

의료산업과 AI, 마이 데이터 사업

미국의 의료데이터 시스템은 건강정보의 전자적 교환, 개인정보 보호 및 보안에 대한 국가표준을 설정하는 것을 목표로 1996년에 제정된 HIPAA (Health Insurance Portability and Accountability Act)를 시발로 미국 보건복지부(Department of Health and Human Services)가 제정한 관련 규칙들에 의해 주로 규율 되고 있지만 그 적용 범위가 '적격기관(Covered Entities)' 및 '업무위탁자(Business Associates)'에 한정되어 기술변화에서 발생하는 많은 관련 디지털데이터를 포괄하지 못하는 한계점등이 자주 비판받아 왔습니다. 2025년 3월 25일, EU는 EHDS (European Health Data Space) Regulation을 발효시킴으로써 개인의 디지털 건강데이터를 쉽게 통합관리, 활용할 수 있는 프레임을 통해 개인정보보호와 보안기준을 충족하면서 동시에 의료데이터 기반의 산업발전, 연구생태계 구축을 위한 장기비전을 내 놓았습니다.

EU의 '데이터를 위한 유럽 전략(European Strategy for Data)'의 핵심 이니셔티브 중 하나로, EU 전역의 건강 데이터 접근 및 활용 방식을 혁신하고자 출범했던 결실로 만들어진 것이 EHDS법이기 때문에 개인 건강관리는 물론이고 국가간 데이터의 연계와 연구활용을 목표로 디지털 헬스케어의 발전을 위한 데이터공유인프라 구축을 통해 미국과의 경쟁에서 유럽을 AI기반 의료혁신의 선두 주자로 만들겠다는 메가프로젝트라고 평가할 수 있습니다.

Related Areas

의료산업
마이데이터사업

Contact

구태언 변호사

T. 02-3477-8695

E. tekoo@law-lin.com

방석호 미국변호사

T. 02-3477-8695

E. shbang@law-lin.com

설기석 변호사

T. 02-3477-8695

E. ksseol@law-lin.com

반면, 전 국민의 예방접종정보를 관리하는 질병관리청, 건강검진, 진료내용 정보를 관리하는 국민건강보험공단, 그리고 투약이력정보를 관리하는 건강보험심사평가원이라는 중앙 공공기관 중심으로 거대한 개인의료정보를 단일 공공 데이터베이스화 하여 운영하고 있는 우리로서는 상대적으로 디지털의료산업의 선도적 발전과 혁신을 위한 데이터 인프라 구조는 세계에서 가장 잘 짜인 상태라고 할 수 있습니다. 사업 또한 2019년 12월에 4차산업혁명위원회가 '개인 주도형 의료데이터 이용활성화 전략'을 발표한 이래 개인정보보호법 개정 등의 준비작업을 거쳐 2025년 3월부터 My Healthway라고 불리는 마이데이터사업을 본격적으로 시행하고 있습니다.

특히 유럽의 EHDS법이 2027년 3월부터 진료목적의 데이터 1차적 사용, 2029년 3월부터 익명처리를 통한 연구 및 공공보건 목적의 데이터 2차적 사용, 그리고 유전자 등의 데이터 활용은 2031년 3월부터 적용되게 되는 등 단계별 접근을 취할 수밖에 없는 EU라는 구조적 한계를 드러내고 있다는 점에서 AI시대 의료데이터분야에서는 우리만의 제도적 장점을 더욱 극대화하여 경쟁력을 키울 상황이 전개되고 있습니다. 예를 들면, EU는 국가별 건강데이터의 접근기관설립에 따른 분산된 집행체제, 전자건강기록 (Electronic Health Record: EHR) 시스템의 인증메카니즘 구축, MyHealth@EU라는 국가간 인프라 구축, 더 나아가 국가간 의료데이터의 교환시스템 등의 과제를 극복하여야만 되는 반면, 우리의 My Healthway는 공공의료데이터베이스를 기반으로 IT기업, 보험회사 등 의료데이터사업을 원하는 비의료기업들에게도 일단 문호를 열고 데이터를 관리, 처리할 수 있는 특수전담사업자 선정을 현재 진행하고 있습니다.

법규 또한 의료기기분야로 국한하여 볼 때, EU는 2024년에 AI법, MDR (Medical Device Regulation) 제정 등을 통해 AI확산에 따른 대응을 하고 있지만, 우리는 2024년에 제정된 이후 1년여의 준비기간을 거쳐 2025년 2월부터 시행되고 있는 디지털의료제품법, 그리고 식품의약품안전처가 2025년 1월에 '생성형 인공지능 의료기기 허가, 심사 가이드라인'을 내놓는 등 적극적으로 움직이고 있습니다.

이하에서는 AI시대 EHDS법, 우리의 My Healthway 등 의료데이터 활용을 둘러싼 최근의 주요 움직임과 법 이슈들을 살펴보고자 합니다.

1. AI법과 EHDS법의 관계

EHDS법은 데이터의 2차 활용 시 주로 과학적 연구 및 혁신의 맥락에서, 알고리즘 및 AI 시스템의 훈련, 테스트, 평가를 위한 건강 데이터 활용을 명시적으로 허용하고 있습니다. 구체적으로 EHDS법은 2차 활용이 허용되는 목적 중 하나로 "의료기기, 체외진단 의료기기, AI 시스템, 디지털 건강 애플리케이션을 포함한 알고리즘의 훈련, 테스트 및 평가"를 포함함으로써 EHDS법을 통해 AI 개발을 촉진하려는 의도를 잘 보여주고 있으며 의료분야와 같은 '고위험' AI시스템 활용분야에서의 단일 시장 조성을 지원하게 됩니다.

다만 EHDS법은 의료데이터 접근을 위한 인프라와 감독, 관리체제를 규정하고 있는 반면, EU AI법은 해당 데이터를 사용하여 개발된 AI 시스템을 규제하면서 안전성, 신뢰성 확보 및 기본권 준수 등의 상호 역할 분담을 하고 있습니다.

구체적으로 EHDS법 자체는 의료데이터를 활용하여 개발되는 AI 시스템에 대한 기술표준이나 요구사항을 부과하지 않으며, 의료데이터의 접근 및 활용을 규제하는 데 초점을 맞추고 있습니다. 다시 말해, 의료분야에서의 AI 시스템에 대한 규제, 구체적으로 의료분야 '고위험' AI시스템의 설계, 개발, 배포 등은 AI법 및 의료기기법 (MDR/IVDR)의 영역으로 넘어가게 되며, EHDS법에 규정된 의료데이터 보호 및 보안 규정 등은 의료 AI시스템 개발목적으로 데이터를 활용하는 경우에도 동일하게 적용되면서 결과적으로는 간접 규율을 하게 됩니다. 예를 들면, 의료데이터의 2차 활용 시 AI 훈련 데이터셋은 규제기구가 승인한 데이터 허가서상 명시된 특정 목적 달성에 필요한 범위로 한정되어야만 하는 식입니다.

또한 AI시스템의 개발, 활용에서 EHDS법이 AI 시스템의 훈련, 검증, 테스트에 필요한 고품질 데이터 제공을 담보할 수 있는 데이터 소스로서 기능한다는 사실은 우리에게도 중요한 시사점을 제공합니다. 2026년 1월부터 시행되어질 우리의 인공지능기본법도 '고영향 인공지능'이 활용되는 의료분야 영역에 보건의료기본법, 의료기기법, 디지털의료제품법을 열거하고는 있지만 정작 AI의 훈련, 테스트, 검증 등에 필요한 데이터가 편향적이지 않고 법적으로도 문제가 없는지 등의 여부는 아직까지 사업자 자율규제의 영역에 맡겨져 있기 때문입니다.

2. EHDS법의 주요 규정들

2-1. 개인전자건강데이터와 GDPR

EHDS법은 전문에서 '개인전자 건강데이터' (personal electronic health data)의 종류, 수집, 처리방법 등을 불문하고 EU 개인정보보호법 (GDPR)상의 원칙들이 EHDS법에서도 준수되어야 함을 밝히고 있습니다. 즉 EHDS법은 GDPR을 대체하거나 수정하는 것이 아니라 GDPR의 원칙과 권리를 기반으로 건강 데이터라는 특정 영역에 대한 구체적인 규칙과 추가적인 보호 장치를 마련하는 방식으로 작동하고 있습니다.

전자적 형태로 처리된 건강과 유전자 (genetic)데이터를 통칭하는 '개인전자건강데이터' 개념은 제14조에서 환자요약, 전자처방전, 전자조제, 의료 영상검사 및 관련 영상보고서, 의학검사결과 (임상병리 및 기타 진단 결과와 관련 보고서 포함), 퇴원요약정보의 6종을 최우선적으로 추려 '헬스케어 제공목적' (primary use)에 대해서 먼저 사용되어 짐을 천명하고 있습니다. 이 과정에서 자신의 우선순위 개인전자건강데이터에 접근하고 다운로드할 수 있는 권리 (제3조), 환자 스스로 자신의 건강기록에 추가적인 정보를 제공하여 의료 맥락을 풍부하게 할 수 있도록 보장하는 권리 (제5조), 자연인이 자신의 '개인전자건강데이터'를 정정하도록 요청할 수 있는 권리 (제6조)를 명시하고, 제7조는 자연인이 자신의 '개인전자건강데이터'를 다른 의료 제공자에게 이동시키거나 접근 권한을 부여할 수 있는 권리 등을 규정하고 있습니다.

한편, 익명화된 건강정보는 2029년 3월부터 '2차 사용' (secondary use) 용도로 활용되게 되며 제51조는 의료기기에서 수집되는 건강데이터, 인간 유전체정보 등을 포함한 17개 전자건강정보를 명시하고 있고 데이터 이용을 거부할 수 있는 권리 (opt-out) 또한 지켜지고 (제71조) 있습니다. 또한 EHDS법은 의료현장에서 개인 디지털 의료데이터를 수집, 효율적으로 활용하고자 하는 분명한 목적을 갖고 있기 때문에 GDPR상의 개인정보보호를 위한 권리들을 목적에 맞게 다소 수정, 변경하고 있음도 주목할 필요가 있습니다.

예를 들면, 데이터 접근권은 서면이나 스캔 문서 형태로 구체화되는 경우도 많아 실제 현재 병원진료에서 요구되는 전자적 접근방법과 즉답의 필요성과는 거리가 멀기에 EHDS법 제8조의 "접근제한권리"는 의료 분야에 특화되어 의료 전문가의 전자건강데이터 접근을 직접적으로 제한할 수 있도록 명시하고 있고, 제9조는 "Right to obtain information on accessing data"로서 '개인전자건강데이터'에 대한 접근 정보를 얻을 권리에 관한 내용으로 GDPR의 상응 개념을 수정하였습니다. 즉 제9조는 의료 환경에서 의료 전문가가 '개인전자건강데이터'에 접근한 모든 사례에 대한 정보를 자동 알림을 포함하여 얻을 권리를 명시하고, 접근한 의료 제공자 또는 개인, 접근 날짜 및 시간, 접근한 '개인전자건강데이터'의 종류와 같은 상세 정보를 무료로, 또한 지체 없이 제공하고, 최소 3년간 보관하도록 규정함으로써 디지털 진료현장에 맞도록 맞춤형으로 수정하는 식입니다.

2.2. 데이터보유자와 데이터사용자

법상 개인정보보호의 대상이 되는 개인의료데이터는 물론이고 익명화 되어 2차적 사용용으로 처리된 건강데이터를 보유하고 있는 '건강데이터보유자' (health data holder)는 의료분야의 법인, 공공기관, 연구소는 물론이고 건강 관련 제품이나 서비스를 개발하거나 건강 관련 제품을 제조하는 기업도 포함한 광의의 개념입니다. 이런 '건강데이터보유자'는 단순한 치료목적을 넘어 공중보건, 직업건강, 통계, 교육, 연구, 정책결정 등의 2차적 사용목적에 가지고 데이터접근을 요청한 자연인 또는 법인을 의미하는 '데이터사용자' (health data user)와 데이터를 공유하고 정보를 제공할 의무를 부담케 함으로써 EHDS법에 담긴 EU 데이터전략의 핵심 역할을 수행하고 있습니다.

그러나 2차적 목적으로 개인의료데이터를 사용하고자 하는 경우 환자는 이를 거부할 권리 (opt-out)를 가지며, '건강데이터보유자'는 환자가 opt-out하지 않는 한, 접근이 승인된 데이터를 공유해야 할 의무가 있습니다. 또한 공중 보건 또는 직업보건 분야의 공익, 정책결정, 통계, 교육, 과학연구 등의 허용된 목적을 벗어나 보험회사에 의한 보험료 산정이나 상업적 광고, 제3자에 대한 데이터 판매와 같은 2차적 사용목적은 공공의 신뢰를 확보하기 위해 금지되어 지게끔 (제54조)했습니다.

2-3. 기타

EHDS법은 의료데이터가 지식재산권, 영업비밀 또는 데이터 보호의 대상일 수 있음을 전제로 데이터보유자는 이러한 보호조치에 대해 각국 정부가 데이터의 2차적 사용을 처리, 책임지도록 신설하도록 한 '건강데이터접근기구' (Health Data Access Bodies, HDABs)에게 알리도록 하고 있습니다.

즉 2차 활용을 위한 새로운 거버넌스 구조로 EHDS법이 신설토록 한 것이 HDABs이며, 2차 활용 목적의 건강 데이터 접근 요청을 평가하고, 접근허가를 발급하며, 데이터 활용의 적법성 및 규정준수 여부를 감독하는 핵심 기관인 셈입니다. HDABs는 구체적으로 요청된 데이터의 접근 형식(익명화 또는 가명화)을 결정하고, 지식재산권 및 영업비밀 보호 조치를 관리하게 됩니다. 특히 임상시험 데이터에 대해서는 지식재산권과 영업비밀 보호를 위해 모든 필요한 조치를 취하면서 가능한 범위 내에서 데이터를 제공하도록 EHDS법은 규제하고 있습니다.

한편, 이런 활동들을 뒷받침할 수행할 도구인 표준화된 '전자건강기록' (EHR) 시스템을 EU회원국과 EHR 시스템제조사가 구축하도록 하되, 모든 EHR 시스템이 유럽 전자건강기록교환형식 (European Electronic Health Record exchange Format, EEHRxF)을 준수하도록 하여 EU 전역에서 상호운용성을 보장되고 이를 통해 현재 회원국 간 EHR 시스템의 상이함으로 인해 발생하는 국경 간 데이터 공유장벽을 해결하려 하고 있습니다.

EHDS법은 의료데이터의 1차 활용과 EHR 시스템의 관리는 각국의 디지털건강기구 (Digital Health Authorities)가 하도록 하고 있고 각국의 디지털 건강기구는 회원국이 설립한 접근 지점 (access points)을 연결하는 국경 간 디지털 인프라 (MyHealth@EU)를 의무 구축하여 환자가 데이터를 공유할 수 있도록 추가 규정하고 있습니다..

3. My Healthway

3-1. 개요

My Healthway사업은 우리 정부 주도로 추진되는 개인의료정보 플랫폼 접근 방식으로서 개인이 여러 기관에 흩어진 자신의 건강정보를 통합 조회하고, 동의 하에 원하는 곳에 전송하여 활용 (주로 1차 활용)하도록 지원하는 것을 핵심 목표로 삼고 있기 때문에 개인의 데이터 자기결정권 강화에 중점을 두고, 플랫폼을 통한 데이터 이동, 활용은 철저히 개인의 동의 (opt-in)에 기반하고 있습니다. 따라서 2차 활용에 대한 구체적인 정책 등은 EU의 EHDS법에 비해 아직 최종 확정되지 못한 단계라고 할 수 있고, 데이터 표준화 및 참여자간 신뢰 구축 등도 중요한 과제로 남아 있습니다.

법적으로 현재의 의료법은 의료기관 상호간에만 의료데이터의 전송을 허용하고 있기 때문에 결국 개인이 자신의 건강정보 (마이 데이터)를 한곳에 모이게 하고 원하는 대상에게 데이터를 제공하고, 또한 이를 직접 활용토록 하기 위해서는 개인정보보호법 개정을 통한 정보 주체의 전송요구권을 통할 수밖에 없습니다. 그러나 My Healthway는 개인 진료를 주된 목적으로 만들어진 건강정보고속도로 구상이기 때문에 1차 진료기관인 병원이 자신들의 EHR시스템상의 의료정보를 쉽게 내놓으려 하지 않는 경우에 해결책을 어떻게 할 것인지의 문제는 2차적 사용을 위한 사업설계시 반드시 풀어야 될 숙제입니다.

특히 우리 저작권법은 “데이터베이스의 개별 소재 또는 그 상당한 부분에 이르지 못하는 부분의 복제등이라 하더라도 반복적이거나 특정한 목적을 위하여 체계적으로 함으로써 해당 데이터베이스의 일반적인 이용과 충돌하거나 데이터베이스제작자의 이익을 부당하게 해치는 경우에는 해당 데이터베이스의 상당한 부분의 복제된 것으로 본다”는 규정 (제93조 2항)을 통해 의료기관이 EHR시스템에 투자한 재산권을 확실히 보장해주고 있기 때문에 정보주체의 제3자 전송요구권 행사에 따라 해당 정보의 제공을 정보수신자가 합법적으로 요구하더라도 의료기관이 이를 거부할 권리가 있다고 다룰 수 있는 법적 여지가 있습니다.

현재 시범사업은 유료로 병원이 제공하는 의무기록, 진료비세부내역과 같은 사항은 제외하고 제3자에게 요구받은 데이터를 제공하도록 진행하고 있습니다.

한편, 처리, 전송되는 데이터는 현재 공공건강데이터, 병원의료데이터, 개인건강데이터의 유형별로 플랫폼을 통해 수집하되, 제공기관별 다양한 건강정보를 개인을 중심으로 통합하고, 상호 호환이 가능하도록 보건복지부 산하 한국보건의료정보원에서 데이터 표준화를 수행하게 하고 있습니다.

3-2. 운영구조

My Healthway는 개인정보보호법상 환자본인의 전송요구권에 기초하여 의료마이데이터 구상이 구체화되었기에 전송요구권을 행사할 주체를 중심으로 정보전송자와 정보수신자, 그리고 이들을 매개하는 중계전문기관으로 짜이는 구조입니다.

의료분야의 정보전송자는 질병관리청, 국민건강보험공단, 건강보험심사평가원, 그리고 의료법상 상급종합병원 4곳이고 상급종합병원은 환자정보, 내원정보, 진단정보, 약물처방정보, 수술 및 처치내역, 진단검사, 기타검사, 알레르기 및 불내성, 영리검사, 병리검사의 8종류 세부정보항목을 담당합니다. 정보수신자는 일반수신자, 일반전문기관, 특수전문기관으로 세분되는데 의료분야에서 특수전문기관은 가톨릭중앙의료원, 룰루메딕, 카카오헬스케어가 각각 맞춤형 만성질환 예방관리서비스, 해외체류시 국내 의료기록 연동서비스, 약물비서서비스를 현재 시범사업으로 수행하고 있습니다.

한편, 정보수신자는 개인정보보호법상 본인에게 직접 전송할 것을 요청하는 본인 전송요구권외에 제3자에게 요구할 수 있는 전송요구권 (제35조의 2 제2항)이 만들어짐에 따라 탄생되어진 개념으로서 정보주체의 요구에 따라 정보전송자로부터 중계전문기관을 경유, 안전하게 받은 의료정보를 개인맞춤형 서비스로 제공하는 역할을 하게 됩니다. 이 과정에서 정보주체의 제3자 전송요구권에 기해 정보전송자와 정보수신자간의 안전한 중계역할을 수행하도록 만들어진 '중계전문기관'은 의료개인정보의 안전성과 신뢰성이 보장되도록 데이터의 표준화, 인증식별 등의 처리를 담당합니다.

또한 정보주체가 제3자 전송요구권을 행사하려면 개인정보보호법 시행령상 전송 요구목적, 전송 요구를 받는 자, 개인정보를 전송받는 자, 전송을 요구하는 개인정보, 정기적 전송을 요구하는지 여부 및 요구하는 경우 그 주기, 전송 요구의 종료시점, 전송을 요구하는 개인정보의 보유 및 이용기간의 7가지를 특정 (제42조의 5)해서 엄격하게 행사하도록 규정되어 있기 때문에 이를 중계전문기관이 도와줄 수 있도록 그 역할이 추가로 부여되어 있습니다.

4. 시사점

EHDS법은 AI시대 의료데이터 접근을 위한 인프라와 거버넌스를 제공하는 역할을 담당하고는 있지만 고위험 영역인 의료분야에서의 대표성 있는 데이터를 만들어내는 것에 초점이 있지는 않습니다. 따라서 의료분야 AI시스템 개발자는 의료데이터를 활용하면서 AI법에 따라 고품질의 데이터를 제공, 확보하여야 하는 궁극적 책임을 지게 되며 우리의 인공지능기본법, 의료관련법도 같은 입장을 취하고 있습니다.

우리는 2019년 제4차 산업혁명위원회에서 '개인 주도형 의료데이터 이용활성화 전략'을 발표한 이래 사업의 구체적 결실인 My Healthway가 지금 시범 실시되고는 있지만 주로 데이터의 1차 사용, 즉 개인이 자신의 건강관리를 위해 의료기관의 데이터를 활용하는 데 초점을 맞추고 있기 때문에 신약개발 등의 R&D는 물론이고 시장개척 등의 2차적 활용을 둘러싸고 다음과 같은 해결과제도 드러나고 있습니다.

첫째로는 개인동의기반 (opt-in방식)의 의료데이터 활용 생태계를 중앙 집중적 방식으로 구축하겠다는 구상이 My Healthway 사업 바탕에 깔려 있기 때문에 데이터의 공유결정 자체에서부터 환자의 동의가 필요한 것으로 셋팅이 될 수밖에 없었고 결과적으로는 의료데이터의 활용을 둘러싼 잠재력을 극대화, 산업화하는 측면보다는 의료데이터의 이동을 중심으로 '통제가능한 범위내에서' 설계, 운영되고 있다고 평가할 수 있습니다.

결과적으로는 디지털 의료에서의 사회적 이익확보와 공공의료체계의 개선목표에 집중되어진다는 점에서는 장점도 있을 수 있지만 EHDS법이 2차적 활용 시 개인의 명시적 활용거부권 (opt-out)을 부여하는 것과 대조적으로 우리는 2차적 활용 시 추가로 개인의 명시적 동의 (opt-in)를 잘 받아낼 수 있을지를 또 고민하여야만 하는 숙제를 안고 있습니다.

둘째로는 더욱이 정보주체가 의료데이터에 대한 제3자 전송요구권을 행사할 경우 My Healthway 성공의 키를 쥐고 있는 의료기관에 대해 해당 데이터 제공을 강제할 법 규정이 전혀 없고 오히려 의료기관이 저작권법상의 데이터베이스 제작자의 권리를 합법적으로 주장하면서 거부도 할 수 있는 구조이기 때문에 법적 보완작업이 불가피해 보입니다. 즉 의료데이터의 2차 활용을 위한 '데이터접근'에서부터 정보수신자는 데이터보유자의 저항에 부딪칠 수 있고, AI가 제대로 활용되기 위한 필수전제조건인 고품질의 데이터를 어떻게 확보하여 산업화 시킬 것인지의 다음 난제 또한 큰 숙제로 남아 있습니다.

미국 법무부 (DOJ)는 2025년 4월 8일부터 시행되는 규칙 (rule)에서 미국인의 유전자, 의료정보가 중국에 이전되지 못하도록 규제함으로써 AI를 기반으로 빠른 속도로 발전하고 있는 중국 의료기기산업을 견제하기 시작하는 등 AI 의료분야에서의 전운도 더 짙어지고 있습니다.

매월 발간하는 법무법인 린 AI산업센터의 뉴스레터인 AID 내용에 대한 질문이나 조언 등은
 구독인 TMT 전문그룹장 (tekoo@law-lin.com), 방석호 AI산업센터장 (shbang@law-lin.com),
 설기석 구성원 변호사 (ksseol@law-lin.com)에게 보내주십시오.