아태연구 제31권 제1호 (2024) https://doi.org/10.18107/japs.2024.31.1.003

HIPAA 위반 사례를 통한 미국의 건강정보 정책에 관한 법적 연구

이한주*

| 목 차 |

| 논문요약 |

건강정보가 외부로 유출되면, 정보주체의 사생활의 비밀과 자유가 침해되고, 보험·근로 관계에서 불이익을 받거나 사회적 낙인이 찍혀 정상적인 사회생활을 하기 어려운 상황이 되는 등 심각한 문제를 가져올 수 있다. 그런 점에서 건강정보의 활용만큼 보호도 필요하고, 건강정보를 보호하기 위한 다양한 대책을 마련해야 한다.

미국은 1996년 '건강보험 이전 및 책임에 관한 법률(HIPAA)'의 제정으로 직원이 직장 간 의료 보장을 유지하고 기존 질환으로 인해 차별받지 않도록 하고 있다. 이는 단순히 보험의 문제에 국한되는 것이 아니라 건강보험에 기록된 다양한 건강정보의 처리와 관련해서 발생할 수 있는 다양한 문제를 해결하기 위해서 도입되었다. 미국은 건강정보의 보호 또는 활용에 대한 기준을 명확하게 제시하고 있지는 않다. 다만, 건강정보를 규제하는 방향으로 규정하고 있는 것은 아니므로 원칙적으로 활용할 수 있는 것으로 해석할 수 있고, 규정을 위반한 때에는 그에 상응하여 엄격하게 책임을 묻는다는 점에서 우리의 법체계와는 다르다.

본 논문에서는 미국 보건복지부(HHS) 산하 인권국(OCR)에서 HIPAA를 위반한 것으로 판단한 최근의 사례를 살펴보려 한다. 이를 통해서 우리나라에서도 건강정보를 포함한 개인정보보호법제가 실효적으로 보장받을 방안을 제안해 보고자 한다.

* 한국의료법학연구소 책임연구원

▪ 주제어: 건강정보, 전자건강기록, 의료행위, 건강보험 이전 및 책임에 관한 법률, 의료 빅데이터

Ⅰ. 서론

AI(인공지능), Big Data(빅데이터), IoT(사물인터넷), Cloud Computing(클라우드 컴퓨팅), 3D Printing(3D 프린팅), Precision Medicine(정밀의료), Gene Scissor(유전자가위) 등 최근 언론을 통해 많이 언급되는 보건의료 분야의 최첨단 정보통신기술은 지금까지도 눈부신 성과를 가져왔지만, 우리 인간이 지금까지 도달하지 못했던 새로운 영역을 정복하려는 꿈을 현실로 만들 수 있을 것으로 기대한다. 물론 이런 긍정적인 평가와 함께 우리가 전혀 예상하지 못한 새로운 문제가 발생할 것이라는 우려도 함께 있다. 특히 다양한 기술을 구현하기 위해서는 기본적으로 개인(환자)의 건강정보를 활용할 수 있도록 하는 것이 전제되어야 한다. 그러나 개인정보, 그중에서도 건강정보는 '민감정보'에 해당하여 일반 개인정보와 비교해서 특별히 보호받아야 하는 것으로 인식된다.

만약 건강정보가 외부로 유출되면, 정보주체의 사생활의 비밀과 자유가 침해되고, 보험·근로 관계에서 불이익을 받거나 사회적 낙인이 찍혀 정상적인 사회생활을 하기 어려운 상황이 되는 등 심각한 문제를 가져올 수 있다. 그런 점에서, 건강정보의 활용만큼 보호도 필요하고, 건강정보를 보호하기 위한 다양한 대책을 마련해야 한다.

물론 건강정보의 보호를 우선하는 정책을 실행하게 되면, 정보 유출의 문제는 그만큼 줄어들 수 있다. 그러나 정보의 보호범위가 넓어지게 되면, 이와 반대로 정보를 활용할 수 있는 범위는 줄어들게 되고, 위에서 언급한 보건의료 분야의 발전은 앞으로 먼 미래의 희망 사항에 불과하게 될 수 있다. 그러므로, 건강정보의 보호와 활용을 위해서 적절한 방안을 찾아내는 것이 무엇보다 중요하다.

미국은 1996년 '건강보험 이전 및 책임에 관한 법률(Health Insurance

Portability and Accountability Act of 1996: 이하 'HIPAA')'의 제정으로 건강보험에 기록된 다양한 건강정보의 처리와 관련해서 발생할 수 있는 다양한 문제를 해결할 수 있게 되었다. HIPAA 제정 이후 3년 동안 의회에서 구체적인 기준을 마련하지 못해서 프라이버시 보호와 관련하여 보건부(Department of Health and Human Services: 이하 'HHS')에 의한 규칙제정으로 위임되었고, HHS는 2000년 12월 28일 프라이버시규칙(HIPAA Privacy Rule)을 공표하였으며, 이 내용을 2001년 4월 13일 확정하여 2003년 4월 14일부터 시행하게 되었다.

그리고 2009년 의료보험개혁법이 제정된 이후에, 전자의무기록(EMR) 도입을 활성화하고 연구목적으로 건강정보의 교류를 활성화하기 위해 경제 및 임상건강을 위한 건강정보기술법(Health Information Technology for Economic and Clinical Health Act: 이하 'HITECH')이 도입되었다(김재선 2021, 120).

본 논문에서는 건강정보에 대해 규정하고 있는 HIPAA, HIPAA Privacy Rule, HITECH에 대해서 개관하고, 미국 HHS 산하 인권국(Office for Civil Rights: 이하 'OCR')에서 HIPAA를 위반한 것으로 판단한 최근의 사례를 살펴보려 한다. 이를 통해서 우리나라에서 건강정보를 포함한 개인정보보호법제가 실효적으로 보장받을 방안을 제안해 보고자 한다.

Ⅱ. 미국의 건강정보 관련 법제와 구축현황

1. 건강정보 관련 법제

(1) 건강보험의 이전과 책임에 관한 법률(HIPAA)

① 개요

미국은 HIPAA의 제정으로 직원이 직장 간 의료 보장을 유지하고 기존 질환으로 인해 차별받지 않도록 하고 있다. 이는 단순히 보험의 문제에 한정되는 것이 아니고, 건강보험에 기록된 다양한 건강정보의 처리 과정에서

생길 수 있는 여러 문제를 해결하기 위해서 도입되었다. 이 법은 각 지역(주)에서 경계를 넘어 다른 지역(주)으로 정보를 이전하기 위해서 해당 건강정보를 생성·관리·전송 등의 처리시스템이 규격화되어야 한다는 것이 핵심이다. 결국 이러한 처리시스템을 통해서 미국 전역의 각 의료기관에서 보유하고 있던 건강정보를 규격화된 전산망으로 관리할 수 있도록 하여 건강보험의 사기 또는 남용을 방지하고 의료사무를 간소화할 수 있게 되었다.

미국은 건강정보의 보호 또는 활용에 대한 기준을 명확하게 제시하고 있지는 않다. 다만, 건강정보를 규제하는 방향으로 규정하는 것은 아니므로 원칙적으로 건강정보를 활용할 수 있는 것으로 해석할 수 있고, 해당 규정을 위반한 때에는 그에 상응하여 엄격한 책임을 묻고 있어서, 이는 우리 법체계와 다르다.

② 주요 내용

HIPAA는 5개의 편(Title)으로 구분되었는데, 그중에서 건강정보와 관련된 것은 제2편의 의료사무 간소화(Administrative Simplification)에 포함된 US Code Title 42의 §1320d~§1320d-8의 총 9개 조문이다.

§1320d는 정의규정으로, 보험정보 표준기관(Health care clearinghouse), 의료기관(Health care provider), 건강정보(Health information), 보험회사(Health plan), 개인식별건강정보(Individually identifiable health information), 기준(Standard), 기준설립조직(Standard setting organization)에 관해 규정하고 있다.

특히 건강정보는, 1) 의료기관, 보험회사, 공공의료기관, 고용인, 생명보험회사, 초중등학교 또는 대학, 또는 보험정보 표준기관에 의해 생성되거나 수집된 것,[1] 2) 개인의 과거·현재 또는 미래의 육체적·정신적 건강 또는 상태, 개인에 대한 진료 제공, 또는 과거·현재 또는 미래의 진료 제공에 관한 비용 지급과 관계된,[2] 어떠한 형태나 매체인지 상관없이 구술되거나 기록된 모든

1) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
2) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or

정보를 말한다.

건강정보 중에서 보호건강정보(protected health information: 이하 'PHI')가 있는데, PHI에는 18개 정도의 식별자(identifiers)가 있어서,[3] 법 체계적으로 HIPAA는 건강정보 정의 부분에서 건강정보의 범위와 개인식별건강정보로 정의하고, PHI는 건강정보 중에서 개인식별이 가능한 건강정보로 정의하고 있는 것으로 볼 수 있다(김재선 2021, 128). HIPPA에서는 건강정보를 치료목적 여부에 따라서 구분하고, 치료목적이 없는 경우의 PHI는 별도로 규정하고 있다. 원칙적으로 건강정보의 수정, 치료목적 외의 활용이나 유출은 금지된다. 그러나 보험료율을 책정하거나 학술연구 등의 공익적 필요가 있는 때에는 정보를 예외적으로 활용할 수 있다.[4]

그리고, 건강정보를 처리하려는 의료기관은 반드시 보건부 장관이 정하는 기준을 준수하도록 규정하고 있는데(§1320-d), 보험회사는 건강정보처리기준을 준수한 의료기관의 처리를 거절해서는 안 되고, 보험회사도 그러한 기준에 관한 처리를 지연시켜서는 안 되며, 건강정보의 처리를 위한 취급정보와 수집정보는 건강정보의 데이터 구성요소 기준에 따라야 한다. 그리고 보험정보 표준기관들이 정보처리의 절차와 내용을 정보처리기준에 부합하도록 해야 할 기한을 24개월로 하고, 예외적으로 소규모 의료기관은 36개월로 완화했다(§1320d-4 (b)(1)).[5]

한편, 그 기준을 위반한 때에는 엄격하게 처벌하도록 했는데(§1320d-6), 악의적으로 정보를 공개하는 유형으로, 특이한 건강이상자의 자료 활용, 개인을 식별할 수 있는 건강정보의 수집, 개인을 식별할 수 있는 건강정보의

---

future payment for the provision of health care to an individual.

3) 이름, 지역, 날짜, 전화번호, 사회보장번호, 의료기록 번호, 건강보험번호, 모든 사진과 관련 정보, 자동차, 은행 계좌 등.

4) 42 C.F.R. § 495.; 45 C.F.R. § 170.

5) (A) In general
Not later than 24 months after the date on which an initial standard or implementation specification is adopted or established under sections 1320d‐1 and 1320d‐2 of this title, each person to whom the standard or implementation specification applies shall comply with the standard or specification.
(B) Special rule for small health plans
In the case of a small health plan, paragraph (1) shall be applied by substituting "36 months" for "24 months". For purposes of this subsection, the Secretary shall determine the plans that qualify as small health plans.

제3자 제공으로 규정하고, 1) 단순 수집 등을 한 때에는 $50,000 이하의 벌금, 1년 이하 징역, 또는 양 형벌 병과, 2) 부당한 방법으로 수집 등을 한 때에는 $100,000 이하의 벌금, 5년 이하 징역, 또는 양 형벌 병과, 3) 수집된 정보의 판매 등으로 금전적 이익을 취득한 때에는 $250,000 이하 벌금, 10년 이하 징역, 또는 양 형벌 병과에 처할 수 있도록 했다(§1320d-6 (b))(이한주 2012, 152-154).[6]

(2) HIPAA 규칙

1996년 HIPAA 제정 이후 1999년 8월까지 의회에서 구체적인 기준을 마련하지 못해서 프라이버시 보호와 관련하여 보건부에서 규칙을 제정하도록 위임되었다. 이에 따라 보건부는 클린턴 행정부 말기인 2000년 12월 28일 프라이버시규칙(HIPAA Privacy Rule)을 공표하였고,[7] 부시 행정부에서 이 내용을 2001년 4월 13일 확정하여 2년의 준비기간(작은 의료기관은 3년)을 인정하여 2003년 4월 14일부터 시행하게 되었다. 이 규칙으로 의료기관, 학교 등 건강정보를 관리하는 전국 단위의 기관을 대상으로 한 프라이버시 보호와 관련된 법체계가 확립되었다고 할 수 있다(이한주 2012, 152-155).

이 규칙은 적용대상 기관에 의해 보호되는 개인의 건강정보 사용과 공개에 대해서 규율한다. 이 규칙의 주요 목적은 건강정보를 적절하게 보호하면서 동시에 높은 수준의 의료 서비스를 제공하여 환자의 생명과 건강을 보호하는 데 필요한 건강정보를 제공 및 활용할 수 있도록 하는 것이다. 이 보호

---

6) (b) Penalties
A person described in subsection (a) of this section shall－
(1) be fined not more than $50,000, imprisoned not more than 1 year, or both;
(2) if the offense is committed under false pretenses, be fined not more than $100,000, imprisoned not more than 5 years, or both; and
(3) if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than 10 years, or both.

7) 이는 연방 보건복지부에 의해 만들어진 'the Standards for Privacy of Individually Identifiable Health Information'으로 약칭하여 HIPAA 프라이버시규칙(HIPAA Privacy Rule)으로 불리기도 한다(65 Fed. Reg. 82462, 82463(Dec. 28, 2000)). 이 규칙은 45 CFR Part 160 and Subparts A and E of Part 164에 위치하게 되었다.

규칙은 건강정보가 상업적인 목적으로 활용되는 것을 허용하면서, 다른 한 편으로 환자의 건강정보를 엄격하게 보호하고 있다.

HHS는 건강정보 보호를 위하여 2003년에 HIPAA 보안규칙(HIPAA Security Rule)을 마련했다. 이 규칙은 전자적으로 보관 또는 전송되는 특정 건강정보를 보호하기 위하여 국가 보안 표준세트를 설정하려는 목적으로 제정되었다. 이 보안규칙은 개인의 전자적 보호건강정보(e-PHI)를 보호하기 위해서 해당 기관이 구비해야 하는 기술적 및 비기술적 보호 장치를 해결하여 HIPAA 보호규칙 상의 정보보호 기능을 규율한다(전한덕 2022, 84).

(3) HITECH

① 개요

2009년에 개정된 건강보험개혁법(Patient Protection and Affordable Care Act)은 의료비 증가의 문제를 해결하고 기술혁신을 통해서 비용을 절감하기 위해서, 의료기록의 표준화 및 활용, 복제 의약품 지원 등을 제안했다. 이에 따라 같은 해에 HITECH가 제정되었다. 이 법은 의료진이 환자의 진료(건강)정보를 공유하여서 비용을 절감하고 의료행위의 효율성을 증진하는 것을 목적으로 하고, 의료기관 간에 전자의무기록(EMR)을 공유하며, 이를 통한 건강보험의 가입 촉진, 연방정부의 기금 지원 등을 구체적 방안으로 제안하였다(김재선 2016, 279).

HIPPA와 마찬가지로 HITEC에서 환자의 건강정보는, 식별할 수 있는 건강정보(Identified Health Information: IHI), 비식별 건강정보(De-identified Health Information: DHI), 제한된 데이터 세트(Limited Data Sets: LDS)로 구분하고 있다. 식별할 수 있는 건강정보는 엄격하게 보호되지만, 비식별 건강정보와 제한된 데이터 세트는 일정한 조건을 충족하면 활용할 수 있다. HITECH는 HHS에 보건정보기술조정국(Office of the National Coordinator for Health Information Technology's: 이하 'ONC')를 설치할 수 있도록 규정하였고, ONC에게 전자건강기록(EHR)과 개인 건강정보를 안전하게 공유할 수 있도록 하여 건강관리의 증진을 위한 프로그램을 운영할 수 있도록

권한을 부여했다(전한덕 2022, 85-86).

② HIPAA 위반에 대한 처벌 강화

HITECH가 도입되기 전에는 해당 기관이 HIPAA를 위반했다는 사실을 몰랐다고 주장하고 해당 기관이 인지하고 있다는 것을 입증하지 못한다면, HHS 산하 OCR이 해당 기관에 부과할 수 있는 벌금은 위반 시마다 $100, 최대 벌금 $25,000 정도로 대단히 적었다.

그러나, HITECH 제정 이후 HIPAA 위반에 대해서 엄격한 처벌이 도입되었고, 처벌은 다양한 과실 수준(유형)에 따라 여러 단계로 세분되었다. HIPAA 위반에 대한 최대 연간 벌금 한도는 150만 달러로 늘어났고, 2016년부터 HIPAA 위반 벌금은 인플레이션을 고려하여 매년 조정되어서, 2023년 12월을 기준으로 최대 연간 벌금은 $2,067,813이다.

<표 1> HIPAA 위반 처벌[8)]

과실 수준 (Level of Culpability)	위반 유형별 최소 처벌 (Minimum Penalty per Violation Type)	위반 유형별 최대 처벌 (Maximum Penalty per Violation Type)	연간 벌금 한도 (Annual Penalty Limit)
지식부족 (Lack of Knowledge)	$137	$34,464	$34,464
감독부족 (Lack of Oversight)	$1,379	$68,928	$137,886
고의적인 방치 (Willful Neglect)	$13,785	$68,928	$344,638
고의적 방치가 30일 이내 시정되지 않음 (Willful Neglect not Corrected within 30 days)	$68,928	$68,928	$2,067,813

HIPAA 위반에 대해 부과되는 벌금은 미국 재무부(Department of the Treasury)에 직접 전달되고, HITECH 시행 이후 강화된 집행 조치로 HHS

8) The HIPAA JOURNAL, https://www.hipaajournal.com/what-is-a-hipaa-violation/. (2024년 2월 18일 검색)

는 의회에 예산 증액을 요청할 수 있게 되었다. 더 많은 예산을 활용하여 여러 정책(Resources)을 시행할 수 있게 되면서 HHS는 2011년에 HIPAA 규정 준수 감사 프로그램을 시작했고, 2016년에 HIPAA에서 법 적용기관으로 규정한 수범기관(covered entities)에 대한 '사무 감사(desk audits)'를 통해서 상설 감사 프로그램의 기반을 마련했다.[9)]

2. 건강정보 구축현황

(1) 전자건강기록(EHR) 시스템

미국은 2009년부터 HITECH를 근거로, 환자의 의료기록을 디지털화하여 환자 개인이 열람할 수 있고, 필요시 정보를 교환할 수 있는 '전자건강기록(Electronic health record: 이하 'EHR')' 시스템을 시작했다.[10)]

EHR은 1960-70년대에 기본 프레임워크가 개발됐으나, 인터넷 사용이 활성화된 1990년대에 들어서야 실현되기 시작했다. 그러나 1990년대에는 환자의 건강정보와 처방전, 진료 결과 등의 정보를 디지털화하는 데 그쳤으며, 정보의 공유는 미비했었다. 2011년 미국 HHS 산하 보건의료재정청(Centers for Medicare & Medicaid Service: CMS)은 의료 전문가와 기관들의 EHR 사용을 장려하기 위해 'EHR 인센티브 프로그램(Promoting Interoperability Programs)'을 운영해 참여자를 대상으로 재정적인 지원을 제공하였다. 사용자 친화적인 EHR 플랫폼 개발이 활발히 진행 중이며, 관련 시장은 2021년 기준으로 272억 달러로 추정되었다.[11)]

---

9) The HIPAA JOURNAL, https://www.hipaajournal.com/what-is-the-hitech-act/. (2024년 2월 23일 검색)

10) HealthIT.gov, https://www.healthit.gov/faq/what-electronic-health-record-ehr. (2024년 2월 24일 검색)

11) 미국 보건의료재정청(CMS), https://www.cms.gov/regulations-and-guidance/legislation/ehrincentiveprograms?redirect=/ehrincentiveprograms. (2024년 2월 24일 검색)

(2) ‘All of US’ 연구 프로그램

미국은 2015년 개인 맞춤형 치료와 예방을 위해 의료 빅데이터를 구축하는 ‘정밀의료 이니셔티브(Precision Medicine Initiative: PMI)’를 발표했다.[12] 이 이니셔티브의 일환으로 미국 국립보건원(NIH)이 중심이 되어 ‘All of US’라는 대규모 유전학 프로젝트 연구 프로그램에 착수했다.[13]

이 프로젝트는 비식별 유전자 정보를 연구에 활용될 수 있도록 허용하는 것으로, 2026년까지 약 100만 명의 미국 시민에 대한 생활 습관·유전자·진료 기록·치료 접근성 등의 정보를 수집할 예정이다.

(3) 블루버튼

2010년 미국은 개인 건강정보에 대한 접근성을 용이하게 하고 본인의 의사에 따라 건강정보를 공유할 수 있는 ‘블루버튼(Blue Button)’ 서비스를 출시했다. 블루버튼은 미국 보건의료재정청(CMS), 국방부(Department of Defense) 등이 협력해 개발했고, 이후 기타 국가기관과 민간부문으로 확대되었다. 현재 HHS 산하 ONC에서 관리하고 있다.[14]

2010년 전역한 군인들을 대상으로 한 ‘재향군인 블루버튼(VA Blue Button)’에서 시작되었는데, 2012년 가을부터 ONC로 이관되면서 미국의 국가 노인 의료보험제도인 메디케어(Medicare) 수혜자를 대상으로 한 ‘메디케어 블루버튼’을 출시하는 등 블루버튼 적용 범위를 확대하였다.

의료기관 온라인 포털에서 본인의 건강정보를 쉽게 내려받고 공유 여부를 선택할 수 있다.[15] 2014년 5월에는 보다 안전한 개인정보보호 정책 및 포괄적인 정보 범위를 제공하는 ‘블루버튼 2.0’을 출시했고, 모든 건강정보를 한곳에 모아 개인의 건강관리를 지원하는 모바일 앱을 75개 이상 개발했

12) 오바마 행정부 문서기록보관소, https://obamawhitehouse.archives.gov/precision-medicine. (2024년 2월 24일 검색)
13) 미국 국립보건원(NIH), https://allofus.nih.gov/about/program-goals. (2024년 2월 26일 검색)
14) 미국 보훈처(VA), https://www.va.gov/bluebutton/. (2024년 2월 22일 검색)
15) HealthIT.gov, https://www.healthit.gov/topic/blue-button-faqs. (2024년 2월 26일 검색)

다.[16] 블루버튼을 통해 처리되는 PHI는 HIPAA 및 HIPAA Privacy Rule을 근거로 보호된다.[17]

Ⅲ. HIPAA 위반사례

1. Life Hope Labs, LLC

2021년 8월 24일 OCR은 불만 사항을 접수했는데, 민원인은 2021년 7월 7일 Life Hope Labs에 사망한 환자의 의무기록을 요청했으나 기록이 제공되지 않았다고 한다. 이 연구소는 처음 요청받은 이후 약 7개월(225일)이 지난 후에 사망한 환자의 딸에게 전체 의무기록을 전달했다. OCR은 요청된 의무기록 제공을 지연한 것이, 건강정보에 대한 청구권자의 접근권한(Access of individuals to protected health information)을[18] 위반한 것임을 확인했다.

Life Hope Labs는 잠재적인(potential) HIPAA 상의 접근권 위반을 해결하기 위해서, 위법 행위를 인정하지는 않고 $16,500의 벌금을 지급하는 것으로 OCR과의 사건 해결에 동의했다. Life Hope Labs는 필요에 따라 HIPAA Privacy Rule에 관한 서면 정책을 개발, 유지 및 개정하기 위한 요구 사항을 포함하는 시정 조치 계획을 채택해야 하고, PHI 사본을 작성하고 해당 정책을 모든 직원에게 배포해야 한다. 이 합의에는 2년 동안의 모니터링도 포함되었다.[19]

2. Banner Health

Banner Health는 미국 최대 규모의 비영리 의료시스템 중 하나로, 여기에

16) Medicare FAQ. (2023.2.7). What is the Medicare Blue Button 2.0?.
17) Oak St. Health, https://www.oakstreethealth.com/blue-button-privacy-policy. (2024년 2월 26일 검색)
18) 45 CFR § 164.524.
19) The HIPAA JOURNAL, https://www.hipaajournal.com/diagnostic-lab-settles-medical-record-access-case-for-16500/. (2024년 2월 9일 검색)

는 6개 주에 있는 30개 병원과 69개 이상의 제휴 의료 시설이 포함되어 있었고, 5만 명 이상의 직원이 있었다. 2016년 7월 13일 Banner Health는 보안 위반을 발견했고, 후속 조사에서 해커가 2016년 6월 17일에 Banner Health 시스템에 접근한 것으로 확인되었다. 해커는 281만 명의 PHI가 포함된 시스템에 접근할 수 있었다. 여기에서 PHI에는 이름, 주소, 생년월일, 사회보장번호, 청구 정보, 검사 결과, 약물, 진단 및 건강보험 정보가 포함되었다. OCR은 해커가 침입하여 PHI를 공개한 것에 대해 통보받은 후, HIPAA Security Rule 준수 여부에 대한 검토를 시작하여 규칙 미준수가 PHI 침해의 원인이 되었음을 확인했다.

HIPAA Security Rule은 개인정보처리자(의료기관 등)가 ePHI의 기밀성, 무결성 및 가용성을 보장하기 위해 기술적 보호 장치를 시행하도록 요구하고 있는데, OCR은 Banner Health가 ePHI에 액세스하려는 사람의 신원을 확인하여 본인이 누구인지 확인하는 충분한 절차를 이행하지 못했고, 전자 통신 네트워크를 통해 전송된 ePHI에 대한 무단 액세스로부터 보호하기 위한 기술적 보안 조치가 충분하지 않았다고 판단했다.

OCR은 Banner Health 조직 전체에서 HIPAA Security Rule을 오랜 기간 상당히 위반했다는 증거를 발견했다고 밝혔는데, 이는 해당 기관의 규모를 고려하면 심각하게 우려할 만한 사항이었다. Banner Health는 $1,250,000의 벌금을 지불하고 HIPAA Security Rule 위반 혐의를 해결하기 위한 시정 조치 계획을 채택하는 데 동의했다. 이에 따라, Banner Health는 정확하고 철저한 위험 분석을 수행하여 조직 전체에서 전자 환자/시스템 정보에 대한 위험과 취약성을 파악하고 위험 분석을 통해 식별된 취약성을 해결하기 위한 위험 관리 계획을 포함시켜야 했다. 무단으로 PHI에 접근하는 것을 막기 위해서, 위험 분석, 위험 관리, 시스템 작동 검토, 인증 프로세스 및 보안 조치를 시행하는 정책과 절차를 개발 및 이행하며, 직원에게 배포해야 한다. OCR은 2년 동안 Banner Health의 CAP(Corrective Action Plan) 준수 여부를 모니터링한다.[20]

---

20) The HIPAA JOURNAL, https://www.hipaajournal.com/banner-health-settles-alleged-hipaa-security-rule-violations-for-1-25-million/. (2024년 2월 10일 검색)

3. David Mente, MA, LPC

이 사건은 2017년 12월 세 자녀의 아버지가 미성년 자녀의 의료기록 사본을 면허 상담사인 David Mente에 요청했으나, Mente가 해당 의료기록 사본을 제공하지 않아서 발생하게 되었다. 불만 사항을 접수한 후 OCR은 Mente에게 연락하여 HIPAA 접근권한에 대한 기술 지원을 하고 불만 사항을 종결했다. 그런데, 2018년 4월 아버지가 두 번째로 의료기록 사본을 요청했는데, Mente는 요청한 기록을 다시 제공하지 않았고, 아버지는 OCR에 다시 민원을 제기했다.

OCR은 요청한 기록을 제공하지 못한 것이 HIPAA 상의 건강정보에 대한 접근권을 잠재적으로 위반한 것으로 판단했다. OCR은 Mente에게 $15,000의 벌금을 부과했고, 그는 이에 이의를 제기하지 않기로 하여 사건을 종결했다. Mente는 벌금 외에도, 규정 위반을 해결하기 위한 시정 조치 계획을 받아들일 것에도 동의했다. 이 계획에는 PHI에 대한 개인 접근과 관련된 정책과 절차를 검토·수정하고, 개인 PHI에 직원이 개별 접근하는 것에 관해 개인정보 보호 교육을 제공하고, 신고자가 요청한 기록을 제공하기 위해 최선의 노력을 기울여야 한다는 것이 포함되었다.[21]

4. MedEvolve Inc.

MedEvolve는 HIPAA 적용 수범기관(covered entities)에 진료 관리, 수익 주기 관리 및 진료 분석 소프트웨어를 제공하는 AR 기반 HIPAA 비즈니스 제휴사인데, 사업 특성상 HIPAA 적용 수범기관의 ePHI에 접근할 수 있었다.

2018년 7월 MedEvolve는 FTP 서버 구성에 오류가 발생했음을 OCR에 알렸는데, 자체 조사에 따르면, 서버에는 인증 없이 230,572명의 ePHI에 자유롭게 접근할 수 있었다. 이번 ePHI 침해 사고는 HIPAA 규제를 받는 두 기관인, Premier Immediate Medical Care, LLC(204,607명)와 Dr. Beverly Held(25,965명)에 영향을 미쳤다. 노출된 정보에는 이름, 청구서 수신 주소,

21) The HIPAA JOURNAL, https://www.hipaajournal.com/pittsburgh-counselor-fined-15000-for-hipaa-right-of-access-violation/. (2024년 2월 6일 검색)

전화번호, 건강보험사 정보, 진료소 계좌번호 및 일부 개인의 사회보장번호가 포함되었다.

OCR은 조사를 시작하여 HIPAA Privacy Rule에 대한 세 가지 잠재적 위반 사항을 확인했는데, 다음과 같다. 첫째, 동의 없이 개인 230,572명의 ePHI에 대한 공개(45 CFR § 164.502(a)),[22] 둘째, 하청업체와 사업 제휴 계약을 체결하지 않은 경우(45 CFR § 164.502(e)(1)(ii)),[23] 셋째, ePHI의 기밀성, 무결

22) (a) Standard. A covered entity may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.
(1) Permitted uses and disclosures. A covered entity is permitted to use or disclose protected health information as follows:
(i) To the individual;
(ii) For treatment, payment, or health care operations, as permitted by and in compliance with §164.506;
(iii) Incident to a use or disclosure otherwise permitted or required by this subpart, provided that the covered entity has complied with the applicable requirements of §164.502(b), §164.514(d), and §164.530(c) with respect to such otherwise permitted or required use or disclosure;
(iv) Pursuant to and in compliance with a valid authorization under §164.508;
(v) Pursuant to an agreement under, or as otherwise permitted by, §164.510; and
(vi) As permitted by and in compliance with this section, §164.512, or §164.514(e), (f), or (g).
(2) Required disclosures. A covered entity is required to disclose protected health information:
(i) To an individual, when requested under, and required by §164.524 or §164.528; and
(ii) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the covered entity's compliance with this subpart.

23) (ii) This standard does not apply:
(A) With respect to disclosures by a covered entity to a health care provider concerning the treatment of the individual;
(B) With respect to disclosures by a group health plan or a health insurance issuer or HMO with respect to a group health plan to the plan sponsor, to the extent that the requirements of §164.504(f) apply and are met; or
(C) With respect to uses or disclosures by a health plan that is a government program providing public benefits, if eligibility for, or enrollment in, the health plan is determined by an agency other than the agency administering the health plan, or if the protected health information used to determine enrollment or eligibility in the health plan is collected by an agency other than the agency

성 및 가용성에의 잠재적 위험에 대한 매우 철저하고 정확한 평가(45 CFR § 164.308(a)(1)(ii)(A)).[24]

MedEvolve는 책임이나 불법 행위를 인정하지 않고 사건을 해결하기로 하고 $350,000의 벌금을 지급하기로 합의했다. 이 합의에는 MEdEvolve가 정확하고 철저한 위험 평가를 수행하고, 인식한 위험을 해결하기 위한 위험 관리 계획을 이행하며, HIPAA Privacy and Security Rules을 준수하기 위한 정책 및 절차를 개발 및 이행하며, HIPAA 및 보안 교육 프로그램을 유지하는 것이 포함되었다.[25]

5. Manasa Health Center, LLC

2020년 4월 OCR은 Manasa Health Center가 부정적인 온라인 비평기사(Review)에 환자의 정신 건강 진단 및 치료 정보를 온라인으로 부당하게 공개했다는 불만 사항을 접수했다.

OCR은 Manasa Health Center에 대한 조사를 시작했고, 부정적인 Google 기사에 대한 응답으로 총 4명의 환자 동의 없이 PHI가 공개되었음을 발견하여 2020년 11월 18일에 HIPAA Privacy Rule 위반 여부에 대해 조사하고 Manasa Health Center에 통보했다. 환자의 동의 없이 PHI를 공개한 것(45 CFR § 164.502(a)) 외에도 Manasa Health Center는 HIPAA Privacy Rule의 표준, 이행 사양 또는 기타 요구 사항을 준수하지 않은 것(45 CFR § 164.530(i))으로 확인되었다.

Manasa Health Center는 책임이나 불법 행위를 인정하지 않고 OCR과

---

administering the health plan, and such activity is authorized by law, with respect to the collection and sharing of individually identifiable health information for the performance of such functions by the health plan and the agency other than the agency administering the health plan.

24) (ii) Implementation specifications:
(A) Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

25) The HIPAA JOURNAL, https://www.hipaajournal.com/ocr-fines-arkansas-business-associate-350000-for-impermissibly-disclosing-ephi/. (2024년 2월 10일 검색)

벌금 $30,000로 사건을 해결하기로 했다. 재정적 처벌 외에도 Manasa Health Center는 HIPAA Privacy Rule을 준수하도록 서면 정책 및 절차를 개발, 유지·개정하고, 모든 직원에게 교육을 제공하라는 요구 사항을 포함하는 시정 조치 계획을 채택하기로 했다. 해당 정책 및 절차에 대해 직원들에게 알리고, PHI가 동의 없이 온라인에 공개된 개인(정보주체)에게 위반 통지문을 발송하며, 해당 공개에 대해 OCR에 위반 보고서를 제출하도록 했다.[26]

6. Yakima Valley Memorial Hospital

2018년 2월 28일 워싱턴 주에 있는 222개의 병상을 갖춘 비영리 지역사회 병원인 Yakima Valley Memorial Hospital에서 비교적 소규모의 데이터 유출이 OCR에 보고되었다. 병원 측은 경비원이 환자의 진료기록에 접근해 419건의 진료기록을 무단으로 열람한 사실을 적발했다.

OCR은 2018년 5월 이 사건에 대한 조사를 시작했고, 병원 응급실 경비원이 의료기록을 광범위하게 열람했다는 것을 밝혀냈다. 23명의 경비원은 정당한 이유 없이 자신의 로그인 권한을 통하여 병원의 EMR 시스템에 있는 의료기록에 접근했다. 경비원들은 시스템 안에 저장된 이름, 주소, 생년월일, 의료기록 번호, 치료 관련 특정 메모, 보험정보 등 보호 대상 건강정보를 볼 수 있었다. OCR은 병원이 HIPAA Security Rule 상의 표준, 이행기준 또는 기타 요구 사항을 준수하기 위해 합리적이고 적절한 정책 및 절차를 이행하지 못했다고 판단했다.

Yakima Valley Memorial Hospital은 OCR과 책임 인정 없이 벌금 $240,000를 지급하기로 합의하고 사건을 마무리하기로 했다. 그 외에도 정확하고 포괄적인 위험 분석, 위험 분석에서 식별된 위험을 해결하기 위한 위험 관리 계획의 개발 및 이행, HIPAA 정책 업데이트 및 HIPAA 규칙의 철저한 준수를 보장하기 위한 시정 조치 계획도 포함했다.[27]

---

26) The HIPAA JOURNAL, https://www.hipaajournal.com/30000-penalty-disclosing-phi-online-negative-reviews/. (2024년 2월 11일 검색)

27) The HIPAA JOURNAL, https://www.hipaajournal.com/washington-hospital-security-guard-snooping-240000-hipaa-penalty/. (2024년 2월 9일 검색)

7. iHealth Solutions, dba Advantum Health

Advantum Health로 사업을 하고 있는 iHealth Solutions는 서버 중 하나를 보호하지 못하면서, 2017년 5월 2일 개인이 무단으로 접근하여 267명의 ePHI가 포함된 파일을 유출했다는 것을 확인했고, OCR은 2017년 8월 22일 데이터 침해 사실을 통보받았다.

데이터 유출 보고 후 OCR의 조사를 받은 iHealth Solutions는 HIPAA 규칙의 가장 기본적인 조항 중 하나인 위험 분석을 준수하지 않은 것으로 밝혀졌다. HIPAA의 적용을 받는 수범기관(covered entities)은 정확하고 철저한 조직 전반의 위험 분석을 수행하여 ePHI의 기밀성, 무결성 및 가용성에 대한 모든 위험과 취약성을 식별해야 한다.

iHealth Solutions는 동의 없이 ePHI 유출 및 위험 분석 실패에 대해서 OCR과 $75,000의 벌금을 지급하기로 합의하고 사건을 마무리했다. iHealth Solutions는 재정적 처벌 외에도 iHealth Solutions ePHI의 기밀성, 무결성 및 가용성에 대한 잠재적인 보안 위험과 취약성을 정확하고 철저하게 평가하고 위험을 개발하기 위한 요구 사항을 포함하는 시정 조치 계획을 이행하는 데 동의했다. HIPAA Privacy & Security Rule을 준수하여, 위험 분석에서 식별된 모든 보안 위험을 해결 및 완화하고, iHealth Solutions ePHI의 보안에 영향을 미치는 환경 또는 운영 변경을 평가하는 프로세스를 개발하며, 필요에 따라 서면 정책 및 절차를 개발, 유지 및 수정하기 위한 관리 계획을 수립하기로 했다. 그리고 OCR은 HIPAA 규칙 준수 여부를 확인하기 위해 2년 동안 iHealth Solutions를 모니터링한다.[28]

8. UnitedHealthcare

UnitedHealthcare Insurance Company(UHIC)는 2021년 1월 고객이 PHI 사본을 요청했는데, 어느 정도의 시간이 지나도 회사의 응답이 없어서 2021년 3월 25일 OCR에 민원을 제기했다. OCR은 2021년 4월 조사를 시작했는

28) The HIPAA JOURNAL, https://www.hipaajournal.com/ihealth-solutions-75000-hipaa-settlement/. (2024년 2월 6일 검색)

데, UHIC는 2021년 7월에 고객이 요청한 PHI를 발송했다.

UHIC는 OCR을 통해 이 문제를 인지했을 때, 자체적으로 내부 조사를 시행하여 규정 미준수가 직원의 감독(oversight) 때문으로 파악했다. 그런데도 OCR은 고객에게 제때 PHI를 제공하지 못한 것에 대해서 HIPAA Privacy Rule(45 CFR §164.524) 위반으로 결론 내려 $80,000의 벌금을 부과하는 것으로 사건을 마무리했다. 그 외에도 UHIC는 최소 1년 동안 시정 조치 계획을 준수하기로 합의했다. 이 계획은 UHIC가 고객의 PHI 접근 요청과 관련된 정책 및 절차를 적절히 수정하고, 수정된 정책을 직원에게 배포하며, 직원들이 수정된 정책과 관련된 교육을 받는 것을 포함한다.[29]

9. L.A. Care Health Plan

LA Care Health Plan은 미국에서 가장 큰 공공 건강보험사로 270만 명 이상의 회원을 보유하고 있다. OCR은 LA Care Health Plan에 대해 두 가지 사항을 조사했는데, 첫째는 회원 포털을 통해서 동의 없이 PHI를 공개하여 언론 보도에 대응한 것이고, 둘째는 1,498명의 회원의 PHI와 관련하여 규정을 위반한 것이다.

2014년 3월, 한 온라인 언론 매체는 LA Care Health Plan 보험 가입자가 2014년 1월 22일부터 1월 24일 사이에 온라인 회원 포털을 통해 다른 회원의 PHI에 접근할 수 있었다고 보도했다. 이것은 수동 조작과정의 오류(a manual processing error)가 원인으로, 회원이 다른 회원의 이름, 주소, 회원 식별번호 등의 정보를 열람할 수 있도록 되어 있었다. 2016년 1월 OCR은 규정 준수 검토를 시작하여 2016년 2월 LA Care Health Plan이 500명 미만의 개인회원 PHI가 유출된 것으로 판단했다. 그리고 2019년 3월 LA Care Health Plan은 2019년 1월 30일경에 1,498건의 기록 데이터가 침해되었다고 OCR에 통보했다. 이것은 회원들이 우편으로 다른 회원의 ID 카드를 받는 과정에서 발생했다.

OCR은 HIPAA Privacy and Security Rule의 요구 사항을 제대로 준수하

29) The HIPAA JOURNAL, https://www.hipaajournal.com/potential-hipaa-right-of-access-violation-settled-for-80000/. (2024년 2월 16일 검색)

지 않은 사항들을 확인했고, 못한 여러 가지 실패가 있음을 확인했고, 해결 방법에 대한 합의서에 HIPAA 위반 사항 6가지를 다음과 같이 나열했다.

① 모든 ePHI의 기밀성, 무결성 및 가용성에 대한 잠재적 위험과 취약성에 대해서 정확하고 철저한 위험 분석을 수행하지 못함(45 CFR § 164.308(a)(1)(ii)(A) 위반)
② 위험과 취약성을 합리적이고 적절한 수준으로 줄이는 데 충분한 보안 조치를 실행하지 못함(45 CFR § 164.308(a)(1)(ii)(B) 위반)
③ 정보 시스템 운영 기록을 정기적으로 감독하기 위한 충분한 절차를 구현하지 못함(45 CFR § 164.308(a)(1)(ii)(D))
④ 초기에는 이 규칙에 따라 이행된 표준을 기반으로 했으나, 이후 ePHI의 보안에 영향을 미치는 환경 또는 운영 변화에 대응하여 주기적인 기술 및 비기술적 평가를 수행하지 못함(45 CFR FR § 164.308(a)(8) 위반)
⑤ ePHI를 포함하거나 사용하는 정보 시스템 운영을 기록하고 조사하는 하드웨어, 소프트웨어와 절차적 메커니즘을 구현하지 못함(45 CFR 164.312(b) 위반)
⑥ 1,498명의 개인 ePHI에 대해 동의 없이 공개(45 CFR § 164.502(a) 위반)

LA Care Health Plan은 책임을 인정하지 않고 조사를 해결하기로 했고, $1,300,000의 벌금을 지급하고 HIPAA 위반 혐의를 시정하기 위한 시정 조치 계획을 받아들일 것에 동의했다. 시정 조치 계획에는 조직 전체의 포괄적인 위험 분석을 수행하고, 위험 관리 계획을 개발하며, 위험 분석 및 위험 관리 계획을 위한 정책 및 절차를 개발, 실행 및 배포하며, 환경 및 위험 평가 시 OCR에 보고해야 하며, HIPAA 규정을 위반하면 30일 이내에 OCR에 보고해야 한다는 내용이 포함되었다.[30]

30) The HIPAA JOURNAL, https://www.hipaajournal.com/la-care-health-plan-1300000-hipaa-settlement/. (2024년 2월 15일 검색)

10. Doctors' Management Services

Doctors' Management Services(DMS)는 의료 관리 회사로 의료비 청구 및 지급 자격 증명을 포함한 서비스를 제공한다. DMS는 2018년 12월 24일 네트워크의 파일을 암호화할 때 GandCrab 랜섬웨어가 침입한 것을 확인했다. 포렌식 조사를 통해 2017년 4월 1일 처음으로 네트워크에 접근한 것으로 확인되었다. DMS에 따르면, 침입자는 워크스테이션 중 하나에서 원격 데스크톱 프로토콜(RDP)을 통해 네트워크에 접근하여 이름, 주소, 생년월일, 사회보장번호, 보험정보, 메디케어/메디케이드 ID 번호, 운전면허증 번호 및 진료 정보를 유출하면서, 최대 206,695명의 정보가 침해되었다. 이 사실은 2019년 4월 22일 OCR에 보고되었다.

OCR은 DMS의 HIPAA 규칙 위반 여부를 조사하여 여러 개의 위반 사항을 발견했다. OCR은 206,695명의 회원의 PHI를 동의 없이 유출되도록 한 것 외에도, DMS가 ePHI 처리와 관련된 기술적·물리적·환경적 위험과 취약성을 평가하기 위한 정확하고 철저한 위험 분석을 수행하지 못했다고 판단했다.

또한 DMS는 감사 로그, 액세스 보고서, 보안 사고 추적 보고서 등 정보 시스템 운영 기록을 정기적으로 검토하는 절차를 이행하지 않은 것으로 밝혀졌다. 게다가 OCR은 DMS가 보안 규칙의 기준, 이행사항 또는 기타 요구사항을 준수하기 위해 합리적이고 적절한 정책과 절차를 실행하지 않았다고 판단했다.

DMS는 책임을 인정하지 않고 조사를 해결하는 데 동의했고, 합의 조건에 따라 $100,000의 벌금을 지불하고, OCR에서 식별한 잠재적인 HIPAA 위반을 해결하기 위해 시정 조치 계획(CAP)을 실행하기로 합의했다. CAP에는 위험 분석, 위험 관리 프로그램, HIPAA Privacy and Security Rule 정책 및 절차, 직원들에게 HIPAA 교육을 위한 요구 사항이 포함되었다. OCR은 이것이 랜섬웨어 공격에 대응하여 체결한 최초의 HIPAA 합의 계약이라고 했다.[31]

---

31) The HIPAA JOURNAL, https://www.hipaajournal.com/doctors-management-services-settles-ocr-hipaa-probe-for-100000/. (2024년 2월 11일 검색)

11. St. Joseph's Medical Center

HIPAA Privacy Rule은 치료, 지급 및 의료 운영 목적으로 PHI의 공개는 허용하지만, 환자의 동의 없이 PHI의 공개는 일반적으로 허용하지 않는다. OCR은 AP 기자가 언론에 기사를 게재한 것에 따라 2020년 4월 20일 St. Joseph's Medical Center에 대한 조사를 시작했다.

기사에는 기자가 코로나19를 치료받는 환자 3명을 관찰하도록 허락받은 것으로 드러났다. 해당 기사에는 코로나19 비상사태에 대한 해당 의료기관의 대응 정보와 해당 시설 환자에 대한 사진 및 정보가 포함됐다. 해당 기사는 미국 전역으로 배포되어서, 환자의 코로나19 진단명, 현재 의료상태 및 의학적 예후, 활력징후, 치료계획 등의 PHI가 공개되었다. OCR의 조사 결과 St. Joseph's Medical Center가 기자에게 환자와 임상 정보에 대한 접근을 허용했다는 증거가 발견되었다. St. Joseph's Medical Center는 환자로부터 동의와 적법한 HIPAA의 승인을 받지 않았으므로, HIPAA Privacy Rule에 따라 PHI를 공개해서는 안 되었다.

St. Joseph's Medical Center는 책임을 인정하지 않고 OCR과 HIPAA 위반 혐의를 $80,000의 벌금을 부과하는 것으로 결정했고, 시정 조치 계획(CAP)을 받아들이는 것에 동의했다. CAP는 St. Joseph's Medical Center가 HIPAA Privacy Rule을 준수하는지 확인하기 위해서, 서면으로 개인정보 보호 정책 및 절차를 검토하여 필요한 범위 내에서 개발, 유지 및 수정하고, 검토를 위해서 OCR에 해당 정책 및 절차를 제공하도록 요구했다. 업데이트된 정책과 절차를 직원들에게 배포하고, 모든 직원이 새로운 정책과 절차를 읽고 이해했음을 확인하는 문서에 서명하거나 전자 규정 준수 증명서를 제출하도록 했다.

이 외에도, St. Joseph's Medical Center는 모든 직원에게 60일 이내에, 신규 채용자에게는 30일 이내에 '리더십'을 포함한 HIPAA 재교육을 실시해야 한다. 추가 재교육은 매년 실시해야 하고, 정책 및 절차의 후속 변경 사항, 개정된 OCR 지침, 규제 변경 사항 또는 위험 평가 등은 PHI의 개인 정보 보호 및 보안에 대한 위협이 확인되면 더 자주 교육해야 한다. St. Joseph's Medical Center는 OCR의 규정 준수 여부를 2년 동안 모니터링한다.[32)]

12. Lafourche Medical Group

OCR은 2021년 3월 30일 해커가 의료 그룹인 Lafourche Medical Group의 소유주 중 한 명을 스푸핑(Spoofing)하여 그 소유주의 이메일 계정에 액세스할 수 있게 되었다는 신고를 받았다. 해커는 환자의 정보가 포함된 Microsoft 365에 대한 액세스 권한을 얻었다. Lafourche Medical Group은 이메일 시스템의 규모가 커서 노출된 모든 환자 정보를 확인할 수 없기에 모든 환자에게 알림 편지를 발송했다고 한다. 노출된 정보에는 이름, 주소, 생년월일, 서비스 날짜, 이메일 주소, 전화번호, 의료기록 번호, 보험 및 건강보험 수혜자 번호, 보증인 이름, 진단, 치료 의사 이름 및 실험실 테스트 결과가 포함되었다.

OCR은 HIPAA Security Rule을 준수하지 않은 것이 보안 위반으로 이어졌거나 어느 정도 영향을 미쳤는지를 확인하기 위해서 사건에 대한 조사했다. OCR 조사관은 Lafourche Medical Group이 피싱 공격 이전에 보안 위험 분석을 수행하지 않았다는 사실을 발견했다(HIPAA Security Rule 45 CFR § 164.308(a)(1)(ii)(A)[33] 위반). 또한, OCR은 Lafourche Medical Group이 피싱 공격 이전에 정보 시스템 활동 기록을 정기적으로 검토하는 절차를 이행하지 않았다고 판단했다(HIPAA Security Rule 45 CFR § 164.308(a)(1)(ii)(D)[34] 위반).

Lafourche Medical Group은 책임이나 불법 행위를 인정하지 않고 조사를 마무리하는 데 동의하여 $480,000의 벌금을 지급하는 것 외에도 ePHI에 대한 보안 위험과 취약성을 줄이기 위한 보안 조치 수립 및 이행, 서면 정책 및 절차의 개발, 유지 및 수정을 포함하는 강력한 시정 조치 계획(CAP)을 실행하기로 합의했다. 또한, Lafourche Medical Group은 HIPAA Security

32) The HIPAA JOURNAL, https://www.hipaajournal.com/st-josephs-medical-center-pays-80000-hipaa-fine-for-phi-disclosure-to-a-reporter/. (2024년 2월 11일 검색)

33) (A) Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

34) (D) Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

Rule을 준수하고, 필요한 경우에 PHI에 접근할 수 있는 모든 직원에게 HIPAA 교육을 제공해야 한다. 또한 OCR은 Lafourche Medical Group을 HIPAA Security Rule을 준수하는지 2년 동안 모니터링한다.[35]

13. Optum Medical Care of New Jersey

2021년 가을 OCR은 민간 종합 전문 의사 그룹인 Optum Medical Care에 기록 제공을 요청했으나 오랜 기간 기록을 받지 못한 개인으로부터 6건의 민원을 접수했다. 민원인들은 본인 기록 사본 또는 미성년 자녀의 기록 사본을 요청했다.

HIPAA Privacy Rule은 개인에게 자신과 미성년 자녀의 의료기록 사본을 제공받을 권리를 인정한다. HIPAA의 적용을 받는 수범기관(covered entities)은 이처럼 의료기록 사본 제공의 요청을 받으면, 해당 기록은 30일 이내에 제공되어야 하고, 예외적으로 30일 연장할 수 있다. OCR은 위의 민원에 대해서 2022년 2월 조사를 시작하여 Optum Medical Care가 해당 기록 제공에 허용된 기간을 초과했다고 결정했다. 민원인은 요청한 기록을 받기까지 84일에서 231일을 기다려야 했다.

Optum Medical Care는 위반 혐의를 해결하기로 하여 $160,000의 재정적 벌금을 지불하고, PHI에 대한 개인 접근에 대한 정책 및 절차를 검토 및 수정하고 직원에게 새로운 절차에 대한 교육을 제공하는 것을 포함하는 시정조치 계획(CAP)을 채택하기로 했다. 따라서 모든 환자가 요청한 기록을 30일 이내에 제공해야 하고, 사본 제공 요청을 거부할 때는 OCR에 이를 알리고 해당 거부를 증빙하는 자료를 제공해야 한다. OCR은 Optum Medical Care의 CAP 준수 여부를 1년 동안 모니터링한다.[36]

---

35) The HIPAA JOURNAL, https://www.hipaajournal.com/lafourche-medical-group-first-hipaa-penalty-phishing/. (2024년 2월 12일 검색)

36) The HIPAA JOURNAL, https://www.hipaajournal.com/optum-medical-care-new-jersey-hipaa-settlement/. (2024년 2월 13일 검색)

Ⅳ. 결론: 시사점과 우리 제도에의 적용 가능성

미국은 우리와 달리 개인정보와 관련한 일반법은 존재하지 않으나, 앞에서 언급한 HIPAA, HITECH 외에도 21세기 치료법 등 다양한 개별법을 통해서 건강정보의 보호와 활용을 할 수 있도록 하고 있다. 무엇보다 미국은 우리나라보다 건강정보를 포함한 개인정보의 활용에 훨씬 유연한 태도를 보여서 건강정보를 활용할 수 있는 정도와 범위가 더 넓은 것으로 생각된다. 그러나, 우리도 미국처럼 활용 범위를 넓혀야 한다는 주장이 받아들여지기는 쉽지 않다. 오히려 지금까지 우리나라에서 외국과 비교하여 건강정보를 포함한 개인정보의 보호적 측면이 더 많이 강조되었던 원인을 살펴보고, 건강정보 활용의 필요성과 범위, 활용한 이후에 문제가 발생할 경우의 해결방안, 정보 유출 시 책임의 소재와 방법 등에 대해서 다양하게 고민하는 것이 우선해야 할 것이다.

특히, 앞의 HIPAA 위반사례에서 기술한 것처럼, HIPAA, HIPAA Privacy and Security Rule, HITECH 등을 위반한 경우에 엄격한 재정적 부담을 주는 것은 우리도 도입할 필요가 있다고 생각한다. 물론, 우리나라도 개인정보보호법, 의료법, 정보통신망법 등을 통해서 개인정보처리자, 의료인을 포함한 의료기관 등이 해당 규정을 위반하면 이를 처벌할 규정이 있다. 그러나 지금까지 우리는 대체로 관대한 처벌로 위반한 본인뿐만 아니라 다른 제3자에게 예방효과가 전혀 없었고, 오히려 개인정보 유출에 대한 경각심이 사라지면서 국민이 정보보호에 별로 관심을 두지 않는 경향이 강하다. 특히 개인(건강)정보처리자 또는 처리 권한이 없이 (건강)정보를 유출한 사람을 제대로 처벌하지 않은 것은 심각한 문제이다.

미국 HIPAA 등을 위반한 경우에, 위반 수준에 따라서 처벌 수위가 다양하게 구분되어 있는데, 중대한 위반의 경우 최대 $200만 이상의 벌금을 부과하고 있고, 재발 방지를 위해서 다양한 대책을 마련하도록 하면서, 미국 보건부의 OCR에서 1-2년 정도 계속 모니터링을 하고 있다.

물론 너무 과도한 처벌로 법령을 위반한 개인정보처리자에게 경제적 부담을 줄 수 있다는 반론도 있을 것이다. 그러나 적어도 개인정보, 특히 건강정보의 활용에 대한 논의를 위해서는 정보 활용에 대한 책임도 커져야 하고,

이를 위해서는 관련 법령을 통해서 적절한 책임을 부담할 수 있도록 해야 할 것이다.

| 참고문헌 |

1. 논문 및 단행본

김재선 (2016). “의료정보의 활용과 개인정보의 보호: 미국 HIPPA/HITECH 연구를 중심으로.”『행정법연구』. 제44호, pp. 269-290.

_____ (2021). “미국의 보건의료데이터 보호 및 활용을 위한 주요 법적 쟁점: 미국 HIPAA/HITECH, 21세기 치료법, 공통규칙, 민간 가이드라인을 중심으로.”『의료법학』. 제22권. 제4호, pp. 117-157.

이한주 (2012). “개인의료정보의 헌법적 보호.” 고려대학교 박사학위논문.

전한덕 (2022). “보건의료데이터의 활용과 정보보호에 관한 연구.”『보험학회지』. 제131호, pp. 57-102.

2. 기타

미국 국립보건원(NIH). https://allofus.nih.gov/about/program-goals. (2024년 2월 26일 검색)

미국 보건의료재정청(CMS). https://www.cms.gov/regulations-and-guidance/legislation/ehrincentiveprograms?redirect=/ehrincentiveprograms. (2024년 2월 24일 검색)

미국 보훈처(VA). https://www.va.gov/bluebutton/. (2024년 2월 22일 검색)

오바마 행정부 문서기록보관소. https://obamawhitehouse.archives.gov/precision-medicine. (2024년 2월 24일 검색)

HealthIT.gov. https://www.healthit.gov/faq/what-electronic-health-record-ehr. (2024년 2월 24일 검색)

_____. https://www.healthit.gov/topic/blue-button-faqs. (2024년 2월 26일 검색)

Oak St. Health. https://www.oakstreethealth.com/blue-button-privacy-policy. (2024년 2월 26일 검색)

The HIPAA JOURNAL. https://www.hipaajournal.com/30000-penalty-disclosing-phi-online-negative-reviews/. (2024년 2월 11일 검색)

_____. https://www.hipaajournal.com/banner-health-settles-alleged-hipaa-security-rule-violations-for-1-25-million/. (2024년 2월 10일 검색)

_____. https://www.hipaajournal.com/diagnostic-lab-settles-medical-record-access-case-for-16500/. (2024년 2월 9일 검색)

_____. https://www.hipaajournal.com/doctors-management-services-settles-ocr-

hipaa-probe-for-100000/. (2024년 2월 11일 검색)
_____. https://www.hipaajournal.com/hipaa-violation-cases/. (2024년 2월 13일 검색)
_____. https://www.hipaajournal.com/ihealth-solutions-75000-hipaa-settlement/. (2024년 2월 6일 검색)
_____. https://www.hipaajournal.com/la-care-health-plan-1300000-hipaa-settlement/. (2024년 2월 15일 검색)
_____. https://www.hipaajournal.com/lafourche-medical-group-first-hipaa-penalty-phishing/. (2024년 2월 12일 검색)
_____. https://www.hipaajournal.com/ocr-fines-arkansas-business-associate-350000-for-impermissibly-disclosing-ephi/. (2024년 2월 10일 검색)
_____. https://www.hipaajournal.com/optum-medical-care-new-jersey-hipaa-settlement/. (2024년 2월 13일 검색)
_____. https://www.hipaajournal.com/pittsburgh-counselor-fined-15000-for-hipaa-right-of-access-violation/. (2024년 2월 6일 검색)
_____. https://www.hipaajournal.com/potential-hipaa-right-of-access-violation-settled-for-80000/. (2024년 2월 16일 검색)
_____. https://www.hipaajournal.com/st-josephs-medical-center-pays-80000-hipaa-fine-for-phi-disclosure-to-a-reporter/. (2024년 2월 11일 검색)
_____. https://www.hipaajournal.com/washington-hospital-security-guard-snooping-240000-hipaa-penalty/. (2024년 2월 9일 검색)
_____. https://www.hipaajournal.com/what-is-a-hipaa-violation/. (2024년 2월 18일 검색)
_____. https://www.hipaajournal.com/what-is-the-hitech-act/. (2024년 2월 23일 검색)

| **논문투고일** : 2024년 02월 16일 |
| **논문심사일** : 2024년 02월 26일 |
| **게재확정일** : 2024년 03월 07일 |

| ABSTRACT |

Legal Issues on U.S. Health Information Policy through HIPAA Violation Cases

Lee, Han Joo
(Korean Medico-legal Institute)

The information protected under HIPAA law is known as Protected Health Information – a subset of individually identifiable health information that is protected under HIPAA law when it is created, received, maintained, or transmitted by a covered entity. Individually identifiable non-health information is also protected under HIPAA law when it is maintained in the same designated record set as Protected Health Information.

The Healthcare Insurance Portability and Accountability Act (HIPAA) consist of five Titles, each with their own set of HIPAA laws. Four of the five sets of HIPAA compliance laws are straightforward and cover topics such as the portability of healthcare insurance between jobs, the coverage of persons with pre-existing conditions, and tax provisions for medical savings accounts.

However, Title II – the section relating to administrative simplification, preventing healthcare fraud and abuse, and medical liability reform – is far more complicated. It contains subsets of HIPAA laws which sometimes overlap with each other and several of the provisions in Title II have been modified, updated, or impacted by subsequent acts of legislation.

In this paper, we will examine recent cases that the Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services (HHS) determined to have violated HIPAA. Through this, we would like to propose a plan to ensure that personal information protection laws,

including the Personal Information Protection Act, are effectively guaranteed in Korea as well.

▪ Key words: Health Information, EHR(Electronic Health Record), Healthcare, HIPAA, Medical Big Dada