연구논문

연구에 있어서 피험자의 건강정보보호를 위한 HIPAA Privacy Rule의 적용*

박 수 헌**

차 례

* 본 논문은 숙명여자대학교 2012학년도 교내연구비 지원해 의해 수행되었음.
** 숙명여대 법과대학 교수, 법학박사
접수일자 : 2012. 4. 27 / 심사일자 : 2012. 6. 18 / 게재확정일자 : 2012. 6. 22

I. 머리말

최근의 신문보도에 따르면 우리나라의 건강정보화가 급속히 증가하고 있다고 한다.[1] 건강정보화의 증가에 비례하여, 건강정보보호 또한 중요한 법적 과제로 대두하고 있다. 이러한 건강정보는 정보주체의 프라이버시 보장에 있어 매우 민감한 정보[2]임에도 불구하고, 다양한 기관에서 여러 부서의 구성원들이 사용하거나 공유해야 할 필요성이 있다. 특히, 연구를 할 경우에는 연구기관, 연구자, 의뢰자, 임상시험수탁기관, 독립자료모니터링위원회, 임상시험심사기관 등 다수 당사자들 간에 피험자의 건강정보가 이용되거나 공개될 수 있다.[3] 따라서, 건강정보가 연구에 사용될 때 피험자의 건강정보를 어떻게, 어느 범위까지 이용·공개하여 피험자의 프라이버시를 보호할 것인가에 관한 법적 해결방안을 마련하는 것이 급선무라 하겠다. 이에, 우리정부는 2011년 9월 30일 개인정보보호법을 시행하여 연구뿐만 아니라 모든 분야에서 정보주체의 개인정보가 적절히 보호될 수 있도록 법적 장치를 마련하였다. 다만, 동법은 그 제정이유와 전체 법률 내용에 비추어 인터넷상 경제활동에 대한 규제에 관한 일반법이라 할 수 있겠지만, 건강정보의 보호에 관해서는 동법이 일반법으로서의 기능과 역할을 그다지 충실하게 수행할 수는 없는 것으로 보인다. 왜냐하면, 의료정보를 포함하는 건강정보에는 성

1) 실제 건강보험심사평가원이 국내 1만 2218개 병원을 대상으로 조사한 결과 전자의무기록(EMR)은 종합병원 66%, 병원급 52%, 처방전달시스템(OCS)은 종합병원 93%, 병원급 74%, 의료영상저장전송시스템(PACS)은 종합병원 96%, 병원급 43% 등 절반 이상의 병원에서 사용하고 있는 것으로 나타났다. 매일경제, 2011. 12. 7. 수요일, B7면. 건강정보는 “의료기관, 의료보험, 보건행정기관, 고용주, 보험회사, 학교, 건강정보처리기관에 의해 형성되거나 접수되는 살아있거나 죽은 사람의 과거, 현재, 또는 미래의 신체적 또는 정신적 상태, 치료, 또는 치료비 지급과 관련하는 구두 또는 기록된 모든 형태(문서, 전자적, 그리고 엑스레이나 초음파와 같은 영상 등)의 정보” (HIPAA Administrative Simplification Regulation 45 CFR § 160.103)를 말한다.

2) 개인건강정보의 부적절한 누설은 의료보험·생명보험·고용·경제활동·교육 등에서 차별과 사회적으로 불리한 낙인의 원인이 되고 정신적인 스트레스나 대인관계의 파괴로 연결될 수 있고, 개인건강정보의 적절한 보호가 이루어지지 않는다는 사실은 환자와 의사 간 불신을 조장하여 의료서비스의 질에 악영향을 미칠 수 있다고 한다. 백윤철·김상겸, 「미국의 의료정보보호에 대한 연구」, 한국학술정보, 2006, 32쪽.

3) Cynthia McGuire Dunn & Gary L. Chadwick, Protecting Study Volunteers in Research, CenterWatch, 2004, p. 148.

명, 주소, 주민등록번호, 전화번호 등과 같은 개인식별정보와 진료, 검사결과 등이 결합하여 존재하므로 인터넷상의 개인정보보다는 개인의 프라이버시에 더 중요한 내용을 가지고 있기 때문이다.[4] 따라서, 인터넷상의 개인정보보호를 위주로 하는 동법을 가지고 그와는 훨씬 더 강하게 보호되어야 할 건강정보를 적절하게 규제하기는 어렵다고 본다. 그 결과, 연구에 있어서 피험자의 건강정보를 적절히 보호하기에도 적합하지 않은 것으로 보인다.

이와는 달리 미국의 경우, 개인의 건강정보보호를 위해 1996년 「의료보험의 이전과 그에 수반하는 책임에 관한 법」(Health Insurance Portability and Accountability Act; 이하 'HIPAA'라 함. Pub. L. No. 104-191, 110 Stat. 1936 (1996))을 제정하여 시행하고 있고, 이에 근거한 법규명령인 Privacy Rule (이하 '프라이버시룰'이라 함)을 제정하여 2003년부터 개인식별가능한 건강정보에 관한 정보주체의 프라이버시를 안전하게 보호하기 위한 최소한의 연방기준을 마련하여 시행하고 있다. 이 프라이버시룰은 연구에 있어서 피험자의 건강정보를 보호할 목적으로만 제정된 것은 아니지만, 개인건강정보의 이용 및 공개의 주체·방법·범위·시기 등을 규정하고 있기 때문에, 건강정보를 사용하는 연구에도 실질적 영향을 미친다. 따라서, 연구에 있어서 피험자의 건강정보의 보호를 위해 연구자등은 이 프라이버시룰을 이해하는 것이 매우 중요하게 되었다. 앞서 언급한 바와 같이, 연구의 경우에는 피험자의 건강정보를 이용하고 공개하는 범위가 연구 이외의 경우에 비해 매우 넓기 때문에 피험자의 건강정보 보호가 중요하다는 사실, 프라이버시룰이 연구에 있어서 피험자의 건강정보를 적절히 보호할 수 있는 유용한 규제수단이라는 사실, 그리고 우리의 개인정보보호법으로는 연구에 있어서 피험자의 건강정보를 적절히 보호할 수 없다는 사실 등에 기초하여 이 논문은 연구에 있어서 피험자의 건강정보를 적절히 보호할 수 있는 규정을 가지고 있는 프라이버시룰에 대한 고찰을 주된 목적으로 한다. 또한, 이러한 고찰을 바탕으로 연구에 있어서 피험자의 건강정보를 적절히 보호할 수 있도록 우리의 개인정보보호법에 대한 개선방안의 제시도 이 논문의 목적으로 한다.

4) 김장한, "의료기관 개인건강정보의 이차적 이용", 「의료법학」 11권1호, 한국의료법학회, 2010, 119쪽.

Ⅱ. HIPAA의 개관

1. HIPAA의 제정 이유 및 목적

HIPAA는 1996년 연방법률로 제정되어, 이전에는 개별 주에서 독자적으로 취급한 의료보험을 연방 차원에서 통일적으로 규제가능하도록 하였다.[5] 즉, HIPAA에 따라, A 기업의 근로자가 다른 주의 B 기업으로 이직한 경우, 이전 A 기업에서 들고 있었던 의료보험을 B 기업으로 가져갈 수 있게 되었다. HIPAA 이전에는 위의 예의 경우 B 기업에서 의료보험을 들때까지 이직 근로자는 의료보험 없이 지내야만 하였다. 왜냐하면, 각 주별로 의료보험의 기준이 제 각각 달랐기 때문이다.[6] 그리고, 의료보험을 각 주별로 이전한다는 것은 건강정보를 전자적으로 전송하기 위한 전국적 통일기준을 정립하여 비용을 절감한다는 것을 의미하며,[7] 개인건강정보를 포함하고 있는 의료보험의 표준화·안전한 보호 및 프라이버시 보호 등 개인건강정보의 전자적 이전과 관련한 제반 사항들에 관한 규제가 필요하다는 것을 동시에 의미하기도 한다.[8] 실제로, HIPAA의 의료보

---

5) HIPAA는 고용주, 의료기관, 의료보험업자에게는 개인건강정보가 이용되고 공개되는 방법을 근본적으로 변화시킴으로써, 근로자들에게는 실직하거나 직장을 옮기더라도 이전 의료보험을 훨씬 더 쉽게 유지할 수 있도록 하는 이전가능성을 통해 영향력을 미치게 된다. Nick Littlefield & Colin Zick, “HIPAA: New Federal Privacy Rules and Their Implications”, 46-OCT B. B.J. 14 (September-October, 2002).

6) HIPAA는 직장의 이동문제(전직)에 관한 관심에 대한 연방의회의 결과물로서 의료보험의 이전가능성 문제에 중점을 두었다. 참고로, 1995년 현재 85% 이상 의료보험이 직장보험이다. 그리고, 직장선택에 있어서 의료보험의 이익이 매우 중요한 기준이 된다. 예컨대, 의료보험을 제외한 모든 면에서 A 기업이 낫다고 하더라도 의료보험이 좋은 B 기업을 선택하기도 한다. 이를 “job lock” 라고 하기도 한다. Rebecca Lewin, “Job Lock: Will HIPAA Solve The Job Mobility Problem?”, 2 UPAJLEL 507, 507-08 (Winter 2000).

7) 건강정보의 전자적 교환은 개인과 미국 의료보험체계에 향상된 의료보호와 감소된 비용을 통해 잠재적 이익을 약속한다. U.S. Department of Health and Human Services, Office of the National Coordinator for Health Information Technology, Nationwide Privacy and Security Framework For Electronic Exchange of Individually Identifiable Health Information 1 (December 15, 2008).

8) 수십년 동안 각 주는 건강정보의 프라이버시를 보호하기 위해 법을 제정하여 시행해 오고 있다. 이러한 법들은 주마다 다르고 특정 인구집단, 건강 상태, 데이터 수집 노력, 또는 특별한 형태의 건강보호기관들만을 목표로 하는 경우도 많았다. 그 결과, 각

험의 이전에 관한 행정사무의 간소화 조항들이 이러한 규제를 위한 근거로 작용한다. 즉, HIPAA는 의료보험의 이전에 따른 비용을 줄이고, 개인식별 가능한 건강정보의 공개와 이 정보에 대한 기망과 승인받지 않은 접근을 방지하여 개인건강정보의 비밀을 보장하고, 건강정보의 전자적 교환을 단순하게 하는 것을 그 목적으로 한다.[9)]

2. HIPAA 행정사무 간소화 조항

HIPAA의 조항들은 i) 전자적 전달과 데이터 해독을 위해 사용되는 코드셋(의료비청구와 관련하여 의료계에서는 서로 다른 전자적 양식과 데이터의 개념을 사용하였는데, 연방의회는 이를 통일함으로써 처리시간 감소/데이터질 향상/행정적 비용 감축이 가능하도록 의도함. 보건복지부장관은 2000. 4. 17 최종규칙을 공포하여 대규모 의료계는 2002. 10. 16까지, 소규모 의료계는 2003. 10. 16까지 양식과 개념을 통일하도록 함. 42 U.S.C. § 1173(a)(c)), ii) 고유식별표지(실수와 행정적 비용을 줄이기 위해 각 의료기관별로 고유명칭을 사용하도록 하였고, 2004. 1. 23에 보건복지부장관이 최종규칙을 공포함. 2005. 5. 23부터 효력을 발생하였고, 준수기한은 2007. 5. 23(소규모는 2008. 5. 23)까지임. 이후에 전자적 양식으로 건강정보를 전송하는 모든 '프라이버시룰의 적용대상자'(Covered Entities, 이하 '정보처리자'라 함)는 이 규칙을 준수하여야 함. 42 U.S.C. § 1173(b)), iii) 보안(전자적으로 보호된 건강정보의 통일성과 기밀성을 보장하기 위해 보건복지부장관이 2003. 2. 20 최종규칙(Security Rule, 45 C.F.R. §§

주는 종합적이지도 쉽게 이해될 수도 없는 프라이버시 보호를 만들어 내고 있었다. 많은 주들은 또한 정보의 보안과 관련된 이슈들을 고려하기 시작하여 개인식별 가능한 정보에 관한 보안위반을 고지하도록 다양한 기관들에 요구하는 법들을 제정하여 시행하고 있다. 연방차원에서는 건강정보의 프라이버시 보호와 보안에 관련한 HIPAA Privacy Rule과 Security Rule, Privacy Act of 1974, Confidentiality of Alcohol and Drug Abuse Patient Records Regulation (42 CFR Part 2), Family Educational Rights & Privacy Act (특정 교육기관들이 가지고 있는 정보의 프라이버시를 다룸), Gramm-Leach-Bliley Financial Services Act (금융기관들이 가지고 있는 정보의 프라이버시를 다룸), Federal Information Security Management Act of 2002와 같은 다양한 법들이 존재한다. Id. at 2-3.

9) 백윤철·김상겸, 앞의 책, 21-22쪽과 필자의 의견을 첨부함.

160, 162, and 164.302 (2006))을 공포하였고 2003. 4. 21부터 효력을 발생함. 42 U.S.C. § 1173(d)), iv) 프라이버시(Privacy Rule, 45 C.F.R. §§ 160, 164.102-500 (2006). 42 U.S.C. § 264)에 관한 사항들을 규정하여 각각에 대한 기준과 규칙을 제정할 수 있는 권한을 보건복지부장관에게 부여하는 것을 명확히 규정하였다. 특히, 프라이버시룰을 준수하지 못할 경우에는 민사벌(42 U.S.C. § 1176)과 형사벌(42 U.S.C. § 1177)이 부과될 수 있도록 강제집행규칙(Enforcement Rule, 45 C.F.R. § 160 (2006))이 제정되었다.[10)]

3. HIPAA의 최근 변경: HITECH Act

그런데, 글로벌화의 증가와 대량의 전자기록 시스템화에 따라, 개인건강정보에 관한 프라이버시와 보안장치를 강화하는 것이 중요하다고 판단되어, 연방의회는 American Recovery and Reinvestment Act of 2009의 일부로 2009년 2월 17일 Health Information Technology for Economic and Clinical Health Act (HITECH Act; Pub. L. No. 111-5 13410(d), 123 Stat. 115 (2009))를 제정하였다. HITECH Act는 전자적 건강기록 작성을 전국적으로 채택하는 것을 촉진하기 위한 법이고 (2014년까지 전국환자전자기록시스템 구축), 이 목적을 달성하기 위해 전자적 건강기록 작성을 위한 프라이버시와 보안을 변경하고 강화하였다. 이러한 HITECH Act의 제정으로 HIPAA는 많은 영향을 받게 되었다. 특히, HIPAA 위반에 대해 더 엄격한 민사 및 형사벌을 부과하기 위해 강제집행조항들을 강화하여 2009년 10월 30일 강제집행규칙을 제정하였다.

그 결과, 정보처리자가 프라이버시룰을 준수하지 않을 경우 민사 및 형사벌을 부과하기 보다는 자발적으로 이를 준수하도록 돕기 위해 기술적

10) Elizabeth Hutton, Devin Barry, “Privacy Year In Review: Developments In HIPAA”, 1 I/S: J. L. & Pol'y for Info. Soc'y 347, 347-355 (Spring/Summer, 2005). 그리고, HIPAA, Privacy Rule, Security Rule, Enforcement Rule을 묶어 HIPAA라 명명하기도 한다. Inside The Minds, Recent Developments With HIPAA, Thomson Reuters/Aspatore, 2010, p. 20. 그러나, 이 논문에서는 HIPAA는 법률로, Privacy Rule, Security Rule, Enforcement Rule은 규칙(=법규명령)으로 서로 구분하여 사용하기로 한다.

지원을 제공하던 종래의 협력적 강제집행 모델(corroborative enforcement model)[11]은 사라지고, 정보처리자가 프라이버시룰을 준수하지 않을 경우 바로 민사 및 형사벌을 부과하도록 하는 엄격한 강제집행(gloves-off enforcement)[12]

11) 2004년 7월 31일까지 보건복지부 시민권국(Office for Civil Rights, OCR)은 프라이버시룰 위반으로 7,577건을 접수하여 조사를 개시하였지만, 100건 정도만 형사벌 부과를 위해 법무부에 넘겼을뿐, 단 한건의 민사벌도 부과하지 않았다. 민사금전벌은 OCR이 부과한다. OCR의 강제집행 전략은 벌금부과가 아니라 자발적 준수와 교육에 중점을 두었고, OCR이 접수한 프라이버시 관련 위반 이유는 ① 건강정보를 승인받지 않고 공개, ② 건강정보의 승인받지 않은 이용을 예방하기 위한 충분한 안전장치의 결여, ③ 환자들로 하여금 자신들의 의료기록에 접근하는 것을 허용하지 못하게 한 경우, ④ 건강정보의 공개를 위한 필요최소한의 원칙을 위반한 경우 등이었다. Id. at 355. 민사금전벌은 위반 건 당 $100, 년 $25,000 이하이지만, ① 합리적 이유로 인한 경우, ② 고의적인 태만이 없는 경우, ③ 위반을 안날로부터 또는 위반을 알았었을 날로부터 30일 이내에 위반이 교정된 경우에는 민사금전벌을 부과하지 않는다.

12) HITECH Act 제정 이후 프라이버시룰 위반에 대해서는 다음과 같은 4가지 경우가 적용된다: ① 정보처리자가 어떤 조항을 위반하였다는 것을 몰랐고 합리적 주의를 다하더라도 알 수 없었을 경우 위반 건 당 $100 이상 $50,000 이하. ② 위반이 고의적 태만이 아니라 합리적 원인에 기인한 경우 위반 건 당 $1,000 이상 $50,000 이하. ③ 위반이 고의적 태만에 기인하였지만 적시에 정정된 경우 위반 건 당 $10,000 이상 $50,000 이하. ④ 위반이 고의적 태만이고 적시에 정정되지 않은 경우 위반 건 당 $50,000 이상. 단, 동일한 요건이나 금지의 위반에 대한 민사금전벌은 년간 1백 5십만 달러를 초과할 수 없다(45 C.F.R. § 160.404). 정보처리자가 몰랐다고 하는 것이 이전에는 면책이었으나 개정규칙에서는 면책이 아니다. 그럼으로써 정보처리자의 대행인의 위반에 대해 정보처리자에게 책임을 부과하게 된다. 그러나, 개정규칙은 고의적 태만이 아니고 30일 이내에 교정되는 위반에 대해서는 새로운 면책사유로 신설하였다(45 C.F.R. § 160.410). 형사벌은 이전과 마찬가지로 법무부가 부과한다. 벌금형과 징역형을 동시에 부과할 수 있다. 고의로 HIPAA를 위반하여 PHI를 획득하거나 공개한 사람은 벌금 $50,000과 최고 1년 징역. 기망에 의한 위반인 경우에는 벌금 $100,000과 최고 징역 5년. 상업적 이득/개인적 이득/또는 악의적 해악을 위해 PHI를 판매/이전/이용한 경우에는 벌금 $250,000과 최고 징역 10년을 부과한다. 다음은 벌칙부과에 관한 실제 사례들이다: ① Providence Health System 사건: PHI를 저장하고 있던 랩탑컴퓨터 등을 직원이 건물 밖으로 가지고 나간 5건의 사건에 따라 보건복지부와 2008년 7월 15일 분쟁해결협약을 체결하여 직원재교육, 정책과 절차 개정, 자체감시 강화 등을 실행하도록 요구. 이를 제대로 이행하지 못할 경우 $100,000+벌금을 내도록 약속함. ② CVS 사건: CVS 소속 약국에서 환자와 종업원의 민감한 자료를 부적절하게 폐기처분한 것에 대한 보건복지부와 연방거래위원회의 합동조사에 따라 2009년 2월 18일 HIPAA 위반에 대한 고발의 합의금으로 2백 2십 5만 달러 지불하고 추가로 회사의 약 6,000개 이상의 소매약국들이 정보를 폐기처분하는 정책과 절차를 정립하고 집행, 훈련프로그램 집행, 내부 모니터링 수행, 3년 간 준수를 평가하기 위해 외부 평가자 고용 등의 의무를 이행하도록 한 사건. ③ Rite Aid 사건: 2010년 7월 27일 Rite Aid 소속 약국이 처방전과 사용설명서가 부착된 약병을 부적절하게 폐기처분하여 HIPAA를 위반한 사실에 합의하기 위해 연방정부에

으로 바뀌었다. 또한, 최초 프라이버시룰에서 규정했던 '정보처리 대행인'(Business Associates, 이하 '대행인'이라 함)의 개념과 적용범위를 전면적으로 개정한 프라이버시룰안(Proposed Privacy Rule)을 2010년 7월 15일 마련하였다. 이에 따라 대행인은 정보처리자로 간주되어 프라이버시룰의 적용대상정보인 「보호된 건강정보」(Protected Health Information, 이하 'PHI'라 함)의 위반에 대해 정보처리자와 대행인 모두 고지하여야 하는 의무를 부과하였다.

Ⅲ. 프라이버시룰의 개관 및 내용

HIPAA를 근거법으로 하여 보건복지부장관은 개인건강정보의 이용 및 공개의 주체·방법·범위·시기 등에 관한 법규명령인 프라이버시룰을 2002년 8월 14일 제정하여 2003년 4월 14일부터 효력을 발생하게 하였다(소규모 대상자들에 대해서는 2004년 4월 14일부터 효력 발생). 프라이버시룰은 건강정보의 프라이버시를 광범위하게 다룬 연방 최초의 규정이고, 정보처리자가 가지고 있는 개인식별 가능한 건강정보를 위한 전국적 프라이버시 기준을 정립하고 건강상태, 건강프로그램 유형, 인구, 행위가 발생하는 주, 또는 그밖의 상황적 특징과는 상관없이 보호를 제공한다.[13] 연구와 관련하여, 프라이버시룰은 피험자 스크리닝과 모집, 의료기록과 그밖의 기존 건강정보에의 접근, 건강정보의 수집·창출·수령, 새로운 데이터베이스 또는 조직은행 구축, 기존 데이터베이스와 조직은행의 사용, 현장 모니터링, 다기관 연구의 관리와 결과의 발표 등 건강정보의 이용과 공개에 의한 모든 연구에 적용된다. 또한, 연구를 효율적으로 진행하기 위해서는 연구에 관련된 정보처리자를 포함한 모든 당사자들은 프라이버시룰이 건강정보의 이용 또는 공개에 어떤 영향을 미치는가를 이해하여

1백만 달러를 지불하고 추가로 보건복지부와 교정조치 프로그램에 합의하고 연방거래위원회도 향후 20년 간 외부 검사자에 의해 2년 마다 모니터되어야 하는 종합정보보안 프로그램의 적용을 받도록 하는 동의명령(consent order)을 부과한 사건. 이에 대한 자세한 내용은, Inside The Minds, *supra* note 10, at 52-54.

13) U.S. Department of Health and Human Services, *supra* note 7, at 3.

야 한다. 예컨대, 정보처리자는 프라이버시룰의 비준수에 따른 법적 책임을 최소화하기 위해, 그리고 연구계획서를 작성하는 의뢰자는 연구계획서에서 정보처리자의 PHI의 이용 또는 공개와 관련한 프라이버시룰의 요구사항들을 명확히 밝혀야 한다.[14] 이하에서 개인건강정보의 보호에 적용되는 프라이버시룰의 일반적 내용과 연구에 참여하는 피험자의 건강정보의 보호에 적용될 수 있는 내용 등을 고찰한다.

1. 프라이버시룰의 목적

개인식별가능한 건강정보에 관한 프라이버시를 안전하게 하기 위한 최소한의 연방기준을 정립하고, PHI가 정보처리자에 의해 이용되거나 공개될 수 있는 범위를 정하는 것이 프라이버시룰의 주된 목적이다. 즉, 양질의 헬스케어를 제공·촉진하고 일반 공중의 건강과 웰빙을 보호하기 위해 필요로 하는 건강정보의 이동을 허용하는 동시에 개인의 건강정보가 적절히 보호되도록 보장하는 것이다. 결과적으로, 프라이버시룰은 정보처리자로 하여금 정보주체의 PHI의 이용 또는 공개를 하도록 허용하는 것과 정보주체의 프라이버시를 보호하는 것 간의 균형을 도모하는 것이라 할 수 있다.

2. 프라이버시룰의 적용대상자

프라이버시룰의 적용을 받는 자를 정보처리자라 하고, 의료보험기관, 의료기관 등 의료제공자, 의료정보교환사업자만이 정보처리자로서 프라이버시룰의 적용을 받는다(45 C.F.R. § 160.103). 따라서, 정보처리자는 연구목적을 위해 PHI를 수령, 이용 또는 공개하려면 프라이버시룰의 요건에 따라야 한다. 그리고, 연구에 있어서 정보처리자에 해당하는지 여부를 결정하는 것은 매우 중요하다. 왜냐하면, 프라이버시룰은 PHI의 이용과 PHI의 공개에 각기 다른 요건을 적용하고 있기 때문이다. PHI의 이용은 정보처리자 또는 구성원이 정보처리자 내부에서 PHI를 수집·심사·분석 등

14) Dunn & Chadwick, *supra* note 3, at 148.

을 하는 것이고, PHI의 공개는 정보처리자가 PHI를 정보처리자 외부 사람이나 기관에 공유·배포 또는 이전할 때 발생한다. PHI의 공개에 해당할 경우에는 추적요건을 준수하여 행정적 부담을 야기하지만, PHI의 이용의 경우에는 이런 적용을 받지 않는다. 예컨대, 병원이나 연구소와 같은 기관이 정보처리자인 경우, 담당 부서의 기능적 성격에 따라 프라이버시룰의 적용을 받을 수도 받지 않을 수도 있다. 만약 해당 부서가 정보처리자로서 프라이버시룰의 적용을 받으면, 연구에서 PHI의 공유는 이용에 해당한다. 또한, 프라이버시룰의 적용을 받게 되면, 정보처리자인 부서와 정보처리자가 아닌 부서 간에 PHI를 승인없이 공유할 수 없도록 하여 피험자의 프라이버시를 보호하고, 정보주체에 대한 프라이버시실행의 사전고지를 정보처리자에게만 의무지움으로써 사전고지를 단순화 할 수 있는 장점이 있다.[15] 정보처리자와 관련하여, BA의 문제가 또한 중요하게 거론된다. 정보처리자를 대신하여 PHI의 이용 또는 공개, PHI의 개인식별불능화(de-identifying), limited data sets 준비, 데이터 수집 등을 포함하는 기능 또는 활동을 수행하거나 수행을 돕는 정보처리자의 구성원이 아닌 개인 또는 기관을 대행인이라 한다. 정보처리자는 대행인과의 계약을 통해 PHI를 대행인에게 공개할 수 있다. 프라이버시룰은 그 계약에 ① 대행인에 의해 허용되거나 요구된 PHI의 이용과 공개의 범위, ② 대행인은 정보처리자가 프라이버시룰에 따라 허용되어지는 대로만 PHI를 이용/공개할 수 있다는 사실, ③ PHI의 프라이버시와 안전을 보호하기 위한 적절한 안전장치 사용, ④ 계약 만료시에 정보처리자에게 PHI를 돌려주거나

15) 기관 정보처리자에는 다음의 세가지 종류가 있다: ① Hybrid Entities (HE): 단일 법적 기관이지만 내부적으로 프라이버시룰의 적용을 받는 헬스케어 부서와 받지 않는 비헬스케어 부서를 구별해 두고 있는 것. 헬스케어 부서 내에서 PHI를 공유하는 것은 이용에 해당하고, 비헬스케어 부서와 공유하는 것은 공개에 해당함. 대학, 복합부서로 구성된 병원, 비영리 연구기관 등이 여기에 해당함, ② Affiliated Covered Entities (ACE): 법적으로는 별개이지만 복수 기관들이 단일 정보처리자로서 기능하는 것. 주관기관과 협력기관의 관계가 여기에 해당함. PHI를 이들 기관 내에서 공유하는 것은 이용에 해당함. 각 구성 기관은 단일의 프라이버시실행의 사전고지를 할 수 있음. ③ Organized Health Care Arrangements (OHCA): 개개의 기관이 독립된 정보처리자지만 일반인들에게는 통합된 의료서비스를 제공하는 것으로 보일 경우이고, 기관 간 PHI의 공유는 공개에 해당함. 각 구성 기관은 단일의 프라이버시실행의 사전고지를 할 수 있음. Dunn & Chadwick, *supra* note 3, at 159.

폐기하기 등의 내용이 포함되도록 요구한다(45 C.F.R. §§ 160.103, 164.502(e), 164.504(c)).[16] 그리고, 연구에 있어서 의뢰자나 임상시험수탁기관의 피용인은 의뢰자를 대신하기 때문에 대행인 아니며, 다른 장소에 있는 연구자와 같은 연구 협력자들도 연구목적을 위해 PHI를 공유하는 것이 연구자와 대행인 관계를 창설하지는 않기 때문에 대행인이 아니다. 또한, 연구와 관련하여, 프라이버시룰은 연구자 또는 의뢰자로 하여금 정보처리자의 대행인으로 될 것을 요구하지도 않는다.[17] 다만, 프라이버시룰안에서는 대행인도 정보처리자에 해당한다고 규정하고 있다.

3. 프라이버시룰의 적용대상 정보

프라이버시룰의 적용을 받는 정보는 정보처리자에 의해 창출되거나 수령된 개인식별가능한 건강정보이며, 이것을 PHI라 한다(45 C.F.R. § 160.103).[18] 즉, PHI로 되기 위해서는 건강정보가 정보처리자에 의해 창출되거나 수령되어야 하고 동시에 개인식별가능해야 한다. '개인식별가능한'이란 개인을 직접적으로 식별하거나 식별하는데 합리적으로 사용될 수 있는 경우를 말하며, 18개의 식별표지를 프라이버시룰에서 구체적으로 규정해 두고 있고 이 중 어느 하나라도 있으면 직접적으로 개인을 식별할 수 있게 된다(이름, 전화번호, 팩스번호, 주민등록번호 등. 45 C.F.R. § 164.514(b)(2)(i)). 특히, 18번째 식별표지인 'any other unique identifying number, characteristic or code'는 catchall category로 작용하고, 1-17번 식별표지에 해당하지 않더라도 주민등록번호 뒷자리나 임상시험기록번호와 같은 'identifying code'(다른 정보와 결합하여 정보주체를 식별하기 위해

16) 만약 대행인이 그 정보를 적절하게 안전보장을 할 것이라는 충분한 보증서를 정보처리자가 획득한다면, 정보처리자는 PHI를 대행인에게 공개할 수 있고 대행인으로 하여금 정보처리자 대신에 PHI를 수령하거나 만들어 낼 수 있도록 허용한다(45 C.F.R. § 164.502(e)).

17) U.S. Department of Health and Human Services, Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule 7. http://privacyruleandresearch.nih.gov 참조.

18) 그러나, Family Educational Rights and Privacy Act의 적용을 받는 교육기록(education records)(20 U.S.C. 1232g), 20 U.S.C. 1232g(a)(4)(B)(iv)에 규정된 기록들, 그리고 고용주 역할을 하는 정보처리자에 의해 보관된 고용기록은 PHI에서 제외된다.

사용되는 코드)를 이용하여 다른 식별표지와 결합해서 정보주체를 식별할 수 있으면 이는 PHI로 된다. 예컨대, 혈액이나 조직과 같은 인체유래물은 그 자체로는 PHI가 아니지만, 건강정보인 진단정보와 함께 조직은행에 수집/저장될 때에는 프라이버시룰의 18개 식별표지 중 어느 하나에 해당될 경우 개인식별가능하게 되고 이것이 정보처리자에 의해 사용되면 PHI에 해당하게 된다. 인체유래물이 PHI인지 아닌지 여부는 기존 검체를 연구하고 검체은행을 설립하거나 유지하는데 있어서 매우 중요하다. 그리고, 이 18개 식별표지는 프라이버시룰의 요건을 준수할 경우 연구를 위해서 공개될 수도 있다. 또한, 임상시험의 결과가 기재된 환자증례기록서가 18개 개인식별표지에 해당하는지 프라이버시룰에서 신중하게 검토되어야 한다. 만약, 연구자가 임상시험수탁기관이나 의뢰자와 같은 외부 관계인들에게 정보주체의 승인을 얻어 PHI를 공개할 경우에는 환자증례기록서는 PHI를 포함하고 있을 수 있다. 이럴 경우 환자증례기록서와 정보주체의 승인은 일치하여야 하고, 환자증례기록서에 포함되어 있는 어떠한 PHI라도 정보주체의 승인에서 특정되어야 한다. 그밖에, 연구와 관련하여 연구자들은 기존 데이터나 검체를 연구할 경우에는 PHI가 아니라 de-identified data를 사용할 수 있고 이것은 프라이버시룰의 적용대상이 아니다. PHI를 개인식별불가능하게 하는 것은 정보처리자의 책임이며, 연구자는 정보처리자로부터 de-identified data를 수령하여 연구할 수 있다.[19] 또한, 연구자들은 역학연구를 할 때 de-identified data와 PHI 중간에 해당하는 최소한의 개인식별표지를 지닌 건강정보인 limited data sets를 사용할 수도 있다. limited data sets는 정보주체 또는 친척, 고용주, 정보주체의 가족구성원의 이름 등 18개 개인식별표지 중 거리 주소를 삭제한 주소, 날짜, 18번째 식별표지만 기재된 정보로서 연구, 공중보건, 또는 의료업무관리 목적으로만 사용될 수 있다(45 C.F.R. § 164.514(e)(3)(i)). 정보처리자

19) 개인식별 불가능한 정보는 개인을 식별하지 못하는 건강정보와 그 정보가 개인을 식별하는데 사용될 수 있는 합리적 근거가 없는 건강정보를 말한다(45 C.F.R. § 164.514(a)). 개인식별 불가능한 정보가 되기 위해서는 1. 정보주체, 친척, 고용주, 가족구성원 등의 이름, 주민등록번호, 전화번호 등 18개 식별표지를 제거하는 것. 2. 통계학적 방법으로 개인을 식별할 수 없도록 하여 그 증명서를 6년간 보관하는 것의 방법이 있다(45 C.F.R. § 164.514(b).

는 연구자와 자료이용협약을 체결하여 limited data sets를 공개할 수 있다.[20] 보건복지부는 limited data sets를 프라이버시룰의 적용을 받지 않아 자유롭게 이용과 공개할 수 있는 de-identified data와 정보주체의 승인을 받아야만 이용과 공개할 수 있는 PHI의 중간에 위치시킴으로써 프라이버시 보호와 매우 가치있는 역학연구를 허용하는 것 사이의 균형을 꾀하려 노력한다.

4. PHI의 이용과 공개

프라이버시룰은 앞서 언급한 바와 같이 연구뿐만 아니라 건강정보를 사용하는 모든 영역에 적용된다. 여기서는 정보처리자가 PHI를 이용하거나 공개할 때에 적용되는 프라이버시룰의 요건인 일반원칙과 특별히 연구에서의 PHI의 이용 및 공개를 구분하여 고찰한다. 다만, 기술의 편의상 일반원칙에서도 연구에 관련되는 내용은 필요에 따라 해당 부분에서 언급하기로 한다.

(1) 일반원칙(45 C.F.R. § 164.502)

프라이버시룰에서 달리 규정하고 있지 않으면 정보처리자는 정보주체의 서면승인을 받아야 PHI를 이용하거나 공개할 수 있다. 그리고 PHI의 이용이나 공개의 범위는 정보주체의 승인에서 정한 바에 따른다.[21] 그러

20) 자료이용협약은 limited data sets가 어떻게 사용될 것인가에 대한 서술, limited data sets에 접근할 수 있는 사람들의 확정, limited data sets를 수령하는 사람들의 책임(피험자 모집을 위해 사용하지 않을 것 또는 정보주체를 다른 사람들에게 식별되도록 하지 않을 것, 어떠한 부적절한 이용/공개라도 정보처리자에게 보고할 것, 자료이용협약의 범위를 벗어난 이용/공개하지 않을 적절한 안전판을 사용할 것 등)을 포함하여야 한다. Dunn & Chadwick, *supra* note 3, at 164.

21) 정보처리자는 헬스케어와 관련한 의사결정을 하는데 있어서 성인, 법적으로 독립한 미성년자, 사망한 자를 법적으로 대신할 권리가 있는 자를 대리인으로 간주하여 정보주체로 취급하여야 한다. 다만, 법적으로 독립하지 못한 미성년자의 경우에는 부모나 후견인을 헬스케어와 관련한 의사결정을 하는데 있어서 대리인으로 간주한다. 또한, 정보처리자는 아동학대, 방치, 가정폭력 등을 행사한다고 합리적 믿음을 가지고 정보주체의 최상의 이익이 아니라고 결정하면 그 사람을 정보주체의 대리인으로 취급하지 않을 수도 있다(45 C.F.R. § 164.502(g)). 그리고, 정보처리자의 근로자들 가운데 한 사람이 또는 대행인이 내부고발자로서 PHI를 공개할 경우와 정보처리자의

나, ① 정보주체에게 공개할 경우, ② TPO를 위한 경우(45 C.F.R. § 164.506)[22], ③ 정보처리자가 병원에서 정보주체의 디렉토리(환자성명, 나이, 성별, 증상 등 기재)를 유지하기 위해 PHI 이용 또는 공개에 관한 동의 또는 반대 기회를 정보주체에게 제공한 경우(45 C.F.R. § 164.510), ④ 정보주체의 승인이나 PHI 이용 또는 공개에 관한 동의 또는 반대 기회의 제공이 필요없는 이용 또는 공개의 경우(45 C.F.R. § 164.512)[23]에는 정보주체의 서면승인을 받지 않고서 정보처리자가 PHI를 이용 및 공개할 수 있다. 특히, 정신병상담 노트의 이용 또는 공개와 PHI의 마켓팅[24]의 경우에는 반드시 정보주체의 승인을 받아야 한다. 다만, ① 상담에 따른 TPO를 하는 경우, ② 보건복지부가 프라이버시룰의 준수 여부 조사·심사·강제집행을 행할 때, ③ 법에 의해 요구될 때, ④ 보건감시활동을 위한 경

근로자들 가운데 범죄행위의 피해자인 사람이 PHI를 법집행 공무원에게 공개한 경우에는 정보처리자가 프라이버시룰을 위반했다고 간주되지는 않는다(45 C.F.R. § 164.502(j)).

22) TPO는 Treatment, Payment, Health Care Operations를 말한다. Treatment는 의료기관의 의료관련서비스를 말함(예: 의료기관의 환자에 대한 의료서비스 조정/관리, 환자와 관련한 의료기관들 간의 조언/자문, 의료기관들 간 환자의 이송/의료서비스 제공/조정/관리 등). Payment는 의료관련서비스 비용에 대한 의료기관 또는 의료보험회사의 일련의 금전관련 행위를 말함(예: 보험료를 받기 위한 또는 의료보험에 따른 보험보장범위와 보험금의 제공을 결정하는 의료보험회사의 행위. 의료관련서비스 제공에 대한 댓가를 구하거나 제공하기 위한 의료기관 또는 의료보험회사의 행위 등). Health Care Operations는 의료업무관리를 말함. 이에 대한 자세한 내용은 45 C.F.R. § 164.501 참조.

23) 법에 의해 요구된 이용 또는 공개, 공중보건 활동을 위한 이용 또는 공개, 아동학대/방치/가정폭력의 희생자라고 정보처리자가 합리적으로 믿는 경우 정부기관에 그들에 관한 PHI 공개, 보건감시활동을 위한 이용과 공개, 사법적·행정적 절차를 위한 공개, 법의 강제집행을 위한 공개, 사망한 자의 신원확인이나 장례 등을 위해 검시관과 장의사에게 이용과 공개, 사체의 장기/안구/조직 기증 목적을 위한 이용과 공개, 임상시험심사위원회나 프라이버시보호위원회(Privacy Board)로부터 승인면제를 받은 연구를 위한 이용과 공개, 연구준비를 위한 심사에 있어서 이용과 공개, 사망한 자의 정보에 관한 연구를 위한 이용과 공개, 보건이나 안전에 대한 심각한 위협을 방지하거나 감경할 필요가 있다고 정보처리자가 선의로 믿는 경우의 이용과 공개, 군대나 국방 등 특별한 정부활동을 위한 이용과 공개, 근로자 보상을 위한 공개 등은 정보주체의 승인이나 PHI 이용 또는 공개에 관한 동의 또는 반대 기회의 제공이 필요없는 이용 또는 공개의 경우에 해당된다.

24) 마켓팅(marketing)은 수령자로 하여금 그 제품이나 서비스를 구입하거나 이용하도록 권장하는 제품이나 서비스에 관한 모든 의사소통을 의미한다(45 C.F.R. §§ 164.501 and 164.508(a)(3)).

우에는 승인없이 정신병상담 노트를 이용 및 공개할 수 있다. 마켓팅의 경우에도 소통의 형식이 정보처리자가 정보주체와 면대면 소통을 하는 경우와 정보처리자에 의해 제공된 통상적 가치의 판촉용 선물인 경우에는 승인없이 PHI를 마켓팅을 위해 이용 및 공개할 수 있다. 그리고, 연구와 관련한 피험자의 승인은 특정되어야 하여 복합승인(compound authorizations)은 원칙적으로 허용되지 않는다. 예컨대, 연구에 참여하는 피험자의 건강정보를 이용이나 공개할 경우에는 연구에 참여한다는 동의서와 PHI의 이용이나 공개를 허용하는 승인서를 각각 받아야 하는 것이지,[25] 이 양자를 결합하고 있는 문서인 복합승인은 원칙적으로 허용되지 않는다. 다만, 연구를 위한 정보주체의 PHI 이용이나 공개에 관한 승인이 연구종료시까지 유효한 경우, 만료되는 날짜나 사항이 없는 경우, 또는 임상연구 참여 동의를 조건으로 PHI의 공개를 승인받고자 할 경우에는 임상연구에 참여하는 동의와 PHI를 공개하는 승인을 함께 포함하고 있는 문서인 복합승인이 허용된다(45 C.F.R. § 164.508(b)(3)). 정보처리자가 PHI의 이용과 공개를 할 경우에는 정보주체의 서면승인을 받아야 한다는 일반원칙을 구체적으로 실행하기 위해, 프라이버시룰은 프라이버시실행의 사전고지, 필요최소한의 원칙, 정보주체의 권리 등을 규정하여 정보주체의 프라이버시보호를 위한 기준으로 삼고 있다.

25) 임상시험에 참여한다는 충분한 설명에 의한 동의와 프라이버시룰의 승인은 구분되는 개념이다. 전자는 피험자에게 연구내용에 대한 기술, 예상 위험과 편익, 기록의 비밀성이 어떻게 보호될 것인가에 관한 기술 등을 제공한다. 후자는 프라이버시의 위험에 관해 중점을 두고 있고 PHI가 연구를 위해 어떻게, 어떤 이유로, 누구에게 이용 및 공개될 것인가를 진술한다. 그리고, 프라이버시룰의 승인에는 핵심요소(구체적이고 의미있는 방법으로 이용이나 공개되는 PHI에 관한 기술, 이용이나 공개를 하도록 승인된 사람의 이름이나 구체적 식별표지, 정보처리자가 이용이나 공개를 할 수 있는 사람의 이름이나 구체적 식별표지, 이용이나 공개의 각각의 목적 기술, 정보주체와 관련된 또는 이용이나 공개와 관련된 승인종료일이나 종료사항, 정보주체의 서명과 날짜)와 필수 진술서(승인의 철회권과 철회방법에 관한 정보주체의 권리에 관한 진술서, 치료/의료비지급/등록/편익의 수령적격성이 승인에 좌우될 수 있는지 여부에 관한 진술서, PHI가 수령자에 의해 재공개될 것이라는 잠재적 위험에 관한 진술서)를 포함하여야 한다. U.S. Department of Health and Human Services, *supra* note 17, at 11-12.

1) 프라이버시 사전고지(Notice of Privacy Practices, NPP)

정보처리자는 정보주체의 프라이버시와 관련하여 사전고지를 해야 하고, 사전고지에는 PHI의 이용과 공개 방법이 기술되어야 하며 그러한 사전고지와 일치하지 않는 방법으로 PHI를 이용하거나 공개할 수 없다(45 C.F.R. § 164.502(i)). 사전고지는 정보주체의 프라이버시를 보호하기 위한 정보처리자의 의무를 기술하여야 하고, 프라이버시의 내용에 관한 고지를 제공하여야 하고, 현행 고지 조건을 준수하여야 한다. 또한, 보건복지부와 정보처리자에 대한 이의신청권과 같은 정보주체의 권리와 정보처리자의 준수 의무를 사전고지는 기술하여야 한다. 다만, 직장의료보험에 가입한 정보주체와 재소자인 정보주체는 사전고지를 받을 권리가 없다(45 C.F.R. § 164.520(a)). 연구와 관련하여, 사전고지에는 피험자 스크리닝/모집/기존 데이터베이스와 조직은행의 분석에는 정보주체의 승인없이 PHI 이용과 공개가 가능하다는 것을 기술하여야 한다.

2) 필요최소한의 원칙

정보처리자가 PHI를 이용 또는 공개할 때 내지 다른 정보처리자로부터 PHI의 이용 또는 공개 요청을 받았을 때, 이용/공개/또는 요청에 관한 의도된 목적을 달성하기 위해 필요한 최소한도로 PHI를 제한하도록 합리적 노력을 하여야 하는 것을 필요최소한의 원칙이라 한다. 필요최소한의 원칙을 준수하여 정보처리자는 정보주체의 PHI의 이용과 공개를 할 수 있다. 단, 다음과 같은 경우에는 이 원칙이 적용되지 않는다: ① 치료목적으로 의료제공자에게 공개하거나 치료목적을 위한 의료제공자의 요청에 의한 경우, ② 정보주체나 대리인에게 공개하는 경우, ③ 45 C.F.R. § 164.508에 따른 정보주체의 승인에 의한 이용이나 공개인 경우, ④ 이의신청의 조사, 준수심사 또는 강제집행을 위해 보건복지부에 공개하는 경우, ⑤ 법에 의해 이용이나 공개가 요구되는 경우, 또는 ⑥ HIPAA Rules의 준수를 위해 요구된 이용이나 공개인 경우.

3) 정보주체의 권리

정보주체의 권리는 자신의 PHI의 이용과 공개에 관한 것으로 프라이버시실행의 사전고지를 요청함으로써 보장된다. 정보처리자는 평이하게 작성된 문서로 PHI에 관한 정보주체의 권리, 정보처리자의 법적 의무, 정보주체의 이의제기절차, 연락처, 고지의 효력발생일 등이 기술된 사전고지서를 제공하여야 한다(45 C.F.R. § 164.520). 정보주체의 권리는 다음과 같다:

① PHI의 이용이나 공개의 제한요청권

정보주체는 자신의 PHI의 이용이나 공개에 대한 제한을 정보처리자에 요청할 수 있다. 즉, 정보주체는 TPO를 위한 경우, 정보주체의 헬스케어에 관련한 사람들이나 헬스케어 비용을 지불한 사람들에게 공개하는 경우, 정보주체의 일반적 상태/위치/죽음에 관해 가족구성원 또는 정보주체가 인정한 사람들에게 알리기 위해 공개하는 경우에만 PHI를 이용하거나 공개하도록 제한을 요청할 수 있다(45 C.F.R. § 164.522(a)). 이 경우, 정보처리자는 제한요청에 동의해야할 의무는 없지만, 동의하면 응급상황에서 치료하는 것을 제외하고는 제한요청을 준수하여야 한다. 그러나, 정보처리자의 동의를 받은 제한도 45 C.F.R. §§ 164.502(a)(2)(ii), 164.510(a), 또는 164.512에 의해 허용되거나 요구된 PHI의 이용이나 공개에는 적용되지 않는다.[26] 연구에 있어서 프라이버시룰의 효력 발생 이전에 정보처리자가 연구목적으로 PHI를 이용하거나 공개하도록 정보주체로부터 서면승인(§ 164.508)이나 그밖의 명백한 법적 허락(§ 164.512(i))을 받은 경우, 연구에 참여하는 정보주체의 충분한 설명에 의한 동의를 받은 경우, 또는 연구를 위해 충분한 설명에 의한 동의면제를 임상시험심사위원회로부터 받은 경우에는 프라이버시룰의 효력 발생 이전이거나 이후에 정보처리자가 수령하거나 만든 PHI를 연구목적으로 이용 및 공개할 수 있다(45 C.F.R. § 164.532(c)).

---

26) US Department of Health & Human Services, OCR, Summary of the HIPAA Privacy Rule 13. http://www.hhs.gov/ocr/hipaa 참조.

② 비밀의사소통 요청권

정보주체는 정보처리자에 대해 통상적인 방법이 아닌 방법을 통하여 PHI에 관한 의사소통을 요구할 수 있고, 정보처리자는 이를 허용하여야 한다. 예컨대, 지정된 주소/전화번호, 우편엽서가 아닌 봉함편지 등을 통해 정보주체와 소통하도록 요청할 수 있다(45 C.F.R. § 164.522(b)).

③ 접근권과 복사권

정보주체는 지정기록세트[27]에 보관되어 있는 PHI에 접근하고 복사할 수 있는 권리를 가진다. 단, 정신과 상담노트, 민・형사 또는 행정소송을 위한 정보, Clinical Laboratory Improvements Amendments of 1988 (42 U.S.C. § 263a)가 접근을 금지하는 실험실 결과, 또는 특정 연구 실험실의 결과는 예외이다(45 C.F.R. § 164.524(a)). 그리고, 임상시험에 대해서는 접근권의 예외를 인정하고 있다. 임상연구를 수행하는 정보처리자는 피험자가 연구에 참여하기 전에 접근권 정지에 동의한 경우에는 임상시험 기간 동안 PHI에 접근하는 피험자의 권리를 정지할 수 있다. 이 예외는 맹검이나 위약대조군을 잘 유지하여 데이터의 과학적 진실성을 보호하기 위해 인정되는 것이다.

④ 수정요청권

정보주체는 정보처리자로 하여금 지정기록세트에 있는 부정확하거나 불완전한 PHI를 수정하도록 요청할 수 있다(45 C.F.R. § 164.526(a)(1)). 정보처리자가 수정요청을 받아들이면, 수정을 위해 합리적 노력을 기울여야 한다. 정보처리자가 수정요청을 거부하면, 정보주체에게 정보처리자는 거부서면을 제공하여야 하고 정보주체로 하여금 지정기록세트에 기록되는 것에 대한 동의거부 진술서를 제출할 것을 허용한다. 그리고 정보처리자

27) 45 C.F.R. § 164.501. 지정기록세트는 정보처리자에 의해 또는 정보처리자를 위해 관리되는 다음의 기록을 말한다: 병원에 의해 또는 병원을 위해 관리되는 정보주체에 관한 의료기록과 의료비청구기록; 의료보험자에 의해 또는 의료보험자를 위해 관리되는 등록, 지불, 이의신청의 재결, 증례 또는 의료관리기록시스템; 또는, 정보주체에 관한 결정을 내리기 위해 정보처리자에 의해 또는 정보처리자를 위해 사용된 기록세트.

는 다른 정보처리자로부터 수정 고지를 받게 되면 지정기록세트에 기록된 PHI를 수정하여야 한다.[28]

⑤ 공개 내역서 수령권

정보주체는 공개 내역을 요청한 날부터 최대 6년 치의 공개 내역을 수령할 권리를 가지고 있다. 그러나, TPO를 위한 경우, 정보주체나 대리인에게 공개한 경우, 승인을 받아 공개한 경우, limited data sets인 경우, 국가안보를 위한 경우, 재소자 등과 관련한 특정 목적을 위해 교정기관이나 법집행 공무원에게 공개한 경우, 프라이버시룰의 효력발생일 이전의 경우 등에는 이 권리를 주장할 수 없다(45 C.F.R. § 164.528(a)).[29] 정보주체가 연구와 관련된 PHI의 공개를 위한 내역서는 추적관찰을 통해 행해지며 다음과 같은 3가지 방법이 있다: 첫째, 공개시마다 공개의 목적과 날짜, PHI 수령자의 이름과 주소, 공개된 PHI의 개요를 요구하는 통상적 추적관찰, 둘째, 동일한 수령인에게 단일목적을 위해 수차례 공개하는 경우로 공개내역서 수령권 기간 동안 행해진 최초의 공개날짜, PHI 수령자의 이름과 주소, 공개된 PHI의 개요, 공개이유의 개요, 공개내역서 수령권 기간 동안 행해진 빈도/주기/횟수, 공개 내역서 수령권 기간 동안 행해진 최후 공개 날짜를 요구하는 복수공개 추적관찰, 셋째, 50명 이상의 피험자의 PHI를 공개하는 대규모 연구의 경우로 연구계획서나 연구활동의 제목, 연구계획서나 연구활동의 개요/연구목적/특정 기록 선정 기준, 공개된 PHI 유형의 개요, 공개 내역서 수령권 기간 동안 행해진 최후 공개 날짜를 포함하여 공개가 행해진 날짜 또는 기간, 연구를 의뢰한 기관과 PHI를 수령한 연구자의 기관의 이름/주소/전화번호, 특정 연구계획서나 연구활동을 위해 정보주체의 PHI는 공개되거나 되지 않을 것이라는 진술서를 요구하는 대안적 추적관찰(45 C.F.R. §§ 164.502(a)(2)(ii), 164.512(i)). 정보주체가 연구의 피험자로서 이 권리를 행사할 경우, PHI의 공개에 대한 추적관찰로 인해 과중한 행정적 부담을 야기시켜 연구에 심각한 영향을

28) US Department of Health & Human Services, OCR, *supra* note 26, at 13.

29) 다만, 승인면제, 연구준비심사, 대행인에 의한 공개의 경우에는 추적관찰되어야 하고 그 내용이 6년간 보존되어야 한다.

미칠 수 있다. 그럼에도 불구하고, HITECH Act에서는 만약 의료기관이 전자건강기록시스템을 이용하고 있다면, TPO를 위한 경우를 포함해서 모든 공개는 내역서에서 추적되어야 한다고 규정하고 있다. 물론, 이것은 의료기관에게 과도한 부담이 될 수 있겠지만, 연방정부는 자금지원이란 인센티브 부여로 전자건강기록시스템을 사용할 것을 권장하고 있다.[30]

(2) 연구를 위한 PHI의 이용·공개·철회

연구란 연구개발, 테스팅, 평가를 포함하는 일반화 할 수 있는 지식을 개발하거나 기여하도록 설계된 체계적 조사를 의미한다. 아래 ①-⑥이 이러한 연구에 이용 및 공개될 수 있는 건강정보이다.[31] 그리고, 연구용 PHI의 이용이나 공개의 승인을 철회하는 것은 프라이버시룰에 따르면 피험자는 언제든지 할 수 있고 반드시 서면으로 요청해야 한다. 프라이버시룰에서는 연구의 통합성을 보호하기 위해 필요한 경우(예컨대, 의뢰자에게 피험자의 철회를 고지할 때, 이상반응을 임상시험심사위원회/의뢰자/식약청에 고지할 때, 그리고 PHI를 식약청에 대한 시판허가 전 신청에 포함시킬 때 등)에만 철회 이후에도 PHI를 계속 이용하거나 공개를 할 수 있다.[32]

① de-identified data

② 피험자의 서면승인을 받은 PHI

피험자의 서면승인은 특정연구목적을 위해서만 할 수 있다. 따라서, 특정되지 않은 연구 또는 장래의 특정되지 않는 연구를 위한 피험자의 서면승인은 아무런 효력이 없다. 복합승인과 관련하여, 정보처리자가 임상

30) Inside The Minds, *supra* note 10, at 110-111.

31) 이 가운데 ①(각주 19)과 ④(본문 p. 12와 각주 20)에 대해서는 이미 기술하였기 때문에 여기서는 부연 설명을 생략하고 제목만 남겨두기로 한다. 이 건강정보들에 관한 자세한 것은 U.S. Department of Health and Human Services, *supra* note 17, at 9-18 참조.

32) 이에 대한 자세한 내용은, Dunn & Chadwick, *supra* note 3, at 161 참조.

연구 참여 동의를 조건으로 PHI의 공개를 승인받고자 할 경우에는 임상연구에 참여하는 동의와 PHI를 공개하는 승인을 함께 포함하고 있는 문서인 복합승인이 허용된다. 그러나, 임상연구가 조직의 뱅킹과 같은 부수적 활동에서 연구관련 조치와 조직과 결합된 PHI를 모두 포함한다면, 정보처리자는 피험자로부터 연구 동의와 결합될 수 있는 연구관련 조치에 관한 승인과 조직 뱅킹에 관한 승인 등 각각의 승인을 받아야 한다. 이와는 달리, 프라이버시룰안은 특정 조건이 충족되면 각각의 문서를 필요로 하는 요건을 제거하였다. 이것은 승인을 획득하는데 사용되는 문서를 위한 특정 요건들을 포함한다. 예컨대, 문서는 연구관련 조치와 결합된 승인과 부수적 활동과 결합된 승인을 명확히 구분해야 한다. 나아가, 문서는 피험자로 하여금 부수적 활동과 결합된 승인을 승인하거나 거부하는 것을 명확히 허용하여야 한다. 이러한 요건들을 충족하기 위해, 정보처리자는 별도의 페이지에 부수적 활동과 관련된 비조치를 기술할 수 있고 피험자가 치료와 연관이 없는 부수적 활동을 위해 PHI를 공개하는 것을 승인하는지 여부를 나타내는 체크박스나 명확한 서명란을 사용할 수 있다.[33]

③ 임상시험심사위원회나 프라이버시보호위원회[34]의 승인면제를 받은 PHI

승인면제는 승인을 받는 것이 현실적이지 않고 프라이버시에 최소 위험 이상을 부과하지 않는 연구인 경우(예: 데이터베이스, 검체은행, 의료기록과 같은 현존 데이터만을 사용하는 연구)와 피험자 스크리닝 및 모

33) Inside The Minds, *supra* note 11, at 72-73.

34) 프라이버시보호위원회는 임상시험심사위원회로부터 승인면제나 변경을 획득하는 것에 대한 대안으로서 PHI의 이용이나 공개에 있어서 승인면제나 변경을 위한 요청을 심사하고 승인하기 위해 프라이버시룰에서 설립된 위원회를 말한다. 이 위원회는 정보주체의 프라이버시권과 관련 이익에 관한 연구계획서의 영향력을 심사하기에 필요한 정도로 다양한 배경과 적절한 전문성을 지닌 위원들로 구성된다. 이 위원회는 위원 구성과 관련하여, 정보처리자와 관련되지 않고, 연구를 수행하거나 의뢰하는 어떠한 기관과도 관련되지 않고, 그리고 그러한 기관과 관련된 어떠한 사람과도 연결되지 않은 위원을 최소한 1명은 포함시켜야 한다. 이 위원회는 이해상충이 있는 위원으로 하여금 심사에 참여하도록 해서는 안된다(45 CFR § 164.512(i)).

집을 위해 PHI를 수집할 때에 주로 인정된다. 부분승인면제(피험자모집을 위해 정보주체와 접촉할 경우에는 면제하고 등록시에는 승인을 요구하는 것)도 이에 해당한다. 연구활동이 프라이버시에 최소 위험 이상을 부과하지 않는다는 것을 증명하기 위해 연구자는 임상시험심사위원회나 프라이버시보호위원회에 i) 부적절한 이용과 공개로부터 개인식별표지를 보호하기 위한 충분한 계획, ii) 개인식별표지를 유지하기 위한 연구의 정당성이 없으면 가능한 한 빨리 개인식별표지를 폐기하기 위한 충분한 계획, iii) 프라이버시룰에 근거해 허용된 것을 제외하고 PHI는 재이용되지 않고 공개되지 않을 것이라는 서면보증을 제시해야 한다.

④ a limited data sets

⑤ 연구준비를 위한 PHI

PHI는 i) 연구계획서를 준비·개발하거나 유사한 목적(예: 피험자 스크리닝)을 위해 사용될 것이라는 점, ii) 연구가설을 개발하는 것을 돕기 위해 필요하다는 점, iii) 정보처리자가 있는 현장 내에서 행해진다는 점을 연구자가 정보처리자에게 나타낼 경우가 여기에 해당한다(45 C.F.R. § 164.512(i)(1)(ii)).

⑥ 사망한 자의 PHI

사망한 자의 PHI는 연구를 위해서만 그리고 연구를 위해 필요하다는 “증명”을 하면, 정보처리자는 승인없이 이용이나 공개할 수 있다. 증명양식은 특정되어 있지 않지만, 공개의 경우 정보처리자가 추적관찰해야 하기 때문에 서면형식으로 할 것이고, 요청이 있으면 연구자는 사망증명서를 제출하여야 한다. 프라이버시룰은 사망한 자와 살아있는 사람의 프라이버시 보호를 동일하게 규정하고 있다. 그러나, 프라이버시룰안은 i) 일정 기간 이후에는 사망한 자의 PHI를 이용하거나 공개하는 것을 승인하기 위한 대리인을 찾는 것이 어렵고 대략 2세대에 해당하는 50년이면 전부는 아니더라도 대부분의 살아있는 친척들이나 다른 영향을 받는 개인

들의 프라이버시권을 보호하는데 충분한 시간이라는 이유로 사망 후 50년 이상된 경우에는 개인식별 가능한 건강정보를 PHI에서 제외하도록 하고, ii) 현행 프라이버시룰은 사망한 자를 법적으로 대신할 권리가 있는 자를 대리인으로 간주하여 정보주체로 취급하기 때문에 이에 해당하지 않는 가족 구성원들과 사망하기 전에 사망한 자를 보호하거나 의료비용을 지불한 그밖의 사람들에게 사망한 자의 유언 등에 반하지 않을 경우 정보 공개를 허용할 것을 제안하고 있다.[35)]

(3) 연구를 위한 데이터베이스와 검체은행의 설립·이용

프라이버시룰은 연구를 위한 데이터베이스와 검체은행의 설립과 이를 이용하는 것에도 적용된다. 연구를 위한 데이터베이스와 검체은행의 설립을 위한 데이터나 조직을 수집하는 행위(1차적 이용)와 이를 장래 연구를 위해 분석하는 것(2차적 이용)은 프라이버시룰에서는 별도의 연구행위로 간주된다. 정보처리자가 연구를 위해 데이터베이스나 검체은행을 설립할 경우, 그 데이터나 검체가 PHI를 포함하고 있으면 프라이버시룰이 적용된다. 데이터의 경우, 승인 또는 승인면제가 요구되는가 여부는 데이터 수집이 피험자와 직접적 상호작용을 포함하고 있는지 여부에 달려있다. 만약 PHI가 데이터베이스로 되기 위해 피험자로부터 직접 수집되면, 피험자의 승인을 받아야 한다. 의료기록 또는 기존 PHI (예: 기존 비연구 데이터베이스)가 데이터베이스 설립을 위한 자료데이터가 된다면, 데이터 수집은 승인면제를 받을 수 있다. 임상시험심사위원회나 프라이버시보호위원회는 ① PHI의 이용 또는 공개가 피험자에게 최소위험 이상을 가하지 않는다는 사실, ② 그밖의 다른 면제 기준을 충족한다는 사실, ③ 피험자와의 상호작용없이 데이터수집이 가능할 경우, 연구자가 피험자의 승인을 획득하여서는 연구가 불가능할 것이라는 사실 등을 결정하여 승인면제를 할 수 있다. 검체의 경우, 검체수집은 피험자와 직접적 상호작용을 포함하기 때문에 피험자의 승인을 받아야 한다. 다만, 연구자가 임상목적으로만 수집된 남은 조직이나 병리학 검체와 같은 기존검체만을 사

35) Inside The Minds, *supra* note 10, at 73.

용하여 검체은행을 설립할 경우에는 연구를 위한 검체은행설립은 승인면제요건을 충족한다.

연구를 위한 데이터베이스와 검체은행을 설립하기 위해 데이터와 검체 수집을 위해 승인이 요구될 때, 장래의 특정되지 않은 연구를 위한 백지승인은 허용되지 않고 이를 회피하기 위해 서면승인서가 작성되어야 한다. 왜냐하면, 특정되지 않은 장래의 연구를 언급하는 것은 피험자에게 PHI의 이용 또는 공개 목적에 관해 충분한 정보를 제공하지 않기 때문이다. 따라서, 백지승인을 방지하기 위해 연구자는 PHI의 이용과 공개 목적을 연구계획서와 동의서에서 구체적으로 기술하여야 한다. 즉, 연구를 위한 데이터베이스나 검체은행을 설립하기 위해 데이터나 조직을 수집할 목적을 가진 연구자는 연구에서 분석을 위해서만 PHI를 이용 또는 공개한다는 것을 승인시에 명확히 하여야 한다. 결론적으로, 프라이버시룰은 연구를 위한 데이터베이스나 검체은행 설립을 위해 데이터나 검체수집의 승인을 받을 때 장래 연구의 구체적 목적을 기술하지 않으면 그 승인은 장래 연구를 위한 승인이 될 수 없고 다시 승인을 받아야 한다고 하여 연구를 위한 데이터베이스와 검체은행을 설립하는 것과 그 이후의 연구 데이터베이스 또는 검체은행의 이용과는 구분을 짓고 있다. 연구데이터베이스 또는 검체은행의 이용과 관련해서는, 연구자는 ① de-identified data나 조직의 제공 요구, ② limited data sets 요구, ③ limited data sets의 범위를 넘어서는 PHI 필요시 승인면제 요청 등의 방법으로 프라이버시룰의 적용을 피하거나 최소한의 준수를 강구할 수 있다.

5. 정보주체의 프라이버시 보호를 위한 정보처리자의 행정상 의무사항

프라이버시룰은 정보처리자로 하여금 ① 프라이버시 정책 및 절차 개발 그리고 실행과 이를 위한 담당자 지정, ② 프라이버시 보호를 위한 훈련과 관리, ③ 직원의 잘못으로 야기된 유해요소 완화, ④ 의도적·비의도적 이용이나 공개를 예방하기 위한 합리적이고 적절한 데이터 안전장치 마련, ⑤ 이의신청 절차 마련, ⑥ 정보주체의 권리행사에 대한 보복금지

와 권리포기 요구금지, ⑦ 문서화와 기록 보존 등을 하도록 의무지우고 있다(45 C.F.R. § 164.530).

Ⅳ. 맺는말

프라이버시룰은 건강정보의 정보화와 이에 따른 정보주체의 프라이버시 보호를 위해 정보처리자에 의해 수집된 개인건강정보의 프라이버시보호를 위한 새로운 기준을 제시하고 있다. 즉, 프라이버시룰은 정보처리자에 대해 연구목적을 포함하여 PHI가 어떻게 이용되고 공개되어야 하는지 그리고 정보주체가 자신의 건강정보를 어떻게 통제할 수 있는지에 관한 최소한의 연방 기준을 정립해 두고 있는 것이다. 특히, 연구와 관련하여, 프라이버시룰은 연구를 방해하는 것이 아니라 피험자의 프라이버시를 보호하는 방법으로 연구를 위해 필요한 핵심 정보에 접근하는 방법들을 제공하고 있어 연구자 보호 및 연구수행의 효율성에 기여한다. 예컨대, 연구에서 피험자의 PHI를 이용 내지 공개하기 위해서는 피험자의 승인서를 받는 것이 원칙이지만, 승인서를 획득하는 것이 현실적이지 않다면 임상시험심사위원회나 프라이버시보호위원회는 승인을 면제하거나 변경할 수 있다. 프라이버시룰은 또한 limited data sets나 특정 연구활동을 위해 제공된 증명과 같이 승인요건의 면제나 변경 등 승인서 획득 이외의 대안들도 제공하여 연구자 보호 및 연구수행의 효율성을 보장하고 있다. 연구와 관련하여서, 우리의 개인정보보호법은 제18조 제2항 제4호에서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제3자에게 제공하는 경우로서 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 없는 경우에 한하여 개인정보를 제공하여 연구를 수행할 수 있도록 매우 제한적으로 규정하고 있다.[36] 이 조항에 따르면, 개인정보를 직접 수집한 연구자 등은 직

36) 필자는 이 조항 이외에도 연구목적으로 피험자의 건강정보가 사용될 경우 개인정보보호법으로 규정하기는 사실상 불가능할 것으로 판단한다. 그 이유는 다음과 같다: i. 개인정보보호법상 개인정보와는 달리 건강정보는 다양한 집단(의뢰자, 연구자, 임상시험심사위원회, 임상시험수탁기관 등) 간에 정보를 공유할 기회가 많다. 즉, 임상시험 및 연구 관련자의 이용 및 공개가 빈번하게 널리 발생한다. ii. 연구수행 단계

접 연구를 수행할 수 없고, 특정 개인을 알아볼 수 없는 형태로 개인정보를 제3자에게 제공하여서만 연구를 수행할 수 있으며, 거기에다 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 없어야 한다. 개인정보를 수집한 정보처리자가 직접 이를 이용하여 연구를 할 경우에는 어떻게 할 것인지? 특정 개인을 알아볼 수 없는 형태의 정보를 이용하는데 정보주체의 이익이 부당하게 침해될 수 있겠는지? 그리고 제3자의 이익이 어떻게 부당하게 침해될 수 있겠는지? 특정 개인을 알아볼 수 없는 형태란 어떤 개인식별정보를 어떻게/어느 범위까지 제거한 것인지? 역학연구의 경우에는 어떻게 할 것인지? 등에 관한 문제가 있다. 과연, 이 조항을 가지고 연구에서 피험자의 건강정보 사용을 적절히 규제하여 연구를 방해하지 않는 동시에 피험자의 프라이버시 보호도 동시에 할 수 있겠는가? 결론적으로, 개인의 건강정보와 개인정보보호법의 개인정보와는 앞에서 언급한 바와 같이 그 성격, 사용자의 범위, 이에 따른 보호 정도에 있어서 매우 차이가 난다는 것을 인식하여야 한다. 즉, 개인건강정보는 불법적으로 누설될 경우 개인정보에 비해 훨씬 더 치명적 부작용을 정보주체에게 가져다 줄 수 있다(예: 정신병력, 유전정보 등). 그러므로, 서로 다른 규제 대상에 대해 단일의 법인 개인정보보호법으로 규제한다는 것은 규

별(예: 연구계획서 개발단계, 피험자 선정단계, 모집단계 등)로 피험자의 건강정보의 사용이 이용에 해당하는지 공개에 해당하는지 달라지고, 이에 따라 추적관찰의 필요성 여부가 결정된다, iii. 피험자의 건강정보 이용 및 공개에 관한 동의획득 방법은 연구에 참여하기 전에 설명서와 동의서에 관한 충분한 설명에 의한 동의에 따른 서면동의만 가능한데, 개인정보보호법에서는 동의 획득을 위한 다양한 방법(서면, 전화, 인터넷 등)을 규정해 놓고 있다. 예컨대, 서면 동의서 이외의 방법으로 동의를 획득할 경우 피험자의 보호에 문제가 발생할 우려가 있다. v. 프라이버시룰에는 승인철회는 서면으로만 하도록 규정하고, 승인철회 후에도 연구의 통합성을 위해서 피험자의 건강정보를 이용 및 공개할 수 있도록 규정하고 있다. 그리고 승인면제의 요건도 상세히 규정하고 있다. 개인정보보호법에는 이러한 내용이 없다. vi. 프라이버시룰에서는 연구수행을 위해 반드시 피험자의 승인서를 받도록 규정하고 있지는 않다. limited data sets, 연구계획준비, 임상시험심사위원회나 프라이버시보호위원회에 의한 승인면제 등을 두어 연구활성화에 기여한다. 개인정보보호법에는 이러한 규정이 없다. vii. 개인정보보호법에서는 만 14세 미만의 미성년자에 대해서만 법정대리인의 동의를 받도록 보호규정을 두고 있다. 실제로, 연구에 있어서 미성년자의 경우에는 나이대별로 구분하여 법정대리인의 동의를 받도록 하고 있다. 예컨대, 6세까지, 7세부터 13세까지, 14세부터 19세까지 등으로 구분하여 미성년자의 보호에 추가적 안전판을 마련해 두고 있다. 개인정보보호법에는 이러한 규정이 없다.

제법 체계에 맞지 않는다 할 것이다. 따라서, 개인건강정보의 보호를 위해서는 HIPAA와 같은 건강정보의 보호를 위한 별도의 독립된 법률과 이에 근거한 프라이버시룰과 같은 법규명령을 마련하는 것이 정도일 것이다. 특히, 연구에 있어서 피험자의 프라이버시 보호, 연구자 보호, 그리고 연구수행의 효율성 증진 등을 위해서는 별도의 독립된 법령을 제정하는 것이 올바른 길이라 생각한다. 다만, 이러한 독립된 법령의 제정이 시일이 많이 걸리고 현실적으로 어려움이 있다면, 다음과 같은 프라이버시룰의 조항들을 우리의 개인정보보호법에 추가한다면, 연구에 있어서 피험자의 프라이버시 보호를 한층 더 강화하고 동시에 연구자 보호와 연구수행의 효율성을 고양하는데 어느 정도 기여할 수 있을 것으로 판단한다:

첫째, 개인정보보호법 제2조 1호에서 개인식별표지를 더 상세히 규정해야 한다. 프라이버시룰에서는 18개의 개인식별표지를 규정해 두고 있으며, 마지막 18번째는 간접적 식별표지로서 프라이버시룰의 적용대상 정보의 범위를 매우 넓혀 두고 있다. 만약, 우리 법률에서 상세히 규정하기 어렵다면, 시행령이나 시행규칙에서라도 이를 상세히 규정하는 것이 정보주체의 권리를 보호하는 데 도움이 될 것이다. 그리고, 사망한 자의 개인정보 보호에 관한 내용도 법률에서 규정해야 할 것으로 보인다. 다만, 사후 몇 년까지의 정보를 보호대상으로 할 것인지 누구의 승인을 받아야 할 것인지 등의 문제는 하위법령에서 규정해도 문제는 없을 것으로 보인다. 프라이버시룰은 사망한 자의 건강정보도 연구의 대상정보로 사용될 수 있도록 규정해 두고 있다.

둘째, 개인정보보호법 제2조 5호에서 개인정보처리자의 종류만을 기술하고 있다. 그러나 연구의 경우에는 정보처리자 내부 간에서의 정보처리가 제3자에 대한 제공(=공개)에 해당하는지 아니면 정보처리자 자신의 처리(=이용)에 해당하는지를 명확히 해야 할 것이다. 이는 공개의 경우에는 추적관찰이 필요하고, 이용의 경우에는 추적관찰이 필요없어 행정적 부담과 관련이 있기 때문이다. 특히, 정보처리자가 개인이 아니라 기관인 경우에는 이를 더 명확히 해야 할 필요성이 존재한다. 프라이버시룰은 기관정보처리자인 경우에는 HE, ACE, OHCA 등으로 구분하여 PHI의 이용인

지 공개인지를 구분하고 있다.

셋째, 개인정보보호법 제18조 제2항 4호와 관련한 앞의 몇 가지 문제점에 대해서는 동 조항을 개정하는 것이 바람직할 것으로 보인다. ① 개인정보를 수집한 정보처리자가 직접 이를 이용하여 연구를 할 경우에는 어떻게 할 것인지?에 대해서는, 제4호 "... 개인정보를 제공하는 경우"를 "... 개인정보를 이용하거나 제공하는 경우"로 정정하면 될 것이다. ② 특정개인을 알아볼 수 없는 형태의 정보를 이용하는데 정보주체의 이익이 부당하게 침해될 수 있겠는지? 그리고 제3자의 이익이 어떻게 부당하게 침해될 수 있겠는지?에 대해서는, 연구의 경우 특정개인을 알아볼 수 없는 형태의 정보를 사용할 경우 이러한 문제의 발생은 없기 때문에 제4호에 대해서는 적용되지 않는다고 별도로 기술해 두는 것이 해결방안이 될 것이라 여겨진다. de-identified data는 프라이버시룰의 적용을 받지 않아 정보주체의 승인을 받지 않고서도 연구자는 이 정보를 연구에 사용할 수 있다. ③ 특정 개인을 알아볼 수 없는 형태란 어떤 개인식별정보를 어떻게/어느 범위까지 제거한 것인지?에 대해서는 동법의 정의 조항 신설, 제4호 제2문 신설, 아니면 하위법령에서 이에 대한 내용을 규정하는 것이 해결책이 될 것이다. 프라이버시룰의 2가지 방법이 참고될 수 있다. ④ 역학연구의 경우에는 어떻게 할 것인지?는 이 법의 시행으로 연구에서 가장 많은 반발에 부딪치는 문제이다. 왜냐하면, 역학연구에는 피험자의 인적사항이 필수적으로 기재되고 진료기록 등도 기재되는데, 제4호에 따라 특정개인을 알아 볼 수 없는 정보의 사용으로는 역학연구를 할 수 없게 되기 때문이다. 참고로, 프라이버시룰에서는 연구, 공중보건, 역학연구의 경우에는 limited data sets라는 정보의 사용을 허용하여 피험자의 승인 없이도 역학연구를 가능하게 하고 있다. ⑤ 연구용 데이터베이스와 검체은행의 설립과 이용시 정보주체의 프라이버시보호에 대해서는 어떻게 할 것인지?에 대해서는, 양자를 구분해서 각각 달리 적용되는 프라이버시룰의 규정을 참조하는 것이 도움이 될 것이다.

넷째, 개인정보보호법 제23조에서 건강, 성생활 등 민감정보는 정보주체의 별도의 동의를 받은 경우에만 처리할 수 있도록 규정하고 있다. 여

기서 별도의 동의란 백지동의도 포함하는 것인지? 역학연구의 경우에는 별도의 동의를 어떻게 받을 수 있겠는지? 등의 문제가 있다.

다섯째, 개인정보보호법 제20조에서 “정보주체의 요구가 있으면” 정보주체 이외로부터 수집한 개인정보의 수집 출처 등을 정보주체에게 고지하도록 규정하고 있는데, 동법이 정보주체의 프라이버시 보호에 관한 법이라면, “정보주체의 요구가 있으면”이라는 문구는 삭제하는 것이 바람직하다. 왜냐하면, 정보주체의 요구가 없더라도 당연히 정보주체에게 그 내용을 알려야 정보주체의 권리가 적법하고 적절하게 보장될 수 있기 때문이다. 프라이버시룰에서는 정보처리자로 하여금 프라이버시실행의 사전고지를 통해 PHI 이용과 공개에 관한 정보처리자의 방법, 정보주체의 권리, 정보처리자의 법적 의무를 고지해야 하도록 요구한다. 특히, 연구와 관련하여, 피험자 스크리닝, 피험자 모집, 기존 데이터베이스와 조직은행의 분석 등 정보주체의 승인없이 PHI 이용과 공개가 가능하다는 것을 사전고지의 내용으로 기술해야 한다.

여섯째, 피험자의 PHI 이용과 공개에 앞서 연구의 참여 여부를 결정하기 위해서는 피험자 는 동의서를 작성해야 하는데, 이 동의서에는 연구에 참여하는데 동의하지 않더라도 어떠한 불이익이 없다는 것을 핵심적 내용을 하고 있다. 반면, 개인정보보호법 제15조 제2항 4호의 경우 “동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용”을 규정하고 있다. 이럴 경우, 동법으로 연구에 참여하는 피험자의 권리를 적절히 보호할 수 없을 것으로 보인다.

참 고 문 헌

김장한, “의료기관 개인건강정보의 이차적 이용”, 「의료법학」, 11권1호, 한국의료법학회, 2010

매일경제, 2011. 12. 7. 수요일, B7면

백윤철·김상겸, 「미국의 의료정보보호에 대한 연구」, 한국학술정보, 2006

Cynthia McGuire Dunn & Gary L. Chadwick, Protecting Study Volunteers in Research, CenterWatch, 2004

Inside The Minds, Recent Developments with HIPAA, Thompson Reuters/ Aspatore, 2010

Nick Littlefield & Colin Zick, “HIPAA: New Federal Privacy Rules and Their Implications”, 46-OCT B. B.J. 14 (September-October, 2002)

Rebecca Lewin, “Job Lock: Will HIPAA Solve The Job Mobility Problem?”, 2 UPAJLEL 507 (Winter 2000)

U.S. Department of Health and Human Services, Office of the National Coordinator for Health Information Technology, Nationwide Privacy and Security Framework For Electronic Exchange of Individually Identifiable Health Information, December 15, 2008

Elizabeth Hutton, Devin Barry, “Privacy Year In Review: Developments In HIPAA”, 1 I/S: J. L. & Pol'y for Info. Soc'y 347 (Spring/Summer, 2005)

U.S. Department of Health and Human Services, Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule. http://privacyruleandresearch.nih.gov

US Department of Health & Human Services, OCR, Summary of the HIPAA Privacy Rule. http://www.hhs.gov/ocr/hipaa

<국문초록>

HIPAA 프라이버시룰은 개인건강정보를 보호하기 위해 새로운 연방기준을 정립해서 제공하고 있다. 프라이버시룰은 보호된 건강정보(PHI)가 어떻게 사용되고 공개되어야 하는지 또는 정보주체가 자신의 건강정보를 통제할 수 있는 권리를 어떻게 행사해야 하는지에 관한 방법을 구체적으로 정립해 두고 있는 것이다. 연구와 관련하여, 특히, 프라이버시룰은 연구를 수행하는데 있어서 장애물이 되어서는 안될 것이다. 오히려, 프라이버시룰은 연구자들로 하여금 연구목적을 달성하는데 필요한 핵심 정보에 적절하게 접근할 수 있는 방법을 제공하여 연구자들을 보호하고 연구수행의 효율성을 고양하는데 기여해 오고 있다 할 것이다. 예컨대, 비록 연구에서 피험자의 보호된 건강정보를 사용하거나 공개하기 위해 피험자로부터 서면승인을 획득하는 것이 일반원칙이라고 하더라도, 만약 그 서면승인을 획득하는 것이 현실적이지 않다면, 임상시험심사위원회나 프라이버시보호위원회가 그 서면승인을 면제하거나 변경할 수 있다. 프라이버시룰은 또한 서면승인을 획득하는 것에 대한 대안들을 제공하기도 한다. 그 대안들은 limited data sets를 연구에서 사용하도록 허용하거나 연구에서 필요하다고 증명하는 경우 사망한 자의 보호된 건강정보를 사용하도록 허용하는 것이 될 것이다. 이에 더하여, 프라이버시룰은 적용대상인 정보처리자에게 프라이버시룰을 위반할 경우 강제집행규칙에 따라 민사벌과 형사벌을 부과할 수 있는 실질적 강제력도 가지고 있다. 이에 비해, 우리는 개인정보보호법을 작년에 제정하여 시행하고 있지만, 연구에 있어서 피험자의 건강정보를 보호하기에는 충분하지 않다는 것이 여러 측면에서 지적될 수 있다. 그래서, 이 논문에서는 우리 개인정보보호법이 연구에서 보호된 건강정보의 사용 내지는 공개를 연구수행을 방해하지 않고서 적절하게 규제할 수 있는 몇 가지 방안을 제시한다.

주제어 : 개인정보보호법, 보호된 건강정보, 하이테크액트, 히파, 프라이버시룰, 프라이버시보호위원회

Application of HIPAA Privacy Rule to Protect Human Subjects' Health Information in Research

Park, Soo-Hun*

HIPAA Privacy Rule has provided the new federal wide standards to protect individual health information by establishing the methods how to PHI should be used or disclosed and how to individuals yield rights to control their own health information. In relation to research, especially, Privacy Rule has not been an obstacle to conduct research. Rather it has attributed to protect researchers and to enhance efficiency of conducting research by way of providing proper access to the core information necessary to achieve the goals of research. For example, even though it's the general rule to obtain written authorization from human research subjects in order to use or disclose PHI in research, if it's not practicable to obtain it, IRB or Privacy Board can waiver or change authorization. Privacy Rule also provides the alternatives of obtaining authorization by allowing to use limited data sets or to demonstrate representations in research. In addition, Privacy Rule has real teeth by imposing civil and criminal penalties under Enforcement Rule on CE who violates it. Enforcement Rule was amended by HITECH Act. In contrast, Korean government enacted Personal Information Protection Act (PIPA) last year. However, it's not enough to protect individual health information in research in several aspects.

Key Words : HIPAA, HITECH Act, Personal Information Protection Act, Privacy Board, Privacy Rule, Protected Health Information (PHI)

* Associate Professor, Sookmyung Women's University, SJD