전히 민간의 자율에 맡겨둘 수는 없다. 이러한 서비스가 가능하기 위해서는 신뢰성·안전성을 위한 제도적 기반이 함께 갖추어져야 한다. 이러한 규제방향을 수용하기 위한 법적 개선방안으로 '클라우드컴퓨팅서비스'의 명시적 허용을 위한 법령 개선안, EMR의 활용범위를 확대하기 위한 현행 규제의 개선방안을 모색하였다. 그리고 개인의료정보의 정확성·신뢰성 확보를 위해 헬스케어앱과 디지털 의료기기로부터 데이터를 전달하는 소프트웨어 일명 '메디컬디바이스 데이터 시스템(MDDS)'에 대한 정부의 적절한 규제와 사후 관리감독체계 마련을 제안하였다.

【참고문헌】

Ⅰ. 단행본

박경수 이경현, 「사물인터넷 전쟁」, 동아엠앤비, 2015.
이민영, 개인정보법제론 , 개정증보판, jinhan M&B, 2007.
이창범, 개인정보보호법, 법문사, 2012.
최윤섭, 「이미 시작된 미래 헬스케어 이노베이션」, 2014
행정안전부, 개인정보 보호법령 및 지침 고시 해설, 2011.

Ⅱ. 논문

김경호, “전자의무기록(EMR)을 활용한 원무관리 개선” 법과정책연구 제6집 제1호, 한국법정책학회, 2006.
김민호·김일환, “민간영역에서 개인정보의 처리와 이용에 관한 비교법적 고찰”, 토지공법연구 46권, 2009.
김민호, 공공부문 개인정보보호법제의 현황과 과제, 토지공법연구 제37집 제1호 2007. 8.
김용영・신승수, “신뢰할 수 있는 전자의무기록에 관한 연구”, 디지털정책연구 제10권 제2호, 한국디지털정책학회, 2012.
김현경, ICT규제원칙에 기반한 온라인서비스 비대칭규제의 개선방안에 관한 연구, 성균관법학 제26권제3호, 2014.09.
_____‘개인정보’와 ‘사물정보’의 규제 차별성에 관한 연구 - 사물인터넷 환경 하에서 서비스를 중심으로 -, 성균관법학 第27卷 第3號, 2015.09.
노미진・정경수, “전자의무기록 성과에 관한 연구: 정보신뢰와 기술신뢰를 중심으로”, 경영연구 제28권 제1호, 한국산업경영학회, 2013.
류화신, 전자의무기록의 운용 및 그에 대한 민·형사상 문제점, 인터넷법률 제32호, 2005. 11.

문재완, 개인정보의 개념에 관한 연구", 공법연구제42집제3호, 2014.

배대헌, '잰걸음으로 나선'개인정보 보호법을 보완하는 논의 : 개인정보 보호법 개정 논의 및 관련법률 검토, IT와 법연구 제6집, 경북대학교 IT와 법연구소, 2012.

_____, 개인정보 보호·이용에 관한 계약법적 방안 모색, 상사판례연구 제19집 제4권 , 2006년 12월.

백승수 외, "의료산업 패러다임 변화에 따른 IT헬스 발전방향", 『2014 보건산업백서』, 2015.

백윤철, 우리나라에서 의료정보와 개인정보보호, 헌법학연구 제11권 제1호, 한국헌법학회, 2005.

서정욱, '전자건강기록(EHR)의 현황과 전망, 보건산업기술동향, 한국보건산업진흥원, 2005.

성준호, 빅데이터 환경에서 개인정보보호에 관한 법적 검토, 법학연구, 제21권 제2호, 2013.

안창원, 황승구. 빅 데이터 기술과 주요이슈, 정보과학회지 30권6호, 한국정보과학회, 2012.6.

이부하, 환자의 의료정보권, 한양법학 제17집, 2005, 178면 이하;이인영, 개정 의료법의 환자의 개인정보 보호규정에 관한 법리적 고찰, 한림법학 Forum 제11권, 2002.

이상명, "의료정보화와 의료정보보호", 법학논총 제25집 제1호, 한양대 법학연구소, 2008.

이상직, ICT산업활성화를 위한 개인정보보호법의 현황과 과제, 개인정보보호법학회 세미나 자료집, 2015.4.

이은미 외, "의무기록관리의 현황과 개선방안: KS X ISO 15489 표준의 Y 병원 적용을 중심으로" 정보관리학회지 제29권 제3호, 한국정보관리학회. 2012.

이인영, "전자의무기록에 관한 법적 문제", 법학논총 제28집 제1호, 한양대 법학연구소, 2011.

이인호. 개인정보 보호법 상의 '개인정보' 개념에 대한 해석론, 정보법학

19(1), 한국정보법학회. 2015.

, 개인정보보호법제 개선을 위한 정책연구보고서 중 “개인정보처리(수집 이용 제공)의 법적 기준에 대한 타당성 분석”, 프라이버시 정책연구 포럼, 2013.2.

이한주, “개인의료정보보호법 제정의 필요성과 입법방향”, 한국의료법학회지 제22권 제1호, 2014.

이한주, 의료영역에서의 개인정보보호의 문제점과 해결방안, 한국의료법학회지 제20권 제2호, 한국의료법학회, 2012.

이호용, 전자의무기록의 보관과 신뢰할 수 있는 제3의 기관의 활용, 한양법학 제24권 제4집(통권 제44집) 2013.11.

이주연 외, ‘대형 대학병원의 의무기록관리 현황분석 및 개선방안에 관한 연구’, 한국기록관리학회지 제13권 제1호, 2013. 4. 20.

이진수, “디지털 헬스케어 플랫폼과 주요기업 동향”, 보건산업브리프 vol 140, 한국보건산업진흥원, 2014. 9.

이태희·정영철, 의료분야에서의 정보기술 융합연구 동향과 시사점. 보건복지포럼,(209), 2014.

임규철, 개인정보의 보호범위, 한독법학, 제17호, 2012.

임의영, 사회적 형평성의 정의론적 논거 모색: R. Dworkin의 자원평등론을 중심으로.「행정논총」,45(3), 2007.

장석천, “의료정보보호에 관한 입법방향”, 법학연구 제24권 제2호, 충북대학교 법학연구소, 2013. 12.

장주봉, 개인정보의 의미와 보호범위 , 법학평론 제3권, 서울대학교, 2012.

전경근, 개인정보의 활용범위에 관한 연구 , 아주법학, 제6권 제1호, 2012.

전응준, 위치정보법의 규제 및 개선방안에 관한 연구, 정보법학, 제18권 제1호.

전영주, 의료정보와 개인정보보호, 법학연구 23, 한국법학회. 2006.

정규원, 의료정보의 활용 및 보호, 정보법학 제6권 제1호, 2002. 7.

정상조・권영준, “개인정보의 보호와 민사적 구제수단”, 「법조」제58권제3호 통권630호, 2009.

정부균, 환자 의료정보 보호의 문제, 의료법학 제9권 제2호, 대한의료법학회, 2008.

조홍석, 위험사회에 있어 개인의 의료정보 보호방안, 한양법학 제24권 제4집, 한양법학회, 2013. 11.

최경진, 빅데이터와 개인정보 , 성균관법학 제25권 제2호, 2013.

최윤섭, “디지털 헬스케어와 제도 개선 방향”, 『디지털 시대의 기술융합 정책 무엇을 바꾸어야 하는가?』, 한국경제연구원 대외세미나, 2015.

함인선, 개인정보 처리와 관련한 법적 문제 , 경제규제와 법, 제6권 제1호, 20113.

황성기, 개인정보 보호와 다른 헌법적 가치의 조화, 프라이버시 정책연구포럼, 2013.

황창근, 사물인터넷과 개인정보보호, 법제연구 제46호, 2014.6.

Ⅲ. 외국문헌

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.

European Commission, Proposal f or a Regulation o f the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (Jan. 25, 2012).

FTC, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers, March 2012.

McKinsey Global Institute, Big data: The next frontier for innovation,

competition, and productivity. 2011.06.

Paul M. Schwartz & Daniel Solove, Reconciling Personal Information in the United States and European Union (September 6, 2013). 102 California Law Review (2014 Forthcoming)

Paul M. Schwartz & Daniel Solove, The PII Problem: Privacy and a New Concept of Personally Identifiable Information, 86 N.Y.U. L.Rev. 1814 (2011)

Paul M. Schwartz, "BEYOND LESSIG'S CODE FOR INTERNET PRIVACY: CYBERSPACE FILTERS, PRIVACY-CONTROL, AND FAIR INFORMATION PRACTICES", 2000 Wisconsin Law Review 743.

Sharona Hoffman & Andy Podgurski, FINDING A CURE: THE CASE FOR REGULATION AND OVERSIGHT OF ELECTRONIC HEALTH RECORD SYSTEMS, Harvard Journal of Law & Technology Volume 22, Number 1 Fall 2008

Nicolas P. Terry, PROTECTING PATIENT PRIVACY IN THE AGE OF BIG DATA, Robert H. McKinney School of Law, Legal Studies Research Paper No. 2013 - 04

≪ 주제어: Key words ≫

디지털헬스케어기기, 빅데이터, 개인의료정보, 전자적 의무기록, 개인정보 보호법, 의료법
digital healthcare(or medical) equipment, big data, personal health information, electronic medical record, Personal Information Protection Act, Medical Service Act

Study on the Reasonable Regulation and Use of Personal Information on Digital Healthcare Environment

Kim, Soo Young, Kim,hyunkyung

The developments of ICT are anticipated as a solution to address the challenges of medical areas, such as medical treatment, preventive medicine. But now our country has been severely restricted in the "Medical Service Act" and "Personal Information Protection Act", with respect to the use of personal health information in its application for medical purposes, etc, therefore medical services using cloud computing and big data analysis are impossible. Already, leaders in the ICT sector such as Apple, Google and Samsung, pointed to digital healthcare industry as the next generation industry and has ventured a bold investment, however in Korea, the commercialization of these advanced digital healthcare services has been delayed. In this paper, we explore the regulatory Improvement of "personal health information" for the rational implementation of digital health care services.

Restrictions on the personal medical information based on the characteristics of the conventional health care settings are not proper and regulation of personal medical information that meets the new digital healthcare environment must be made. As the way, the paper proposed the following. ; First, the rational modification of the regulatory are needed for acceptance of new technologies such as cloud computing, etc. Second, the application range of the EMR system should be extended as to maximize the added value of personal health information. Third, the appropriate regulation and surveillance and monitoring system of healthcare apps and digital medical equipment that generates the personal health information were established so that the

public interest in the medical area to be compliant in order to ensure the accuracy and reliability of personal health information.