# 번역

전남대학교 법학연구소 공익인권법센터
인권법평론 제25호 (2020년 8월)
https://doi.org/10.38135/hrlr.2020.25.241


# 데이터 접근성을 통한 보건의료와 인공지능의 융합

## — 일반정보보호규정(GDPR)이 정책 입안자들에게 신호등 역할을 할 수 있는가? —

**엄주희*·심지원**·김혜경*****

목차



* 제1저자: 연세대 보건대학원, 연구 교수, 이메일: juheelight@gmail.com
** 공동저자: 중앙대 인문콘텐츠연구소, 연구 교수
*** 교신저자: 인제대 인문문화융합학부 교수, 인간환경미래연구원 원장
논문접수일 : 2020. 7. 22., 심사개시일: 2020. 8. 3., 게재확정일 : 2020. 8. 18.
이 논문은 2019년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구이다.(NRF-2019S1A5A2A03053179)
원문은 캐나다 셜부룩 대학(Université de Sherbrooke)의 Mélanie Bourassa Forcier와 Siobhan Mullan 그리고 맥길 대학(McGill University)의 Yann Joly와 Hortense Gallois가 저자로 참여하여 Journal of Law and the Biosciences에 실린 "Integrating artificial intelligence into health care through data access: can the GDPR act as a beacon for policymakers?" (Journal of Law and the Biosciences, Volume 6, Issue 1, October 2019, Pages 317-335, doi:10.1093/jlb/lsz013)을 번역한 것이다. 한국의 학자들을 위해 원문을 번역해서 2차적 저작물로 만들어 알

| 국문초록 |

보건의료 분야에서 인공지능은 정밀의료, 진단 도구, 심리정신적 치료와 의사결정 지원, 돌봄 서비스 등의 분야에 접목되어 상당한 발전을 이루어오고 있다. 보건의료 분야의 인공지능은 연구대상자로부터 추출된 건강 관련 데이터와 민감 정보를 포함하여 상당 부분의 개인정보와 데이터에 의존한다. 보건의료에 융합된 인공지능의 발전 추이를 감안하면, 인공지능에 기반이 되는 데이터에 대한 규율이 보건의료 인공지능을 규제하는데 크게 영향을 미치게 된다. 유럽연합(European Union; EU)에서 제정된 「일반정보보호규정」(General Data protection Regulation; GDPR)은 데이터 보호 법제를 통해 인공지능을 규율하려는 최초의 시도를 했다. GDPR은 개인정보처리자나 수탁자가 유럽연합 내에서 정보주체에게 상품이나 서비스를 제공하는 것과 관련이 된 경우에, 그리고 정보주체의 행동을 모니터링하는 것과 관련이 있을 때 적용되기 때문에, 유럽연합 뿐 아니라 유럽연합에 속하지 않은 많은 외국 기업들의 활동이 GDPR의 규율 대상에 포함된다. 미국과 캐나다에서는 GDPR의 규율로 인해서 데이터 관련 정책과 법제를 개혁해야 한다는 압박이 제기되고 있다. 보건의료 분야에 대한 인공지능의 기여도와 전망의 개요를 살펴보고, 이 분야의 발전으로 인한 데이터 및 프라이버시 보호에 대한 과제를 탐구하였다. 이를 통해 GDPR의 시사점과 함의를 가지고, 미국과 캐나다의 정책적 개선점을 위한 핵심 방안을 짚어보았다.

**주제어** : 인공지능, 보건의료, 데이터 보호, 개인정보, 개인 데이터, 일반정보보호규정, GDPR, 프라이버시권, 프라이버시

---

리는데 대해 흔쾌히 허락해주신 원저자들께 감사드리고, 특히 본고의 진행을 기쁘게 격려해주신 교신저자 Hortense Gallois 선생님께 감사의 마음을 전한다.

# Ⅰ. 역자 해제

인공지능의 발전에 있어서 데이터의 양과 질은 필수적인 요소이자 전제조건이다. 인공지능이 보건의료 분야에 적용될 때에 방대한 또는 비개인 정보로 이루어진 빅데이터에 의존하고 있기 때문에 정보와 관련된 기본권의 보호와 규율의 문제가 중요한 이슈로 떠오른다. 우리나라도 4차 산업혁명 시대에 산업적 발전을 위해 데이터의 활용범위를 확대할 필요가 있고 이를 원활히 하기 위해서 각종 규제를 완화할 필요가 있다는 문제가 지속적으로 제기되어 왔다.[1] 2020년 1월에 「개인정보 보호법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「신용 정보의 이용 및 보호에 관한 법률」, 소위 데이터 3법이 국회를 통과하여 올해 8월 5일부터 시행된다. 가명정보 개념을 도입하여 공익적 기록 보존 등의 몇몇 지정한 목적을 위해서는 정보주체의 동의 없이 데이터를 활용가능 하도록 하는 등 데이터에 관한 법제의 개정으로 인공지능 의료에도 일말의 변화를 예고하고 있다.[2] 우리나라 보다 앞서 유럽연합(European Union, 이하 EU로 칭한다)는 「일반정보보호규정」(General Data protection Regulation, 이하, GDPR로 칭한다)로서 가명정보와 익명정보를 도입하고 데이터 이동권, 잊혀질 권리 등을 규율하는[3] 등 데이터 활용과 개인정보 및 개인의 프라이버시에 관한 권리 보장 사이에서 합리적인 접

1) 이재훈, 데이터 3법 개정과 연구개발정보 활용을 위한 제언, KISTEP Issue Paper, 2020-02 (통권 제281호), 2020, 2면.

2) 개인정보 보호법 [시행 2020.8.5.] [법률 제16930호, 2020.2.4.일부개정]
문유정, 강지민, 데이터 3법 개정과 의료 빅데이터 활용방안, GBSA Review No. 2020-10, 경기도경제과학진흥원, 2020.3.16.

3) GDPR의 제정 배경, 입법목적, 구성 등 상세 내용에 대해서는 다음의 논문 등을 참조: 조수영, 개인정보보호와과 EU의 GDPR에서의 프라이버시 보호에 관한 연구, 법학논고 제61집, 2018.

점을 찾았고, 이러한 EU의 동향은 미국과 캐나다 법제에 미치는 영향이 크다. 인공지능 의료의 특성을 짚으면서, 이에 개인정보 보호와 데이터에 관한 규율을 논하는 원문을 고찰한다면 우리나라의 관련 논의 진행에도 시사점을 확보할 수 있다는 전망에서 본고가 가치를 가진다.

EU의 GDPR이 미국과 캐나다의 인공지능 의료 관련 법제에 미치는 영향을 비교 고찰한 원문은 정보 데이터를 둘러싼 권리와 책무성 문제를 통해 인공지능 의료에 관한 규율을 조망하고 통찰하였다. 명료하고 정확한 의미 전달을 위하여 직역 보다는 원문과 의미가 달라지지 않는 선에서 의역을 시도하였으며, 설명과 해석이 필요한 부분도 각주로 표기하여 서술하였다. 각주를 원문과 동일하게 표기함으로써, 원문의 체계와 논리가 최대한 전달되도록 하였다. 이하부터 원문의 내용이다.

## Ⅱ. 서론 : 인공지능과 보건의료 그리고 EU의 「일반정보보호규정」(GDPR)

보건의료의 발전을 견인할 인공지능(AI)의 잠재력은 공중보건 및 건강 정책에 관련된 논의의 중심적인 주제가 되고 있다. 인공지능이 오늘날 혁신적인 기술로 추앙받고 있지만, 인공지능의 발전은 이미 반세기에 걸친 역사를 가지고 있다. 앨런 튜링(Alan Turing)이 기계가 인간의 사고방식을 닮을 수 있다는 생각을 해낸 1950년대부터 이미 인공지능 연구는 진행되어온 것이다.[4] 그 후 1959년, 컴퓨

4) Allan M. Turing, *Computing Machinery and Intelligence*, 49 Mind 433, 460 (1950);

터 과학자들은 컴퓨터 스스로 퍼즐을 풀 수 있는 프로그램을 만든 '기계학습(Machine Learning, ML)'을 창조해냈다.[5] 앞으로 인공지능은 전기와 인터넷의 발명과 같이 중추적인 차세대 기술 혁명을 주도할 것이다.[6]

보건의료 분야에서 인공지능은 이미 정밀의료, 진단 도구, 심리적 지지 및 노인을 위한 돌봄 서비스와 같은 분야에서 상당한 진척을 견인해냈다.[7] 인공지능 기술은 대체로 방대한 양의 개인 및 비개인 데이터를 통해 작동되는데, 특히 보건의료 분야의 경우 인공지능 기술은 의료 기록 또는 연구 참여자 (연구 대상자)의 결과에서 추출된 건강 관련 데이터를 포함한 개인 정보에 의존한다.[8] 인공지능을 발전시키고 보건의료 시스템을 위한 혜택을 차지할 수 있는 요인은 대체로 이러한 민감 정보에 대해 용이하게 접근할 수 있는지에 크게 좌우된다.[9] 이런 상황에서 프라이버시 보호 조치를 취하는 것, 특히 의료 및 임상시험 현장에서 본인의 데이터를 공유하는

---

Nils J. Nilsson, *The Quest For Artificial Intelligence*, Cambridge Core 56 (2009), http://core/books/quest-for-artificial-intelligence/32C727961B24223BBB1B3511F44F343E (accessed Mar. 14, 2019).

5) Nello Cristianini, *Intelligence Reinvented,* 232 New Scientist 37, 41 (2016).

6) Roger Parloff, *The Deep-Learning Revolution,* 174 Fortune 96, 106 (2016).

7) Andreas Holzinger, *Trends in Interactive Knowledge Discovery for Personalized Medicine: Cognitive Science meets Machine Learning,* 15 The IEEE Intelligent Informatics Bulletin 6, 14 (2014).

8) Riccardo Miotto et al., *Deep Learning for Healthcare: Review, Opportunities and Challenges,* 19 Brief Bioinform. 1236, 1246 (2018). 역자주: 원문은 personal data와 personal information을 혼용하고 있는데, 원저자들이 personal data로 쓴 부분은 주로 개인 데이터라는 용어로 사용한다.

9) Willem Sundblad, *Data is the Foundation for Artificial Intelligence and Machine Learning Forbes* (2018), https://www.forbes.com/sites/willemsundbladeurope/2018/10/18/data-is-the-foundation-for-artificial-intelligence-and-machine-learning/ (accessed Jan. 23, 2019).

것에 대해 심각한 우려를 표하는 개인들을 위해 적절한 보호 조치를 확보하는 것이 필수적이다.[10]

의료 연구 촉진을 위한 대중적인 오픈 데이터베이스 구현 방안은 유럽과 북미 내에서 논쟁을 불러일으켜왔다. 영국의 경우, 시민들이 프라이버시 침해 우려로 인해 2014년에 시작된 care.data 프로젝트를 거부한 사례가 있다. 이 프로젝트는 보건의료 전문가들에 의해 폭넓은 지지를 받았지만, 이것의 실패는 건강 정보 사용계획의 투명성 결여와 잠재적 옵트 아웃(opt-out) 가능성에 대한 투명성 결여에서 기인했다고 볼 수 있다.[11] 미국에서 진행된 연구에 따르면 이러한 맥락에서 본인의 유전자 데이터를 포함하는 연구에 참여하려는 개인의 자발성은 본인의 프라이버시를 보호받을 수 있는지 여부에 대한 우려에 상당히 영향을 받는 것으로 나타났다.[12] 역설적으로, 이러한 신뢰의 부족은 소비자 대상 직접(DTC: direct-to-consumer) 유전자 검사[13]나 건강 모니터링 기기의 인기를 통해 오히려 상쇄되

10) Brian Scogland, *Artificial Intelligence in Medicine: Hope or Hype? MDDI Online* (2018), https://www.mddionline.com/artificial-intelligence-medicine-hope-or-hype (accessed Jan. 9, 2019).

11) Nick Triggle, *Care.data: How Did It Go So Wrong?* (Feb. 19, 2014), https://www.bbc.com/news/health-26259101 (accessed Jun. 14, 2019).
역자주: 옵트아웃 제도(opt-out:선사용·사후 배제)는 정보주체가 명시적으로 동의하지 않았더라도(명시적인 거부 의사를 밝히지 않는다면) 사업자가 개인 데이터를 활용한 후에 거부 의사를 밝히면 활용을 중지하는 방식이다. 장기기증 제도에서도 옵트아웃을 적용할 경우 장기기증 거부 의사를 밝히지 않았다면 잠재적 기증자로 추정하여 사망 후에 장기 적출이 가능하게 된다. 반면, 옵트인(opt-in) 제도는 정보주체가 개인 데이터 수집을 허용하기 전까지 개인 데이터 수집을 금지하는 것이다. 사전 동의에 의해서 개인 데이터를 수집, 활용할 수 있는 것을 원칙으로 한다.

12) Ellen W. Clayton et al., *A Systematic Literature Review of Individuals' Perspectives on Privacy and Genetic Information in the United States,* 13 Plos One 2 (2018).

13) 역자주: 우리나라의 경우 'DTC 유전자검사'로 통용된다. 보건복지부는 2020년 3월에 'DTC 유전자 검사 가이드라인'을 발표하였다.

는 추세를 띤다. 이러한 기기들은 대부분 사기업들에 개인정보와 건강 데이터가 유입되도록 만든다. 이와 같이 데이터 공유와 관한 개인의 상반된 태도는 프라이버시와 데이터 보호 규제의 주요 이슈로 대두되고 있다. 연구를 위하여 개인 정보의 접근성을 촉진하면서 동시에 시민들의 프라이버시 권리를 적절히 보장하는 것은 AI 기술의 힘을 빌어 의료 분야에서 혜택을 입고자하는 모든 국가의 정책 입안자들이 직면해야 할 가장 큰 과제 중 하나일 것이다.

새로운 「일반정보보호규정」(GDPR)을[14] 채택한 EU는 데이터 보호 법제를 통해 인공지능을 규율하려는 최초의 시도를 했다. 이 규정은 미국과 캐나다의 프라이버시 법제 개혁을 위한 물꼬를 터준 것이기도 하다. GDPR은 EU 내에 설립된 개인정보처리자와 수탁자에 의해 처리된 모든 개인 데이터를 규율한다. (GDPR 제3조 1항) 또한, 다음의 두 가지 상황에서 EU 국경 안의 모든 정보주체의 개인 데이터로 확장된다.[15]: 개인정보처리자가 EU 내에서 정보주체에게 상품이나 서비스를 제공하는 것과 연관되어 있는 경우, 그리고 EU 내에서 정보주체의 행동을 모니터링 하는 것과 관련이 있을 때이다. (GDPR 제3조 2항) 이는 많은 외국 기업들의 활동이 GDPR의 영역에 포함될 수 있다는 것을 의미한다. 더욱이, 이 새로운 개인정보보호규정의 역외 적용은 캐나다와 미국도 자체적인 프라이버시 법제를 개혁해야 한다는 압력을 주게 된다. 실제로 미국과 캐나다

14) Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). [2016] OJ L119/1.

15) 역자주: 원문에서 data controller와 processor는 우리나라 「개인정보 보호법」에서 개인정보처리자(제2조 5호)와 수탁자(제26조 제2항), data subject는 정보주체(제2조 3호)에 해당하므로, 각각 개인정보처리자(또는 약칭으로 '처리자'), 수탁자, 정보주체라는 용어로 사용한다.

양국의 시스템은 EU의 규정에 의해 설정된 새로운 요구 사항을 충족하지 못할 수 있다. 또한 법률들이 충분한 보호를 제공하지 못한다면, EU로부터 북미 즉, 미국과 캐나다로 흘러 들어갈 데이터는 감소할 것으로 보인다. 이는 추가적인 계약 조항의 합의가 이뤄져야하기 때문이다.[16] 이러한 데이터 감소는 양측의 인공지능 기술 연구 및 개발에 부정적인 영향을 끼칠 뿐 아니라 해당 분야의 협력 시도 자체를 저해할 수 있다.[17] 이러한 맥락에서 프라이버시 보호를 강화하고 모든 이해 관계자들의 신뢰를 얻기 위한 적절한 조치를 취하는 것이 매우 시급해 보인다. 건강 분야에 대한 인공지능의 기여도와 전망을 간략하게 살펴본 후, 이 분야의 발전으로 인한 데이터 및 프라이버시 보호에 대한 과제를 탐구한다. 이를 통해 GDPR에서 시사점과 영감을 얻어, 미국과 캐나다의 정책 개선점을 위한 핵심 방안들을 찾아낼 수 있을 것이다.

---

16) H. Evans and S. Togawa Mercer, *Privacy Shield on Shaky Ground: What's Up With EU-U.S. Data Privacy Regulations,* Lawfare (2018), https://www.lawfareblog.com/privacy-shield-shaky-ground-whats-eu-us-data-privacy-regulations (accessed Feb. 7, 2019); S. K. Robertson, Calls Grow for Canada to Modernize Privacy Laws Amid EU Changes, The Globe and Mail (2017), https://www.theglobeandmail.com/report-on-business/industry-news/marketing/calls-grow-for-canada-to-modernize-privacy-laws-amid-eu-changes/article35778176/ (accessed Feb. 7, 2019).

17) International collaboration in AI is based on increasingly large amounts of data, including trans-border data sets. If data exchanges are hindered, the continuation or development of transatlantic research projects in the field are thought to be impeded. See Mark Phillips, *International Data-Sharing Norms: From the OECD to the General Data Protection Regulation (GDPR),* 137 Hum. Genet. 575, 582 (2018).

# Ⅲ. 통합 인공지능 : 보건의료 시스템의 기회와 데이터 접근성 수요의 증가

인공지능에 대해서 단일한 개념 정의는 아직 존재하지 않는다. 캐나다 상원의 사회복지 및 과학기술 상임 위원회(Canadian Standing Senate Committee on Social Affairs, Science and Technology)에 의하면, 인공지능은 인간의 문제해결 능력, 추론 능력, 이해력, 인식 능력 등의 고유한 사고능력들이 컴퓨터를 통해 인공적으로 구현할 수 있는 인간의 인지 기능의 복제본으로 지칭된다.[18] 여러 보건의료 시스템에서 이미 머신러닝(ML) 및 딥러닝(DL) 기반의 인공지능 기술이 성공적으로 활용하고 있다.[19]

머신러닝과 딥러닝 모두에서, 결과물(output)을 생산해내기 위해 하나 이상의 알고리즘을 통한 프로세싱을 위해서 시스템에 일정량의 데이터(input)가 제공된다. 머신러닝은 논리적 추론을 기반으로 대량의 데이터에서 패턴을 자동 감지하는 데 주로 사용된다. 머신러닝과 딥러닝의 주요 차이점으로는 시스템에서 처리할 수 있는 데이터의 유형과 양, 알고리즘 생성 방법이 포함된다. 딥러닝은 인공신경망으로 알려진 보다 더 복잡한 형태의 머신러닝으로 설명된다. 딥러닝에서 시스템은 대량의 원시 자료와 복잡한 데이터를 처리할 수 있는 반면, 머신러닝은 기계가 이해할 수 있는 언어('구조적 데이터'라고 일컬음)로 전환되어야 하므로 딥러닝에 비해 정보의 수

18) K. K. Ogilvie and A. Eggleton, *Challenge Ahead: Integrating Robotics,* Artificial Intelligence and 3D Printing Technologies into Canada's Healthcare Systems 5 (2017).

19) F. Jiang et al., *Artificial Intelligence in Healthcare: Past, Present and Future,* 2 Stroke Vasc. Neurol. 230, 243 (2017).

집량이 더 적다. 이와 같이 딥러닝의 전망은 인공지능을 둘러싼 논의, 특히 보건의료 분야의 중심에 있어 왔다. 머신러닝에서 딥러닝으로 전환되면서 발생하는 주목할 만한 변화는 머신러닝이 '사람에 의해 만들어진', 감독에 의한 알고리즘이었다면, 딥러닝을 통해 얻어지는 결과물은 시스템에 의해 자체적으로 생성된다는 것이다. 또한, 이런 높은 수준의 복잡성은 딥러닝 시스템을 불투명하게 만든다. 프로그래머들은 시스템에 어떤 정보가 입력되어 그로 인해 무슨 결과물이 나왔는지를 알고 있지만, 이 결과물이 정확히 어떻게 생산되었는지를 이해하는 것은 거의 불가능하며, 통제하는 것 또한 거의 불가능하다.[20] 특수한 경우, 데이터가 알고리즘의 일부로 흡수되는 현상도 발생하는데, 일부 학자들은 딥러닝에서 이와 같은 투명성의 불안정한 결여 현상을 '블랙박스' 현상[21]으로 지칭한다.

딥러닝을 활용하여 환자들의 민감 정보를 다룰 때 많은 문제들이 제기됨에도 불구하고,[22] 보건의료를 위한 인공지능 연구는 급속도로 성장하고 있는 분야이다.[23] 오늘날의 보건의료 인공지능은 종양

---

20) W. Knight, *The Dark Secret At The Heart of AI-MIT Technology Review* (2017), https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai/ (accessed Jan. 9, 2019).

21) Roger A. Ford and W. Nicholson Price II, *Privacy and Accountability in Black-Box Medicine,* 23 Mich. Tech. L. Rev. 1 (2016); W. Nicholson Price II, *Regulating Black-Box Medicine*, 116 Michigan Law Review 421 (2017); T. Simonite, *AI Experts Want to End "Black Box" Algorithms in Government | WIRED,* Wired (2017), https://www.wired.com/story/ai-experts-want-to-end-black-box-algorithms-in-government/ (accessed Jan. 9, 2019).

22) 블랙박스 기술에 관하여 뉴욕대학교(NYU)의 AI Now 연구소는 형사사법, 의료, 복지, 교육 등 핵심 공공 영역에서는 '블랙박스' AI와 알고리즘 시스템 사용을 자제할 것을 권고한다.
A. Campolo et al., AI Now 2017 Report (2017), https://assets.ctfassets.net/8wprhhvnpfc0/1A9c3ZTCZa2KEYM64Wsc2a/8636557c5fb14f2b74b2be64c3ce0c78/_AI_Now_Institute_2017_Report_.pdf (accessed Jan. 9, 2019).

23) D. Faggella, *The State of AI Applications in Healthcare-An Overview of Trends,*

학(oncology), 신경학(neurology) 및 심장학(cardiology)의 세 가지 영역에 집중되어 있다.[24] 세 가지 모두 조기 발견이 필수적인 중요한 의학 분야다.[25] 임상 치료에서 인공지능 머신러닝과 딥러닝 시스템은 의사의 의사 결정을 지원하고 진단 및 치료에 대한 최신 정보를 제공한다. 인공지능과 영상의 결합은 특정 유형의 암이 존재하는지 여부를 신속하게 식별할 수 있도록 도움을 주는데 상당한 잠재력이 있음을 보여 주었으며, 때로는 전문가보다도 정확도가 높은 것으로 나타났다.[26] 또한 딥러닝 시스템은 향상된 예후 및 진단 모델을 사용하여 정밀 의료의 개발을 촉진할 수 있는 잠재력을 보이기도 했다.[27][28] 디지털 건강 기록 및 원격 진료도 의료 전문가가 특정 업무를 처리하는 데 소요되는 시간을 단축할 수 있는 상당한 능력을 보이면서 점점 더 널리 보급되고 있다.[29] 급속도로 고령화

---

Emerj (2018), https://emerj.com/ai-sector-overviews/state-ai-applications-healthcare-overview-trends/ (accessed Jan. 9, 2019).

24) Paulo J. Lisboa and Azzam F. G. Taktak, *The Use of Artificial Neural Networks in Decision Support in Cancer: A Systematic Review,* 19 Neural Netw. 408, 415 (2006).

25) 기존의 예측 방법보다 정확도가 높은 뇌졸중 진단과 예후를 위한 AI 기법도 개발이 되었다. Jiang et al., *supra* note 21.

26) 그 한 예가 2018년 Annals of Oncology 학술지에 발표되었는데, DL 시스템(악성 흑색종 진단을 위해 10만 개 이상의 피부 영상에서 훈련된 시스템)이 숙련된 의사 그룹을 능가한 결과를 보여주었다. V. J. Mar and H. P. Soyer, *Artificial Intelligence for Melanoma Diagnosis: How Can We Deliver on the Promise?* 29 Ann. Oncol. 1625, 1628 (2018).

27) C. Castaneda et al., *Clinical Decision Support Systems for Improving Diagnostic Accuracy and Achieving Precision Medicine,* 5 J. Clin. Bioinforma. 4 (2015).

28) Z. Obermeyer and Ezekiel J. Emanuel, *Predicting the Future-Big Data, Machine Learning, and Clinical Medicine,* 375 N. Eng. J. Med. 1216, 1219 (2016).

29) W. Glauser, *Artificial Intelligence, Automation and the Future of Nursing,* Canadian Nurse (2017), https://www.canadian-nurse.com/en/articles/issues/2017/may-june-2017/artificial-intelligence-automation-and-the-future-of-nursing (accessed Jan. 10, 2019).

되는 국가에서는 케어봇(carebot, 돌봄 로봇)과 기타 유사한 로봇의 사용이 증가하고 있다.[30]

보건의료 인공지능은 임상 돌봄이나 의사 결정 지원 외에도 다양한 역할을 수행한다. 인공지능 시스템은 환자의 의료 기록에서 유사점을 자동으로 파악함으로써 특정 임상 시험을 위한 최적의 환자 코호트를 신속하게 식별할 수 있도록 임상 연구를 지원할 수 있다.[31] 방대한 데이터 세트를 기반으로 수행되는 인공지능 시스템의 예측능력은 공중 보건에도 유익하게 작용할 수 있다. 빅데이터 기반 인공지능은 공중 보건 위험을 예측하고 이해하며, 한정적이고 균질한 소집단에 대해 맞춤형 치료를 제공하는데 도움이 되는 '정밀 공중보건(Precision Public Health)'의 개발에 기여했다.[32] 이러한 가능성을 극대화하기 위해 임상 시험과 의료에서 수집된 데이터에 대한 접근성을 개방함으로써 보건의료 시스템을 혁신하고자 하는 여러 제안들이 주목받고 있다.[33] 예컨대, '학습 보건의료 시스템(LHS: Learning Health care System)'의 패러다임은 '지식 생성이 임

30) D. Muoio, *Japan Is Running Out of People to Take Care of The Elderly, So It's Making Robots Instead Business Insider* (2015), https://www.businessinsider.com/japan-developing-carebots-for-elderly-care-2015-11 (accessed Jan. 9, 2019).

31) A. Sharafoddini, Joel A. Dubin and J. Lee, *Patient Similarity in Prediction Models Based on Health Data: A Scoping Review,* 5 JMIR Med. Inform. e7 (2017)

32) '공공 보건의 맥락에서의 정밀의료(precision)는 (1) 인구에서 질병, 병원균, 노출, 행동, 민감성 측정을 위한 새로운 방법과 기술을 적용함으로써 (2) 건강 증진을 위한 정책과 목표화된 실행 프로그램을 개발함으로써, 질병을 예방하고, 건강을 증진시키고, 인구 간 건강 격차를 줄이는 능력을 향상시키는 것으로 설명되어 왔다.' Muin J. Khoury and S. Galea, *Will Precision Medicine Improve Population Health?,* 316 JAMA 1357, 1358 (2016); See also S. Dolley, *Big Data's Role in Precision Public Health,* 6 Front. Public Health, 2 (2018), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5859342/ (accessed Jan. 24, 2019).

33) 예컨대, Ruth R. Faden et al., *An Ethics Framework for a Learning Health Care System: A Departure from Traditional Research Ethics and Clinical Ethics,* 43 Hastings Center Report S16, S27 (2013).

상 의학의 핵심에 포함됨으로써 보건의료 전달 과정에서의 자연스럽게 결과물이 발생되고 지속적인 돌봄의 향상을 가져오는' 보건의료 시스템을 의미한다.[34] 따라서 LHS는 의료 데이터(예: 디지털로 수집된 건강 관련 기록)에 대한 접근성을 개선하여 데이터 및 지식의 이전을 촉진하는 방식으로 연구와 임상의 통합을 기반으로 한다. LHS가 수반하는 연구와 임상 간의 경계를 모호하게 하고, LHS의 이런 특징은 전통적인 법적 윤리적 규범과도 어느 정도 상충된다. 그 규범들은 환자와 연구 대상자를 보호하기 위해서는 연구와 임상 치료가 명확하게 구획되어야 한다는 신념을 바탕으로 만들어진 것이었다.[35] LHS 패러다임은 이제 보다 적절하고 윤리적이며 규제적인 새로운 법체계[36]를 필요로 한다. 이 새로운 체계는 보건의료 산업의 핵심적인 추진력이 되는 프라이버시와 데이터 보호 메커니즘을 통합하는 것이어야 한다.

# Ⅳ. 프라이버시와 데이터 보호를 위한 함의

## 1. 프라이버시를 위한 함의

프라이버시는 개인이 자신의 정보에 대한 접근을 제어할 수 있는

34) L. Olsen, D. Aisner and J. Micheal McGinnis, *The Learning Healthcare System: Workshop Summary* 6 (2007). 4.

35) Tom L. Beauchamp and Y. Saghai, *The Historical Foundations of the Research-Practice Distinction in Bioethics,* 33 Theor. Med. Bioeth. 45, 56 (2012); See also G. Bertier, A. Cambon-Thomsen and Y. Joly, *Is it Research or Is It Clinical? Revisiting an Old Frontier Through the Lens of Next-Generation Sequencing Technologies,* 61 Eur. J. Med. Genet. 634, 641 (2018).

36) Faden et al., *supra* note 35 at 29.

권리라고 이해된다. 이는 건강 데이터, 종교적 신념, 정치적 견해 및 성적 취향과 같이 본인만 알고 있거나 소수의 사람들과만 공유한 정보들과 연관이 되어있다. 인터넷과 인공지능이 발전함에 따라 프라이버시권은 현대 프라이버시 법률이 개발될 당시만 해도 예상치 못한 전례 없는 도전에 직면하고 있다.[37] 데이터 보호를 둘러싼 미국과 캐나다, 유럽의 프레임의 차이점은 프라이버시 보호를 위한 각각의 확립된 기초적인 개념에서 찾아볼 수 있다. 미국과 대부분의 영국계 캐나다 지방에서는 프라이버시 보호가 자유를 수호하는 데 기반을 두고 있는데, 그 중 특별히 정부로부터의 간섭을 배제해야 한다는 자유의 개념을 중요하게 다룬다. 프라이버시에 관한 미국의 법체계는 연방 법률, 주 법률 그리고 업종별 규정 등으로 이어붙인 조각보 같아서 복잡하고 때로는 상충한다.[38] 반면, 유럽과 캐나다는 프라이버시와 데이터 보호에 대해 보다 균일하고 포괄적인 접근 방식을 채택했다. 유럽과 캐나다에서, 특히 퀘벡 주에서 프라이버시는 인간 존엄성을 위한 권리의 필수 구성 요소로 간주된다. 캐나다의 프라이버시 개념은 'EU와 미국의 중간' 정도인데, 이는 캐나다가 미국과 같이 정부의 간섭을 염려하면서 동시에 민간 부문에서 개인정보를 남용하는 문제에 대해 깊이 우려하기 때문이다.[39] 프라이버시는 1953년 이래 유럽 인권협약(ECHR 제8조)에서 기본적 인권으로 확립되었다. 퀘벡 헌장(CHRF, QC 제5조)에서도 이와

37) O. Diggelmann and M. Nicole Cleis, *How the Right to Privacy Became a Human Right,* 14 Hum. Rights Law Rev. 441, 458, 442 (2014).

38) J. Halpert, J. Kashatus and K. Lucente, *Data Protection Laws of the World: The United States* (2017) https://www.dlapiperdataprotection.com/index.html?c=US&c2=&go-button=GO&t=law (accessed : Jan. 17, 2019).

39) A. Levin and M. Jo Nicholson, *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground,* 2 U. Ottawa L. & Tech. J. 357, 396, 357 (2005).

유사하게 인정된다. 그러나 미국과 영국계 캐나다의 경우, 헌법적 권리로 명문화되어 있기 보다는 사법적인 해석으로부터 프라이버시권이 도출되고 있다.[40] 이러한 개념상의 차이를 넘어서, 대서양을 사이에 둔 양 대륙의 개인들은 개인의 프라이버시에 대해 점점 더 역설적인 태도를 보이고 있다. 즉 사람들은 보건 연구를 위해 데이터 접근을 승인하는 것은 꺼리는 반면, 휴대용 기기와 소비자 유전자 검사 웹사이트를 통한 개인 데이터는 대개 정기적으로 공유하려는 경향을 보인다.[41] 이러한 역설적인 행태는 소비 습관과 같이 온라인으로 제공되는 다른 개인 데이터로부터 보건 건강 데이터가 종종 논리적으로 추측된다는 점과 관련이 있다.[42] 이 현상은 프라이버시 보호와 규정에는 큰 걸림돌이 된다. 명백한 사례를 들자면, 2016년 미국 대통령 선거 운동을 지원하기 위해 페이스북이 수집한 개인 데이터를 불법적으로 사용한 사례가 있다.[43] 언론에서 심각하게 다뤄진 이 사건은 동의 없이 상업적 또는 정치적 목적으로 개인 데이터가 사용될 위험성을 대중에게 알리는 계기가 되었다. 인터넷

---

40) P. Bender, *The Canadian Charter of Rights and Freedoms and the United,* 28 McGill L. J. 56, 820 (1983).

41) S. Armstrong, *What Happens to Data Gathered by Health and Wellness Apps?* 353 BMJ 353 (2016).

42) 2012년 뉴욕타임스(NYT)에서 밝혀진 대로, 소매상점인 타겟(Taget)은 적절한 시기에 홍보 쿠폰을 보낼 목적으로, 구매 습관에 따라 여성이 임신 중인지 여부와 대략의 출산일을 알아냈다.
C. Duhigg, *How Companies Learn Your Secrets,* The New York Times (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html (accessed Jan. 10, 2019).

43) 역자주: 캐임브리지 애널티카 (Cambridge Analytica)사례이라고 칭하며, 각주 88에서 다시 상술한다.
O. Solon and O. Laughland, *Cambridge Analytica closing after Facebook data harvesting scandal The Guardian* (2018), https://www.theguardian.com/uk-news/2018/may/02/cambridge-analytica-closing-down-after-facebook-row-reports-say (accessed Mar. 13, 2019).

상에서 개인 데이터의 원치 않은 사용을 방지, 예방하기 위해 적용될 수 있는 프라이버시 보호 프레임워크와 거버넌스의 체계가 부족하다는 점도 부각되었다.

데이터의 2차적 사용과 오남용은 유럽의 입법자들이 GDPR을 채택할 때 해결하고자 했던 문제다. 의료 분야에 적용하는데 있어서, GDPR은 이중목적을 가지고 있다. 한 면으로는 (사적 영역과 공공 영역 모두에서) 동의를 받지 않은 2차적 사용을 엄격히 방지하는 것을 목표로 한다. 다른 한 면으로는 프라이버시 보호의 중요성을 염두에 두면서도 연구 개발에서 점점 수요가 증가하고 있는 데이터 접근성을 간소화하는 것을 목표로 한다. 그런 의미에서, GDPR은 건강 데이터에 접근하고 사용하기 전에 행정적이고 형식적인 절차에 따른 의무의 감소를 제공한다. 지침에 따라 국가 당국에 대한 엄격한 신고 절차가 시행된 경우, GDPR은 우선 연구를 시작할 수 있는 능력을 제한하는 대신 데이터 행위자[44]가 더 책무성을 갖도록 하는 것을 목표로 한다.[45] 특히나 건강 관련 데이터는 '민감정보'로 분류된다. 이러한 데이터는 처리를 금지하는 특별한 보호 체계로서 보호된다(GDPR 제9조). 그러나 민감성을 인정받으면서도 관련 데이터에 용이하게 접근할 수 있도록 상당수의 예외를 두고 있다.

---

44) 역자주: 원문에서 data actors라고 지칭하는 것은 개인정보처리자와 수탁자를 의미한다. 원문의 표현을 살리기 위하여 data actors는 '데이터 행위자'라는 용어로 사용한다. 뒤에서 데이터 사용자(data user)로 지칭하는 것도 개인정보처리자와 수탁자를 지칭한다.

45) European Commission, *The GDPR: New Opportunities, New Obligations* (2018), https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-sme-obligations_en.pdf (accessed Feb. 6, 2019).

## 2. 데이터 보호를 위한 함의

법체계에 따라서는 별개의 권리로 정해진 경우가 간혹 있지만, 일반적으로 데이터 보호에 관한 권리는 프라이버시권의 필수 구성요소다. 결과적으로, 데이터 보호를 보장받을 수 없는 경우 프라이버시에 대한 존중도 역시 보장받기 어렵다. 캐나다와 미국에서는 데이터 보호 규정에 개인 데이터의 수집 및 사용이 포함된다. 그러나 인공지능은 개인 데이터를 기반으로 하지 않는 경우가 있기 때문에, 이러한 상황에서는 데이터 보호 규정이 적용되지 않게 된다. 개인 데이터와 비개인 데이터의 정의 기준은 데이터 규정의 적용 범위를 결정하는 데 매우 중요하게 된다. 그러나 EU는 비개인 데이터를 규율할 특별한 규정을 적용하고 있다. 이러한 규정은 비개인 데이터의 자유로운 순환을 증진하고 EU 내에서 일반적인 디지털 시장의 발전을 촉진하는 것을 목표로 한다.[46]

일반적으로 개인 데이터는 정보주체를 직접·간접적으로 – 예컨대 삼각검증 등의 방법으로- 식별할 수 있는 데이터이다.[47] 캐나다 연방법은 개인 정보를 '식별 가능한 개인에 대한 정보'(PIPEDA 제2조)로 정의한다. 이 정의는 '식별되거나 식별 가능한 자연인(데이터 주제)과 관련된 모든 정보'(GDPR 제4조)라고 규정하고 있는 GDPR의 정의 개념과 유사하다. 미국에서는 적용 가능한 규정이 부처와 주마다 다르기 때문에 개인 데이터와 관련된 정의 개념이 다양하다.[48] 간략히 말하자면, 세 관할권 모두 개인 데이터로 간주되

46) Regulation (EU) 2018/1807 of the European Parliament and of the Council of November 14, 2018 on a framework for the free flow of non-personal data in the EU. [2018] OJ L119/1.

47) L. Pangrazio and N. Selwyn, '*Personal Data Literacies': A Critical Literacies Approach to Enhancing Understandings of Personal Digital Data,* 21 New Med. & Soc. 419, 437 (2019)

는 점이 상당히 유사하다. 그러나 프라이버시가 실제로 보호되는 방법에는 차이점이 있다. 특히 새로운 유럽의 규정은 개인 데이터와 비개인 데이터의 통상적인 분류를 뛰어넘는다. 건강, 유전자 데이터 및 생체 데이터에 관한 데이터는 고도로 민감한 것으로 간주된다. '민감 정보'에는 다른 유형의 개인 정보(GDPR 제6조)에 적용할 수 있는 것보다 GDPR에 의한 더 강화된 보호체계가 부여되며, 모든 민감 정보의 처리는 GDPR에 따라 금지되지만 제9.2조에는 일반적인 금지 원칙에 대한 예외사항의 목록이 명시되어 있다. 이 예외사항 중 첫 번째는 '정보주체가 하나 이상의 특정 목적을 위해 해당 개인 데이터를 처리하는 데 명시적으로 동의한 경우(GDPR 9.2조 a)'이다. 흥미롭게도 이러한 예외사항들이 대체 조건들로 설정된다. 즉 이 조항의 문구는 다른 법률로서 데이터 처리의 법적 근거가 적용되는 한, GDPR 동의 하에 요구되는 특정한 설명에 의한 동의(informed consent)를 얻을 필요가 없다는 것을 의미한다. 예컨대 적절한 보호 조치가 마련된 경우(GDPR 제89조), '공공의 이익, 과학 또는 역사적 연구 목적용 또는 통계용으로 아카이빙 목적에 필요한 경우(GDPR 제9.2조 j),' 민감 정보의 처리가 허용된다. GDPR의 목표는 민감 정보를 사용하는 과학 연구의 맥락에서 다소 융통성을 허용하는 것이라고 판단된다. 그러나 EU 회원국은 '유전자 데이터, 생체 데이터 또는 건강 관련 데이터 처리와 관련하여 제한 사항을 포함한 추가 조건을 유지하거나 도입할 수 있으며 (GDPR 제9.4조, 89조),' '특정 조항으로 동의의 요구조건을 강화할

48) D. Thoren-Peden and C. Meyer, *Data Protection 2018 International Comparative Legal Guides,* in Data Protection 2018 | Laws and Regulations | USA | ICLG (2018), http://iclg.com/practice-areas/data-protection-laws-and-regulations/usa (accessed Feb. 7, 2019).

수 있다(제 6.2조, 9.2.a, GDPR).' 필자들의 관점에서는 이러한 재량의 부여는 GDPR의 목표를 저해할 수 있으며, 국제적인 조화 계획에 악영향을 줄 수 있기 때문에 비판을 받아왔던 것이다.[49]

흥미롭게도, 미국에서는 연방 규정이 규정한 단체가 특정 유형의 데이터로 수집한, 보호된 건강 정보(이하, PHI 라고 칭함, Protected Health Information)도 규율한다.[50] 「건강보험 이전 및 책무에 관한 법」(이하, HIPAA 라고 칭함, Health Insurance Portability and Accountability Act)[51]는 1996년부터 PHI의 수집 및 사용에 대한 표준을 제공해왔다. 그러나 건강 데이터 및 환자의 프라이버시를 적절하게 보호할 만한 HIPAA의 효과는, 적용 범위의 제한성 때문에 상당한 어려움을 겪어왔다. HIPAA는 '담당 법인'(covered entities)과 '거래처'(business associates)가 처리한 데이터에만 적용된다. 즉, 데이터 마이닝을 하는 주체들이 전형적으로 적용대상에서 제외된다는 것을 의미한다.[52] 건강 관련 데이터를 포함한 많은 양의 개인 데

---

49) 민감 정보를 처리하기 위해 제한적이고 이질적인 조건을 채택하면 회원국들 간에 EU 내 법률 충돌을 야기할 수 있으며, 이는 결국 특히 유전학 분야에서 국경 간 연구를 방해할 수 있다.
K. Pormeister, *Genetic Research and Applicable Law: The Intra-EU Conflict of Laws as a Regulatory Challenge to Cross-Border Genetic Research,* J. Law Biosci. (2019), https://academic.oup.com/jlb/advance-article/doi/10.1093/jlb/lsy023/5172932 (accessed Jan. 3, 2019).

50) PHI의 예로는 인구통계학적 데이터, 의료 기록, 시험 결과, 보험 정보 및 환자를 식별하거나 의료 서비스 또는 의료 서비스 범위를 제공하는 데 사용되는 기타 정보를 포함하고 있다.
What is Protected Health Information? HIPAA Journal (2018), https://www.hipaajournal.com/what-is-protected-health-information/ (accessed Jan. 24, 2019).

51) The Health Insurance Portability and Accountability Act of 1996 (HIPAA). P.L. No. 104-191, 110 Stat. 1938 (1996).

52) A. Tanner, *Strengthening Protection of Patient Medical Data The Century Foundation* (2017), https://tcf.org/content/report/strengthening-protection-patient-medical-data/ (accessed Mar. 13, 2019).

이터를 매일 처리하는 구글, 아마존과 같은 대기업들은 일반적으로 이 규정에 포함되지 않는다.[53] 더구나 HIPAA의 '프라이버시 규칙'은 식별 가능한 정보만 보호한다. (160장과 164장). 미국 법률에 따라 '비식별(de-identification)' 정보는 비개인 정보로 간주되므로 데이터 보호 규정이 적용되지 않는다. HIPAA 하에서, 비식별 처리는 두 가지 방식으로 완료될 수 있다. 하나는 데이터 세트에서 법률에 열거된 특정 식별자를 제거하는 것이고, 다른 하나는 통계 전문가가 특정 데이터 세트에 연결된 재식별(re-identification) 위험이 충분히 작다는 것을 확인해주는 것이다 (HIPAA 45 CFR § 164.514(b)(1)). 이 두 가지 비식별 기술은 정보주체의 모든 재식별을 방지하기에 불충분한 것으로 입증되었다.[54] 따라서 HIPAA 비식별 기준은 게놈 데이터(genomic data)와 유전자 데이터(genetic data)의 경우에 특히 문제가 있는 것으로 간주된다. 이러한 유형의 데이터는 통상적으로 데이터세트와 관련된 모든 개인정보(예: 이름, 연령, 주소 등)가 제거되면 비식별화된 것으로 간주되어, HIPAA의 적용 범위를 벗어나게 된다. 이는 유전자 정보의 실제적인 비식별화가 가능하지 않고 이러한 유형의 데이터가 민감할 수 있음에도 불구하고 발생한다.[55] 이 경우, 연방 (예컨대, 「유전자정보 차별금지법」) 또는 각 주 차원의 다른 법률이 때때로 추가적인 보호조치를 제공할 수 있다.

GDPR에 따르면, 비식별 처리가 개인의 재식별 방지를 위한 충분

53) Nicholson W. Price and Glenn I. Cohen, *Privacy in the Age of Medical Big Data,* 25 Nat. Med. 37, 43, 39 (2019).

54) K. Benitez and B. Malin, *Evaluating Re-identification Risks With Respect to the HIPAA Privacy Rule,* 17 J. Am. Med. Inform. Assoc. 169, 177 (2010).

55) J. Kulynych and Henry T. Greely, *Clinical Genomics, Big Data, and Electronic Medical Records: Reconciling Patient Rights With Research When Privacy and Science Collide,* 4 J. Law. Biosci. 94, 132, 122 (2017).

한 방법으로 자동적으로 간주되는 것은 아니다. 따라서 비식별화된 데이터는 보호되는 개인 정보의 범주에 여전히 남아 있게 된다. GDPR은 익명 데이터만을 적용 범위에서 제외한다. GDPR에 따라 익명화와 관련하여 엄격한 조건이 설정된다. 익명화 과정에는 재식별을 방지하기 위해 특별히 고안된 많은 기술들이 있다. 이러한 기술들에 대해서 전문 26은 다음과 같이 명시하고 있다.

> "어떤 개인이 식별되는지 여부를 판정하기 위해서는, 예컨대 선별과 같이, 제3자 또는 처리자가 개인을 직접·간접적으로 식별하기 위해 사용할 것으로 합리적으로 예상되는 모든 수단들이 고려되어야 한다. 어떤 수단들이 자연인을 식별하는데 사용될 수 있는 합리적인 가능성이 있는지 여부를 확인하기 위해서는, 데이터 처리와 기술 개발 시점에 활용 가능한 기술과 기술적 발전을 감안하여, 식별을 위해서 요구되는 시간과 비용과 같은 모든 객관적인 요인들을 고려해야 한다."

민감 정보로 분류하는 것은 건강 관련 데이터를 다룰 때 통상의 주의보다 추가적인 주의를 기울여야 함을 알려주기에 이점이 있다. 동의를 획득하지 않은 2차적 사용을 방지하는 것이 효율적일 수 있지만, 민감 정보의 유출시 특히 엄격한 제재가 주어진다는 점을 고려한다면, 이런 특별 분류는 연구자들에게는 불리한 요인으로 작용될 수 있다.

개인정보와 민감 정보의 법적 구분은 캐나다의 데이터 보호 규정에는 존재하지 않는다. 연방 차원에서 데이터 보호는 민간 부문에 적용되는 「개인정보보호 및 전자문서 법」(PIPEDA)[56]과 연방 기관

56) Personal Information Protection and Electronic Documents Act (PIPEDA), SC 2000, c 5b.

에 적용되는 「프라이버시법」의 두 가지 주요 규제 수단으로 보호된다. 몇몇 주에서는 건강 정보와 관련된 자체 규정을 채택했는데 이는 실질적으로 유사한 것들이라 할 수 있다.[57] PIPEDA 및 이와 동일한 조항들은 상업적 목적으로 개인 데이터를 수집, 사용 또는 공개하는 민간 조직에 적용된다. 그런 의미에서 적용 범위는 회사가 수행하는 개인 데이터 처리 (PIPEDA 제2조)를 포함하므로 HIPAA보다 적용 범위가 더 포괄적이다. 이전의 데이터 보호 지침에 따라, PIPEDA는 EU 법률이 적용되는 개인 데이터를 보호하기에 적합한 것으로 간주되었다.[58] EU에서 캐나다 회사로의 데이터 흐름을 보장하는 데에는 적합성이 매우 중요하다. GDPR 제46.5조에 따라 PIPEDA는 다음 평가까지 이러한 우호적 지위로부터 혜택을 얻을 수 있다. 민감 정보를 포함하여 특정 보호 메커니즘의 결여는, PIPEDA가 적합성을 유지하는 데 방해가 될 수 있다. 이러한 지위가 없다면, 각각의 국제적인 개인 데이터 이전은 예외적으로만 허용한다. 이러한 예외적인 경우는 데이터의 주체가 적합성과 관련한 결정의 부재와 관련 위험성에 대해 고지를 받은 후 명확하게 동의를 한 경우를 포함한다.(GDPR 제49.1.조 a). 또 다른 경우로는 정보주체와의 계약을 이행하기 위해 데이터 이전이 필요한 경우, 또는 '중대한 공공의 이익(제49.1.b조 및 49.1.d조)의 이유'를 위해 이전이 필요한 경우다. 이러한 요구조건은 예컨대 딥러닝 시스템을 개발하기 위해 많은 양의 데이터가 필요한 경우에 있어서 특히나 실용적이지

57) Office of the Privacy Commissioner of Canada, Summary of privacy laws in Canada (2014), https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/ (accessed Jan. 9, 2019).

58) J. Stoddart, B. Chan and Y. Joly, *The European Union's Adequacy Approach to Privacy and International Data Sharing in Health Research,* 44 J. Law Med. Ethics 143, 155 (2016).

못할 수 있다.

PIPEDA는 아직 인공지능이 프라이버시와 데이터 보호에 대해 끼칠 수 있는 영향을 고려하지 못하고 있는 상태이고, 특히나 민감 정보와 건강 관련 정보의 경우에 더욱 그러하다. 정치적 목적으로 개인정보를 페이스북에서 불법적으로 사용하는 것에 대해 폭로를 개진한 논평에 따라, 캐나다의 프라이버시 커미셔너 (Privacy Commissioner of Canada)는 프라이버시에 대한 캐나다 법제의 제한성에 대해 경고하고 PIPEDA의 개정을 촉구했다.[59] 프라이버시 커미셔너가 작성한 권고안과 의거하여, 하원의 정보 접근성 및 프라이버시 윤리 위원회 (Committee on Access to Information, Privacy and Ethics of the House of Commons)는 PIPEDA에 대해 유사한 개정 제안 내용을 담고 있는 보고서를 발표했다. 위원회는 유럽의 규정에 대한 적합성 지위를 유지하고 EU와의 상업상의 거래의 감소를 유발하는 잠재적인 냉각효과를 방지하기 위해 캐나다 법률을 조정해야 한다고 강조한다.[60] 한편, 캐나다 학술 협의회(Council of Canadian Academies)는 데이터 규제에 관한 현재 캐나다의 법체계가 프라이버시 보호에도 성공적이지 못할 뿐만 아니라 건강 연구에 있어서

59) 'Canada's archaic privacy laws are not up to that task. Modern laws are urgently needed to protect us, as both citizens and consumers. (. . .) Trust needed to allow the digital economy to flourish hinges on having an appropriate legal framework' D. Therrien, *Op-ed: Facebook allegations underscore deficiencies in Canada's privacy laws* (2018), https://www.priv.gc.ca/en/opc-news/news-and-announcements/2018/oped_180326/ (accessed Jan. 24, 2019). 역자주: 캐나다의 프라이버시 커미셔너는 캐나다인의 프라이버시권 침해를 주장하는 민원 사건을 조사하고「프라이버시법」위반 여부를 의회에 보고하는 캐나다 의회의 사무관이다.

60) Recommendation 16, *Towards Privacy by Design: Review of The Personal Information Protection and Electronic Documents Act* (2018), https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/report-12/ (accessed Mar. 13, 2019).

적기에 이루어져야 하는 데이터 접근성도 심각하게 방해하고 있다고 논평하였다. 협의회의 의견을 보도한 자료에 의하면, 정책 입안자들이 직면하는 딜레마와 이를 해결하기 위한 법개정의 필요성의 증가를 지적하고 있다.[61]

> "캐나다에서는 다른 법체계와 같이 동시에 두 가지 근본적인 목표를 충족해야한 하는 주요하고도 매우 중대한 어려움에 직면해있다. 하나는 공공의 이익에 속하는 연구용으로 건강 데이터와 건강 관련한 데이터에 관한 접근성을 부여하는 것이고, 또 다른 하나는 캐나다 국민들의 프라이버시를 보호하고 국민들의 정보가 연구에 사용될 때 그 정보의 기밀성을 유지해 주는 것이다."

프라이버시를 보다 효과적으로 보호하고, 동의를 받지 않은 데이터 사용을 금지하며, 데이터 공유를 통해 연구를 증진하기 위해, 캐나다와 미국의 법체계도 상당한 개정의 필요성에 직면하고 있다. 앞으로의 개정 작업은 본인의 데이터에 대한 개인의 권리를 강화하는 것을 목표로 설정해야 한다. GDPR에서 구현된 혁신적인 권리뿐만 아니라 새로운 동의 요건은 개인이 본인 자신의 프라이버시를 보호하는 것에 보다 적극적으로 대처할 수 있도록 설계되어, 규제기관에도 흥미로운 영감의 원천을 제공한다. 또 한편으로 GDPR은 미국과 캐나다의 상황에서 데이터 행위자에 대한 강화된 의무사항을 제공하고 있다.

---

61) *Council of Canadian Academies, Accessing Health and Health-Related Data in Canada* 15 (2015).

# Ⅴ. 캐나다와 미국의 프라이버시 및 데이터 보호 증진: GDPR로부터의 시사점

## 1. 권리 강화: 개인정보에 대한 데이터 소유자(data owners)의 통제력 강화

### 가. 동의권과 자동화된 처리

개인들에게 본인의 개인정보에 대한 더 높은 통제력을 부여할 수 있도록, GDPR은 제7조에 의거하여 유효한 동의(valid consent)에 관한 요구사항을 강화하고 있다. 유효한 동의는 현재 '자유롭게 제공되고, 구체적이며, 사전에 고지되고-사전에 정보가 제공되고-, 모호하지 않은 것(GDPR 제4.11조)'으로 정의된다. GDPR은 동의가 반드시 서면으로 이루어져야 한다고 명시하지는 않지만, 명확해야 하며 사전정보를 제공해야 한다. 전문 32는 이 부분을 '그러므로 묵시적이며 사전에 체크 표시하는 형태의 수동적인 방식으로는 동의가 성립되지 않는다'라고 구체화 한다. GDPR에 따른 명시적이고 유효한 동의를 구성하는 것을 평가하기 위한 보다 구체적인 단계는 여전히 국가 법체계의 해석에 따라 상이할 수 있다.[62] 이러한 재량권은 동의 모델의 타당성을 평가할 때 법원에 충분한 융통성을 부여하는 것을 의미한다. 이러한 새로운 요구 사항은 엄격한 관료적인 절차에 비해 의미 있는 동의 절차의 사용을 장려하는 것이다. 이는 일차적으로 개인 데이터에 대한 본인의 통제력을 향상시킴으로 최적의

62) Martin Coulter, *What is GDPR? Everything You Need to Know About the New EU Laws,* Evening Standard (2018), https://www.standard.co.uk/news/uk/what-is-gdpr-everything-you-need-to-know-about-the-new-eu-data-protection-laws-a3847396.html (accessed Jan. 16, 2019).

데이터 공유에 필요한 신뢰도를 높이기 위한 것이다. 그러나 동의 요구 사항이 더 엄격한 경우, GDPR에 의해 많은 예외사항이 설정되어 민감한 데이터(민감 정보)와 민감하지 않은 데이터(민감 정보가 아닌 데이터)를 모두를 처리할 수 있도록 허용할 수 있다. 모든 처리에는 법적인 근거가 필요하며, 유효한 동의는 민감 정보가 아닌 데이터를 다루기 위해 나열된 제6조의 근거들 중 하나일 뿐이다.[63] 그 외 5가지 다른 근거는 '정보주체가 당사자인 계약의 이행을 위해 개인 데이터의 처리가 요구된 경우' 또는 '공익을 위해 사용된 업무(GDPR 제6조 1항 (b) (e))'를 포함한다. 결과적으로, 다른 근거가 적용될 수 있는 한, 유효한 동의를 얻는 것만으로는 데이터 처리의 합법성이 유효하게 되지는 않는다는 것이다.

민감 정보의 경우에, 제9조는 동의에 근거한 처리가 사전 정의된 목적으로만 제한되어야 하며, 동일한 데이터에 관한 추가적인 처리를 할 경우에는 동의를 다시 얻어야 한다는 것을 의미한다고 명시하고 있다. 그러나, 과학적 연구 목적을 위한 프로세스인 경우, 데이터의 2차적 사용도 허용된다(GDPR 제89.1조). 여러 목적으로 동일한 데이터 세트를 사용하도록 허용하는 것은 대부분의 과학적 개발에 결정적이지는 않더라도, 유익한 것으로 생각된다.[64] 그러나

63) 역자주: GDPR 제6조 처리의 적법성 1. 개인정보 처리는 적어도 다음 각 호의 하나에 해당되고 그 범위에서만 적법하다. (a) 정보주체가 하나 이상의 특정 목적에 대해 본인의 개인정보 처리를 동의한 경우 (b) 정보주체가 계약 당사자가 되는 계약을 이행하거나 계약 체결 전 정보주체가 요청한 조치를 취하기 위해 처리가 필요한 경우 (c) 개인정보처리자의 법적 의무를 준수하는데 개인정보 처리가 필요한 경우 (d) 정보주체 또는 제3자의 생명에 관한 이익을 보호하기 위해 개인정보 처리가 필요한 경우 (e) 공익을 위하거나 개인정보처리자의 공식 권한을 행사하여 이루어지는 업무수행에 처리가 필요한 경우 (f) 개인정보 처리자 또는 제3자의 정당한 이익 목적을 위해 처리가 필요한 경우로서, 개인정보가 보호되어야 할 정보주체의 이익 또는 기본적 권리와 자유가 우선되는 경우는 제외한다. 정보주체가 어린이인 경우에는 특히 그러하다.

전문 156은 다음과 같이 명시하고 있다;

> "공공의 이익, 과학 또는 역사적 연구 목적 또는 통계 목적으로 보관하는 개인 데이터의 추가 처리는, 처리자가 정보 처리에 의해 소정의 목적들이 충족될 타당성이 있다고 평가했을 때 실행되어야 한다. 그 데이터는 정보주체의 식별을 허용하지 않거나 더 이상 허용하지 않는 것들이고 적절한 안전장치를 거쳐 제공된 데이터이어야 한다."

따라서 사전에 정보주체로부터 새로운 동의를 얻지 않고 데이터를 2차적으로 사용하는 것은 GDPR에 따라 예외적으로 인정되지만, 엄격한 조건에 의해 제약을 받아 궁극적으로 연구원이 GDPR의 예외 사항을 이용하지 못할 수도 있다. 새로운 동의 요구 사항은 미국과 캐나다의 법체계 모두에 흥미로운 개선점을 제공하는데, 이는 정보주체간의 신뢰를 생성하는 데 도움이 될 수 있다.

캐나다와 미국의 양측의 법체계에서, 개인 정보의 사용 및 처리에 일반적으로 유효한 동의를 요구한다. 그러나 유효한 동의 구성이 GDPR의 새로운 성향, 특히 명백성의 지점과 무조건 일치하는 것만은 아니다. 새로운 유럽의 규정과 북미의 법 사이의 유효한 동의 요건의 차이점은, PIPEDA 혹은 HIPAA 상에서는 합법적이었던 데이터 처리가 유럽의 법제 하에서는 불법이 될 수도 있다는 것을 의미한다. 특히, GDPR은 '옵트 아웃' 기반의 참여, 예컨대 정보주체가 사실상 동의한 것이 명확하지 않은 것 같은 묵시적 동의 시나리오를 방지하려는 의도를 가지고 있다. 따라서 GDPR이 적용되는

64) G. Chassang, *The Impact of the EU General Data Protection Regulation on Scientific Research,* 11 Ecancermedicalscience 709 (2017).

개인 데이터를 다루는 회사의 주요 과제는 동의가 명확하게 사전에 고지되고 표현되도록 보장하는 것이다. 이 새로운 동의 요건으로 인해 프랑스의 국가 프라이버시 보호 관청이 거대 회사인 구글을 상대로 5,000만 유로 – 약 7,500만 달러의 벌금을 부과하기도 했다. 당국은 미국 기업이 사용자들에게 '구글이 시행한 조치의 정도를 이해할 수 없게 했다'는 동의 요구 설정에 대해 비난했다.[65] 이 사건은 앞으로의 GDPR 규정과 북미의 법률 사이에 어떤 문제들이 갈등할지를 보여준다.

개인의 프라이버시와 이익을 더 보호하기 위해 양 국의 법체계에 동의 요구 사항의 수정이 필요하다면, 유용한 기술 개발을 지연시키지 않기 위해 과학 연구의 특수성 또한 고려되어야 한다. 수집된 데이터의 잠재력을 예측하기가 어렵기 때문에, 사전 결정된 목적으로만 사용 제한되는 특정한 동의 요구 사항은 연구 상황을 상당히 제한시킬 수 있다. GDPR 전문 33은 이러한 부분을 인정하지만 GDPR의 의무를 피할 수 있는 수단을 제공하지는 않는다.[66] 개인정보 처리 관련 보호를 위한 실무그룹(The Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, 이하 '실무그룹'이라고 칭한다)은 이러한 이슈에 대해서 고지에 의한 동의(informed consent)를 얻지 못하는 경우에 다른 방법을 사용할 것을 제안한다. 예컨대, 연구가 진행됨에 따라 후기 단계에서 동의를 얻을 수 있다고 하는, 보다 일반적인 용어로서 초기단계에 연구를 정의하는 것도 가능하다.[67] 실무그룹은 몇몇의 경우에

65) CNIL, DÚlibÚration SAN-2019-001 (2019).

66) '데이터 수집 시 과학적 연구 목적을 위한 개인 데이터 처리 목적을 완전히 파악할 수 없는 경우가 많다. 따라서 정보주체가 과학 연구에 대해 공인된 윤리적 기준에 부합할 때 과학 연구의 특정 분야에 대한 동의를 할 수 있도록 허용해야 한다.' (GDPR 전문 33)

적용될 수 있는 동적 동의(dynamic consent)라고 알려진 또 다른 형태의 동의를 인정했는데, 동적 동의란 현대 의사소통 전략을 기반으로 한 모델로, 대상에게 데이터의 다양한 용도에 대해 지속적이고 적절하게 정보를 제공하는 것을 일컫는다. 설득력 있게 보이지만, 동적 동의를 통한 접근 방식은 대규모 연구에서 이 모델을 다룰 때에는 연구자에게 부담이 될 수도 있다는 지적이 있다. 연구에 친화적인 일반화된 형태의 포괄적 동의(broad consent)가 이에 대한 대안이 될 수 있다. 이것은 데이터의 활용이 고려될 때마다 매번 동의를 구할 필요 없이 특정 유형의 미래 연구를 위해 잘 정의된 프레임워크에 대해 동의가 주어진다는 의미이다. 포괄적 동의 프레임워크에서는 각각의 특정 목적에 대해서 고지에 의한 동의(informed consent)가 요구되지는 않지만, 프레임워크의 실제적인 변화가 있을 때 연구자가 연구 참여자에게 동의를 다시 구해야 하는 의무가 발생한다. 프라이버시 보호를 보장하기 위해, 그 프레임워크는 강력한 자율 규제 전략 뿐 아니라 각 연구 프로젝트에 대한 윤리적 검토가 포함돼야 한다. 과학 및 보건의료 연구에서 포괄적 동의를 원칙으로 하고 구체적인 동의를 예외로 하는 것은 바이오뱅킹과 같은 분야에서도 흥미로운 대안이 될 수 있다. 바이오뱅킹과 같은 분야는 생리학적 샘플과 데이터를 재사용하는 것이 핵심적인 분야이기 때문이다.[68] 미국 및 캐나다 프레임워크에서 동의 요건은 강화되어야 하지만, 연구 분야, 특히 보건의료 분야에서는 포괄적 동의가 데이터 수집에 기반한 바이오뱅킹 맥락과 잠재적 인공지능 AI 기술에

67) "Article 29 Working Party-Guidelines on Consent under Regulation 2016/679", (Apr. 10, 2018), https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030.

68) Chassang, *supra* note 66 at 3.

잘 부합할 것으로 보인다.

GDPR은 정보주체에게 본인의 데이터 처리에 대한 통제력을 강화할 목적을 가진 또 다른 권리를 제공한다. 이 권리는 '프로파일링을 포함한 자동화된 처리만을 유일한 근거로 하여 결정하지 않을 것'을 보장하는 것이다.(GDPR 제22조). 보건의료 인공지능 기술은 이 새로운 권리에 직접적으로 관련될 수 있다. 예컨대, 이 권리는 치료 제안을 제공하기 위해 만들어진 딥러닝 시스템이, 어떤 약이 환자에게 처방될 것인지를 결정하는 유일한 근거로 사용될 수 없음을 뜻한다. 이 규칙에 대한 예외는 회원국의 법률에 의해 제공되거나, 계약 체결에 필요한 경우, 또는 그 처리가 개인의 사전 동의에 기반한 경우에 적용된다. 이러한 경우 정보주체는 자동화된 결정에 대한 정당성을 제공받을 권리가 있다. 그러나 인공지능이 극히 복잡해지고 방대한 양의 데이터를 처리하는 바람에 단일한 정당성이 주어질 수 없을 때 문제가 발생한다. 그래서 딥러닝 시스템의 "블랙박스(black-box)" 현상은 보건의료에 인공지능을 접목하는 데 장애물이 될 수 있다.

### 나. 정보 이동권과 잊혀질 권리

GDPR 하에서 개인정보는 체계적이고, 일반적으로 사용되며, 기계가 판독할 수 있는 형식으로 획득되어야 한다. (제20조). 연구 수행 중일 때에는 이 세 가지 형식 내에서, 정보주체도 기관이 수집한 개인 정보에 접근하고 수정할 권리를 가진다. GDPR은 정보 이동권이라는 흥미롭고 새로운 권리를 포함한다. 이 권리는 개인이 자신의 데이터를 보다 잘 통제하고 경쟁력을 갖출 수 있도록 하는 것을 목표로 한다.[69] 보건의료 분야에서 정보 이동권은 데이터에 접근

69) 정보주체가 데이터를 한 기업에서 다른 회사로 쉽게 이전할 수 있도록 허용함으

하는 데에는 실질적인 이점을 가지고 있는 것으로 보인다. 예컨대, 피트니스 추적기 사용자는 앱에서 수집된 수년간의 데이터를 저장하여 의사나 본인이 지지하는 연구 분야에게 공유할 수 있다.[70] 그러나 제20조는 정보주체가 제공하지 않은 개인 정보는 이러한 공유 범위에서 제외시킨다. 건강 관련 웨어러블 디바이스가 수집한 데이터로부터 만들어진 분석의 결과물인 데이터는, 잠재적인 유익이 있는 심화 연구의 가능성이 있음에도 불구하고 이 권리에 포함되지 않게 된다.[71]

HIPAA 하에서 개개인은 자신의 정보를 의료 서비스 제공업체에서 다른 의료 서비스 제공업체로 이전할 수 있는 동등한 권리가 있다. 그러나 개인건강정보(personal health information; PHI, 이하 'PHI'라 칭한다)는 건강 보험, 보건의료 정보 센터와 보건의료 제공자 등의 '대상 단체'가 보유한 경우에만 보호되므로, 미국에서 건강 데이터 보호 면에서 정보 이동권은 약화된다. 이미 앞에서 언급되었듯, 이 범주는 커 보이지만 상당한 영역을 배제하고 있다. 공공의료 기관, 법 집행 기관, 개인 건강 기록 공급 업체는 제외된다. 즉, 비 대상 단체가 보유한 PHI는 HIPAA의 보호를 받지 않는다. 비대상 단체로 이전된 건강 기록은 잘해야 다른 개인정보보호 규정의 적용 범위에 속할 수 있지만, 미국 데이터 보호 규정에서는 완전히

---

로써(예컨대 건강 관련 애플리케이션에 보유된 데이터) 정보 이동권은 경쟁에 친화적이고 기업이 데이터를 보존하기 위해 고객의 프라이버시를 더 잘 보호하도록 장려하는 것으로 생각된다.

70) A. St John, *Europe's GDPR Brings Data Portability to U.S. Consumers,* Consumer Reports (2018), https://www.consumerreports.org/privacy/gdpr-brings-data-portability-to-us-consumers/ (accessed Jan. 9, 2019).

71) P. Quinn, *Is the GDPR and Its Right to Data Portability a Major Enabler of Citizen Science?* 18 Global Jurist (2018), https://www.degruyter.com/view/j/gj.ahead-of-print/gj-2018-0021/gj-2018-0021.xml (accessed Jun. 19, 2019).

제외될 수도 있다.[72] 정보 이동권은 데이터 전송을 용이하게 하여 연구에 도움을 줄 수 있지만, 미국의 경우 HIPAA의 이미 제한한 적용 범위마저 추가적으로 축소될 수 있다는 것이다.

캐나다에서 PIPEDA는 정보 이동권과 관련된 의무가 없다. 연구 분야에서 정보 이동의 잠재적인 유익을 감안해서 (예컨대, 정보주체가 참여하기를 바라는 연구 프로제트로 어떤 수집된 정보의 이동을 원활하게 하기 위하여), 정보 접근성 및 프라이버시 윤리 위원회 (The Committee on Access to Information, Privacy and Ethics)는 PIPEDA가 '정보 이동권에 대한 권리를 제공하기 위해' 개정되는 것이 바람직하다고 권고했다.[73] 정보 이동권은 개인들이 가장 유용한 곳으로 데이터를 재 연결함으로써 본인의 데이터 사용을 더 잘 통제할 수 있도록 하기 때문에 AI 시대에 개인정보 보호 규제의 중요한 부분으로 보아야한다. 그러나 민감 정보 진송이 데이터 규제 완화로 이어지지 않도록, 적절하고 포괄적인 건강 데이터 보호 프레임워크로 구성된 경우에서만 그렇게 할 수 있다.

GDPR에 따라 정보주체에게 부여된 새로운 권리는 데이터를 삭제할 권리이다(GDPR 제17조). 삭제권 또는 잊혀질 권리는 개인 또는 공공 기관이 보유한 개인 데이터를 완전히 삭제하도록 요구하는 것이다. 이것은 HIPAA와 PIPEDA에는 존재하지 않는 GDPR만의 특징이다. 이 권리는 정보주체가 공개한 개인정보에 대한 삭제 요청에 따라 완전히 지워질 수 있도록 보장하기 위한 것이다. 또한 제17조는 열거된 법적 근거 중 하나에 근거할 때만 적용되기 때문

72) *The National Committee on Vital and Health Statistics, Health Information Privacy Beyond HIPAA: A 2018 Environmental Scan of Major Trends and Challenges* 68 2 (2017).

73) *Towards Privacy By Design: Review Of The Personal Information Protection And Electronic Documents Act, supra* note 62.

에, 삭제권의 적용에도 일부 암묵적 제한을 두고 있다.[74] 이러한 근거들에는 수집된 개인 데이터가 더 이상 최초의 수집된 목적과 관련되어서는 필요가 없어졌을 경우를 포함한다. 이 데이터가 여전히 처리될 필요가 있고 다른 어떤 법적 근거도 적용되지 않는 경우, 삭제 요청이 거부될 수도 있다는 뜻이다. 다른 예외로는 공중 보건 분야에 대한 공익상의 이유로 처리가 필요한 경우(GDPR 17조 3항 (c)) 또는 공식 권한 행사와 관련이 있는 경우(GDPR 17조 3항 (b))를 포함한다. 삭제 권한이 적용되는 경우, 특히 공동 작업자와 공유되는 경우에 개인정보를 완전하고 체계적으로 삭제하기 위한 기술적 어려움으로 인해서 삭제 실행이 어려워질 수도 있다.[75]

인공지능 분야의 경우 딥러닝의 특징은, 결과물을 얻는 데 사용된 알고리즘이 이전에 수집된 데이터를 기반으로 자동 생성된다는 데에 있다. 따라서 이 데이터는 알고리즘의 일부가 되므로 특정 데이터를 삭제하기 위해 식별하거나 추출하는 것이 불가능해진다. 그

---

74) 역자 주: GDPR 17조 삭제권(잊혀질 권리) 제1항 정보주체는 본인에 관한 개인정보를 부당한 지체없이 삭제하도록 개인정보처리자에게 요청할 권리를 가지며, 개인정보처리자는 다음 각 호가 적용되는 경우 부당한 지체 없이 개인정보를 삭제할 의무를 가진다.
(a) 개인정보가 수집되거나 또는 처리된 목적과 관련하여 더 이상 필요하지 않은 경우
(b) 정보주체가 제6조 (1)의 (a)호 또는 제9조(2)의 (a)호에 따라 처리의 기반이 되는 동의를 철회하고, 해당 처리에 대한 기타의 법적 근거가 없는 경우
(c) 정보주체가 제21조(1)에 따라 처리에 반대하고 관련 처리에 대해 우선하는 정당한 근거가 없거나, 정보주체가 제21조(2)에 따라 처리에 반대하는 경우
(d) 개인정보가 불법적으로 처리된 경우
(e) 개인정보처리자에 적용되는 EU 또는 회원국 법률의 법적 의무를 준수하기 위해 개인정보가 삭제되어야 하는 경우
(f) 제8조(1)에 규정된 정보사회서비스의 제공과 관련하여 개인정보가 수집된 경우

75) Steven C. Bennett, *The Right to Be Forgotten: Reconciling EU and US Perspectives*, 30 Berkeley J. Int'l L. 161, 195, 161 (2012).

조항 위반과 관련된 GDPR의 높은 제재는 삭제가 불가능한 경우에 적용될 수 있다. 이는 프라이버시 보호를 위한 데이터 행위자의 책무성을 높이고, 규정 미준수 상황을 피하기 위해 자율 규제 개발을 촉진시키려는 EU 입법자들의 일반적인 의도 중 하나이다.

보건의료 분야에서, 삭제권은 환자가 보건의료 서비스 제공자에게 의료 기록을 삭제할 것을 강요할 수도 있다는 점을 의미한다. 결과적으로 환자의 의료 기록 정보를 온전하고 충실하게 –정보의 무결성- 보존하기 어렵게 되고, 이는 보건의료에 부정적인 영향을 미칠 것이다. 의료종사자들은 이미 환자의 전자 의무 기록에 접근할 때 '정보 차단(information blocking)' 문제와 관련된 우려를 표명하고 있다. 그러한 정보 차단은 종종 두 기록 시스템 간의 비 호환성과 같은 기술적 요인뿐만 아니라 엄격한 프라이버시 보호 관련 규정에서 비롯된다. 그러나 치료 시점에 완전한 임상정보에 접근하는 것은 여전히 중요하다.[76] 캐나다와 미국 입법자들은 관할권에서 삭제할 권리를 이행하기로 결정한 경우, 이를 염두에 두기를 원할 수 있다. 입법자들은 적어도 유용한 기술을 실행하려는 보건의료 조직에게 너무 큰 부담이 되지 않도록 그러한 권리를, 예컨대 적용 범위를 제한하는 것과 같은 방식으로 보장해야 한다.

## 2. 의무 강화: 데이터 행위자의 책임 증대

### 가. 개인정보 보호 영향 평가, 설계에 의한 프라이버시 보호(priacy by design) 및 기본설정에 의한 프라이버시 보호(privacy by default)

GDPR은 캐나다와 미국에 비해 투명성, 공정성 및 책무성을 더

76) D. F. Sittig et al., *New Unintended Adverse Consequences of Electronic Health Records,* Yearb Med Inform 7, 12 (2016).

강조점을 두고 있다(GDPR 제5조). 프라이버시와 개인정보 보호를 위한 예방적 접근 방식을 고수하기 위해, GDPR은 개인 데이터를 처리하기 이전에 기술적 수단을 채택할 것을 권장한다(GDPR 제25조 및 제78조). 또한 GDPR은 데이터 처리가 '인간의 권리와 자유에 고도의 위험을 초래할 가능성이 있는' 상황일 때마다, 개인정보 보호 영향 평가(DPIA: data protection impact assessment, 이하 'DPIA'라 칭한다)를 시행할 것을 요구한다. 데이터 처리의 예가 제공되고 있는데(GDPR 제35조 3항), 이 조항의 문구는 이 예가 전부는 아니라는 사실을 암시한다. 따라서 제29조 실무그룹은 DPIA가 요구되는지를 결정하는데 도움이 되는 가이드라인을 발행했다.[77] 다른 기준들 중에서도, 민감 정보, 취약한 대상자(예컨대 환자)에 관련된 데이터나, 새로운 기술 또는 현존하는 것에 대한 혁신적인 사용에 기반을 둔 경우, 처리는 '고도의 위험을 초래할 가능성이 있는' 것으로 간주되어야 한다. 보건의료에 인공지능을 적용하는 것은 일반적으로 보건의료 데이터를 기반으로 하며 종종 혁신적인 첨단 기술의 특성 때문에, 그 분야에서 어떤 처리가 이루어지기전에 DPIA가 필요할 가능성이 매우 높다.[78] 최소한, DPIA는 다음의 사항을 다루어야 한다. 1)처리 작업과 처리 목적에 대한 설명; 2)처리의 필요성과 비례성의 평가, 그리고 정보주체에 대한(정보주체의 관점에서 본) 위험도 평가; 3)이러한 위험을 완화하고 GDPR 준수를 보장하기 위한 조치들의 목록.

---

77) Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (2017).

78) S. Gardner, *High-Risk Processing Triggers EU Data Reg Obligations,* Bloomberg (2016), https://%3A%2F%2Fwww.bna.com%2Fhighrisk-processing-triggers-n57982070517 %2F (accessed Feb. 8, 2019).

DPIA 수행 요건에 대한 예외는 특별히 다음과 같이 명시하고 있는 전문 91에서 찾을 수 있다.

> "해당 데이터 처리가 개개의 의사, 다른 의료 전문가 또는 변호사의 환자 또는 의뢰인으로부터 나온 개인 데이터에 관련된 경우, 대규모의 진행이 고려되어서는 안 된다. 그러한 경우, 개인정보 보호 영향 평가는 의무사항이 아니다."

PIPEDA에는 존재하지 않지만, DPIA 메커니즘은 공공 연방정부 기관만을 위한 캐나다 법률 하에서는 필수적으로 요구된다. 또한 미국 법 하에서 HIPAA는 기업이 HIPAA의 요구사항에 부합하는 법인이라는 점을 보장하기 위해 매년마다 위험 평가를 수행할 것을 권고한다. 그러나 이 평가는 처리 전에 수행되는, 지속적이고 예방적인 프로세스로 인정이 되는 GDPR의 DPIA와는 다르다. DPIA는 그런 의미에서 EU의 규정에 매우 독특한 점이다. 또한 GDPR 하에서, 데이터 행위자는 '규정의 요구 사항을 충족시키고 정보주체의 권리를 보호하기 위해, 데이터 최소화 등 필요한 안전 조치를 개인정보 처리 내로 통합할 수 있도록 설계되어야 한다'(제25조, GDPR). '설계에 의한 프라이버시 보호'(privacy by design)로 알려진 이 원칙은 1990년대 캐나다 온타리오 주의 프라이버시 커미셔너인 앤 카부키안(Ann Cavoukian)에 의해 개발되었다.[79] 흥미롭게도 캐나다 PIPEDA에는 공식적으로 통합되지 않았다. 이에 따라 2018년 하원의 개인정보위원회는 "PIPEDA가 설계에 의한 프라이버시 보호를 중심적인 원칙이 되도록 하고, 이 개념의 7가지 기본 원칙을 포함

79) A. Cavoukian et al., *Remote Home Health Care Technologies: How to Ensure Privacy? Build It In: Privacy by Design,* 3 IDIS 363, 378 (2010).

하도록 개정되어야 한다"고 선언했다.[80] 또한 GDPR은 새로운 '기본설정에 의한 프라이버시 보호'(privacy by default) 원칙(GDPR 제25조)을 시행했다. 이 원칙은 기술을 개발할 때 데이터 최소화를 위한 기술적 수단을 구현하는 것이다. 그래서 데이터 처리자는 사전에 정의된 최종 결과물의 완성에 실제로 필요한 데이터에만 접근하고 처리할 수 있도록 기술적 보증을 설정해야 할 의무가 있다. GDPR은 기본설정에 의한 프라이버시 보호와 같은 예방 메커니즘을 시행하도록 부과함으로써, 잠재적인 위반을 방지하기 위해 적절한 기술적 조치를 신속하게 채택할 것을 권장한다. 기술 개발자에 대한 이러한 새로운 의무는 자율 규제를 촉진하는 데 기여하며, 중대한 제재 사항과 함께 조화를 이루게 된다.[81] 프라이버시 법에 '설계에 의한 프라이버시 보호'와 '기본설정에 의한 프라이버시 보호'와 같은 새로운 요구 사항을 포함시키면, 미국과 캐나다에서 데이터 유출 사고를 줄이는 데에도 실질적으로 도움이 된다.

### 나. 처벌 강화 및 보안 위반 알림에 관한 요구사항

PIPEDA, HIPAA, 및 GDPR 사이에서 발생하는 가장 큰 차이는 처벌 및 보안 위반 통지에 대한 입장이라고 말할 수 있다.

보안 위반 통지와 관련하여, HIPAA의 개인정보보호 규정은 대상 기관이 60일 이내에 보호되는 건강정보 보안 위반 사항을 개인에게 고지할 것을 요구한다(45 CFR §§ 164.400-414, HIPAA 위반 통지 규칙). 캐나다에서는 앨버타, 온타리오, 뉴브런즈윅, 튜펀들랜드 및 래브라도 지방의 건강 프라이버시 법률들에 따라 데이터 위반

80) Recommendation 14 in Towards Privacy By Design: Review Of The Personal Information Protection And Electronic Documents Act, supra note 62 at 52.

81) P. Voigt and A. Von dem Bussche, The EU General Data Protection Regulation (GDPR) 38 (Springer ed. 2017).

고지 시스템이 시행되고 있다.[82] 2018년 11월에 시행된 PIPEDA의 개정안은 프라이버시 커미셔너에게 새로운 데이터 위반 통지 의무를 포함하고 있다. 그러나 일부에서는 법률 개정안에서의 부정확한 용어를 비판하면서 '심각한 피해'의 '실제적 위험'이 있는 경우에만 통지를 줄 것을 요청한다.[83]

미국은 프라이버시 침해에 대해 최초로 강도 높은 처벌을 내린 첫 번째 국가였다. 미국의 모델과 유사하게, GDPR은 프라이버시 위반과 데이터 유출의 경우 무거운 제재 조치를 설정했다. 그러나 미국의 법체계에서는 중앙 데이터 보호기관이 없다. 또한, 제재 및 위반 통지 메커니즘이 존재하는 경우, 국가와 부문 간의 개인정보 보호 및 데이터 보호의 불일치로 인해 새로운 유럽의 기준과 비교하기가 어렵다.[84] GDPR에 따르면, 두 가지 수준의 처벌이 있다. 하위 수준에서는, 데이터 사용자(data user)에게 최대 1,000만 유로 – 약 1,130만 달러 또는 전년도 회계 연도의 전 세계 연간 수익의 2% (GDPR 제83조)까지도 벌금이 부과될 수 있다. 상위 수준에서는, 기업에게 최대 2,000만 유로 – 약 2,260만 달러 또는 전 회계 연도의 전 세계 연간 수익의 4%에 해당하는 벌금이 부과될 수 있다.(GDPR 제83조) 이러한 제재 시스템은 개인정보를 다루는 행위자의 책무성을 증진하고, 개인정보 침해를 방지하기 위해 자율 규제를 장려하는 것을 목표로 한다. 이러한 강도 높은 제재는 상당한 행정적 단순

82) Personal Information Protection Act, 34.1 (AB); Access To Information And Protection Of Privacy Act, 64.4 (NL); Personal Health Information Protection Act, 16.2 (ON); Personal Health Information Privacy and Access Act Subsection, 49.2 (NB).

83) Gardner and 2016, *supra* note 80.

84) Stacey A. Tovino, *The HIPAA Privacy Rule and the EU GDPR: Illustrative Comparisons,* 47 Seton Hall L., Rev. 973, 994 (2016)

화를 수반한다. 이전의 지침에 따르면, 수집 또는 처리 전에 국가의 개인정보보호를 담당하는 당국에 대한 엄격한 신고 절차가 필수 사항이었다. 데이터 처리자에 대한 관리 작업을 완화하기 위해 GDPR에는 더 이상 신고 요구 사항이 포함되어 있지 않지만 이제는 기관들에게 활동 기록(제GDPR 제30조)을 기록하도록 요청한다. 이러한 단순화는 프라이버시 보호 당국에 한층 높은 조사 및 제재 권한을 부여함으로써 가능해진다.

캐나다의 경우, PIPEDA는 벌금에 있어서 훨씬 보수적이다.[85] 「디지털 프라이버시법」(Digital Privacy Act)이 시행된 이래, 데이터 침해 사실을 통지하지 못한 경우 최대 75,300 달러(미화)의 벌금이 부과된다.(PIPEDA 제28조) 그러나 프라이버시 커미셔너의 시행 권한은 제한적이다. 현재의 제도에 따르면, 프라이버시 커미셔너는 위의 법 상 의무 위반 시에 의무이행을 명령하거나 제재를 내릴 권한이 없다. 지방 차원에서, 일부 프라이버시 커미셔너(예: 앨버타와 퀘벡주)는 이러한 권한을 가지고 있다.[86] 이러한 부조화는 캐나다 국경 내에서 실행이 다소 고르지 못하게 되는 결과를 초래하게 된다. 페이스북의 데이터 유출 이후, 프라이버시 커미셔너에게 보다 확장된 조사 권한과 제재 권한을 제공할 가능성이 추가적으로 검토될 수 있다.[87] PIPEDA에 따른 제재가 거대 기업의 규정 준수를 보장하기에 불충분한 경우, 미국 법체계는 국경 내에서 만족스러울

85) Office of the Privacy Commissioner of Canada, *PIPEDA Legislation and Related Regulations* (2015), https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/ (accessed Jan. 17, 2019).

86) P. Kosseim, *Law in Canada-DLA Piper Global Data Protection Laws of the World* 15 54 (2018).

87) Therrien, *supra* note 61.

정도의 조화된 프래임워크를 제공하지 못하므로 때때로 강한 제재를 적용하기 어려울 수 있다.

## Ⅶ. 결론과 향후 과제

보건의료 분야에 인공지능 기술이 통합됨으로써 얼마나 많은 기회가 창출될지를 과소평가되어서는 안 된다. 인공지능의 발전은 인간이 하는 것보다 기계에 더 적합하고 더 잘 수행할 수 있는 일, 즉 패턴을 감지하고 상관관계를 파악하며 복잡한 계산을 수행하는 일을 하도록 방대한 양의 데이터를 통해서 변환하는데 도움을 준다. 보건의료 서비스 제공업체가 시간과 비용을 절약하고 보건의료 연구와 환자 돌봄의 수준을 향상시키는데 있어서 많은 응용프로그램이 이미 사용 중이다. 그러나 사람들이 개인정보에 접근하도록 제공하는 것을 꺼리게 된다면 보건의료 시스템에서 인공지능을 구현하는 데 부정적인 영향을 줄 수 있다. 캐임브리지 애널리티카(Cambridge Analytica) 사례에 의해 밝혀진 개인 데이터의 오용에 대한 유명한 사례를 고려해 볼 때, 대중들의 신뢰가 전반적인 상실된 점은 이해가 될 만하다.[88] 특히 옵트 아웃 시나리오 금지 및 일부 동의 요구 사항을 통해 원치 않는 개인 데이터 사용을 방지하는

88) 역자주: 2018년 초에 케임브리지 애널리티카 (Cambridge Analytica) 회사가 수백만 명의 페이스북 가입자의 프로필을 본인의 동의 없이 수거해서 정치적 선전을 하려는 목적으로 사용했다는 사실이 세상에 밝혀지면서 사회적 파장이 일어났던 사건이다.
D. Simberkoff, *How Facebook's Cambridge Analytica Scandal Impacted the Intersection of Privacy and Regulation,* CMS Wire (2018), https://www.cmswire.com/information-management/how-facebooks-cambridge-analytica-scandal-impacted-the-intersection-of-privacy-and-regulation/ (accessed Jan. 17, 2019).

것을 목표로 하는 GDPR의 새로운 메커니즘은, 북미 정책 입안자들의 이목을 끌고 있다. 인공지능의 특수성과 프라이버시 보호로 인해 발생할 수 있는 새로운 위험은 GDPR에서 적어도 부분적으로라도 다루어진다 : 일부 메커니즘은 제한적으로 보이기도 하고 (삭제권과 같이) 개발자에게 문제가 될 수 있는 소지도 있지만, 데이터 행위자의 책무성을 향상시키려는 전반적인 노력은 인정되어야 하고, 더 보호적인 규정들이 채택되도록 권장해야 한다.

「데이터 프라이버시법」을 GDPR에 부합하도록 하는 정치적 및 경제적 원동력이 법제 개혁을 요청하고 있다고 판단된다. 이는 캐나다와 미국 법제가 인공지능이 제기한 고유 프라이버시 문제와 더 연관성을 갖도록 만들기 위한 것이다. HIPAA는 실질적인 처벌뿐만 아니라 보호 메커니즘을 제공하지만, 해당 법인과 관련자들에 의해 수집한 식별 가능한 데이터만 대상으로 한다. 캐나다는 모든 산업과 상업적 목적으로 수집된 모든 개인 데이터에 적용될 수 있는 모두 아우르는 성격의 법률을 가지고 있다. 그러나 이해 당사자들은 인공지능과 인터넷의 현실에 대응하기에는, 이 법률이 시대에 뒤떨어져있다는데 동의하고 있다. GDPR 규정이 부과하는 부가적인 영토성[89]과 확장된 의무가 불만과 불확실성의 원인일 수 있으며, 한동안 데이터 공유에 부정적인 영향을 끼칠 수 있다. 이것이 인공지능이 제기한 과제를 보다 잘 해결하는 데 도움이 되는 EU의 규정에 포함된 새로운 특징들을 무색하게 해서는 안 된다. 모든 법적 개혁은 캐나다와 미국의 개인정보 보호법에 대한 이러한 요소를 반드시 고려해야 하지만, GDPR의 적용 범위는 아직 판례를 통해 정의되지 않았다는 사실도 명심해야 한다. GDPR의 잠재적 적용에 관한

89) 역자주: GDPR의 적용 범위가 유럽 영토 밖에까지 미친다는 의미이다.

불확실성은 앞으로 북미에서 이루어질 개혁과 함께 다루어질 수 있다. 실제로, 의료기기 규정을 개정하고 있는 캐나다 보건부는 이러한 기회를 의식한 것으로 보인다. 자동화된 데이터 프로파일링을 갖춘 의료기기는 문제가 있는 '블랙박스'에 반대하여, '화이트박스'가 함께 제공될 경우 승인될 것으로 예상된다. 화이트박스는 편향된 자동화된 프로파일링과 관련된 위험을 제한하면서, 장치에 의해 프로파일링이 생성되는 방식을 이해할 수 있도록 해야 한다.

마지막으로, 책임 있는 데이터 공유 및 국경 간 데이터 전송을 가능하게 하는 개인정보 보호를 위한 호환 가능한 국제 프레임워크를 개발하는 것이 모든 당사자들에게 유익할 것이라고 믿는다.[90] 우리가 인공지능으로부터 기대를 걸고 있는 혜택들이, 궁극적으로는 그러한 기술이 사용되고 훈련될 수 있는 데이터의 총합에 따라 직결될 것이라는 점을 잊지 않도록 해야 한다.

90) Stoddart, Chan, and Joly, *supra* note 60 at 152.

## 참 고 문 헌

문유정, 강지민, 데이터 3법 개정과 의료 빅데이터 활용 방안, GBSA Review No. 2020-10, 경기도경제과학진흥원, 2020.

이재훈, 데이터 3법 개정과 연구개발정보 활용을 위한 제언, KISTEP Issue Paper, 2020-02 통권 제281호, 2020.

조수영, 개인정보보호와 EU의 GDPR에서의 프라이버시 보호에 관한 연구, 법학논고 제61집, 2018.

Allan M. Turing, Computing Machinery and Intelligence, 49 Mind 433, 460 (1950); Nils J. Nilsson, The Quest For Artificial Intelligence, Cambridge Core 56 (2009).

Andreas Holzinger, Trends in Interactive Knowledge Discovery for Personalized Medicine: Cognitive Science meets Machine Learning, 15 The IEEE Intelligent Informatics Bulletin 6, 14 (2014).

A. Cavoukian et al., Remote Home Health Care Technologies: How to Ensure Privacy? Build It In: Privacy by Design, 3 IDIS 363, 378 (2010).

A. Levin and M. Jo Nicholson, Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground, 2 U. Ottawa L. & Tech. J. 357, 396, 357 (2005).

A. Sharafoddini, Joel A. Dubin and J. Lee, Patient Similarity in Prediction Models Based on Health Data: A Scoping Review, 5 JMIR Med. Inform. e7 (2017).

A. St John, Europe's GDPR Brings Data Portability to U.S. Consumers, Consumer Reports (2018).

Brian Scogland, Artificial Intelligence in Medicine: Hope or Hype? MDDI Online (2018).

C. Castaneda et al., Clinical Decision Support Systems for Improving Diagnostic Accuracy and Achieving Precision Medicine, 5 J. Clin. Bioinforma. 4 (2015).

C. Duhigg, How Companies Learn Your Secrets, The New York Times (Feb. 16, 2012).

Council of Canadian Academies, Accessing Health and Health-Related Data in Canada 15 (2015).

D. Faggella, The State of AI Applications in Healthcare-An Overview of Trends, Emerj (2018).

D. F. Sittig et al., New Unintended Adverse Consequences of Electronic Health Records, Yearb Med Inform 7, 12 (2016).

D. Muoio, Japan Is Running Out of People to Take Care of The Elderly, So It's Making Robots Instead Business Insider (2015).

D. Simberkoff, How Facebook's Cambridge Analytica Scandal Impacted the Intersection of Privacy and Regulation, CMS Wire (2018).

D. Thoren-Peden and C. Meyer, Data Protection 2018 International Comparative Legal Guides, in Data Protection 2018 | Laws and Regulations | USA | ICLG (2018).

European Commission, The GDPR: New Opportunities, New Obligations (2018).

Ellen W. Clayton et al., A Systematic Literature Review of Individuals' Perspectives on Privacy and Genetic Information in the United States, 13 Plos One 2 (2018).

F. Jiang et al., Artificial Intelligence in Healthcare: Past, Present and Future, 2 Stroke Vasc. Neurol. 230, 243 (2017).

G. Chassang, The Impact of the EU General Data Protection Regulation on Scientific Research, 11 Ecancermedicalscience 709 (2017).

Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 (2017).

H. Evans and S. Togawa Mercer, Privacy Shield on Shaky Ground: What's Up With EU-U.S. Data Privacy Regulations, Lawfare (2018).

International collaboration in AI is based on increasingly large amounts of data,

including trans-border data sets. If data exchanges are hindered, the continuation or development of transatlantic research projects in the field are thought to be impeded. See Mark Phillips, International Data-Sharing Norms: From the OECD to the General Data Protection Regulation (GDPR), 137 Hum. Genet. 575, 582 (2018).

J. Halpert, J. Kashatus and K. Lucente, Data Protection Laws of the World: The United States (2017).

J. Kulynych and Henry T. Greely, Clinical Genomics, Big Data, and Electronic Medical Records: Reconciling Patient Rights With Research When Privacy and Science Collide, 4 J. Law. Biosci. 94, 132, 122 (2017).

K. K. Ogilvie and A. Eggleton, Challenge Ahead: Integrating Robotics, Artificial Intelligence and 3D Printing Technologies into Canada's Healthcare Systems 5 (2017).

K. Benitez and B. Malin, Evaluating Re-identification Risks With Respect to the HIPAA Privacy Rule, 17 J. Am. Med. Inform. Assoc. 169, 177 (2010).

L. Pangrazio and N. Selwyn, 'Personal Data Literacies': A Critical Literacies Approach to Enhancing Understandings of Personal Digital Data, 21 New Med. & Soc. 419, 437 (2019).

L. Olsen, D. Aisner and J. Micheal McGinnis, The Learning Healthcare System: Workshop Summary 6 (2007).

Martin Coulter, What is GDPR? Everything You Need to Know About the New EU Laws, Evening Standard (2018).

Muin J. Khoury and S. Galea, Will Precision Medicine Improve Population Health?, 316 JAMA 1357, 1358 (2016); See also S. Dolley, Big Data's Role in Precision Public Health, 6 Front. Public Health, 2 (2018).

Nello Cristianini, Intelligence Reinvented, 232 New Scientist 37, 41 (2016).

Nick Triggle, Care.data: How Did It Go So Wrong? (Feb. 19, 2014).

Nicholson W. Price and Glenn I. Cohen, Privacy in the Age of Medical Big Data, 25 Nat. Med. 37, 43, 39 (2019).

O. Diggelmann and M. Nicole Cleis, How the Right to Privacy Became a Human Right, 14 Hum. Rights Law Rev. 441, 458, 442 (2014).

O. Solon and O. Laughland, Cambridge Analytica closing after Facebook data harvesting scandal The Guardian (2018).

Office of the Privacy Commissioner of Canada, Summary of privacy laws in Canada (2014).

Office of the Privacy Commissioner of Canada, PIPEDA Legislation and Related Regulations (2015).

Paulo J. Lisboa and Azzam F. G. Taktak, The Use of Artificial Neural Networks in Decision Support in Cancer: A Systematic Review, 19 Neural Netw. 408, 415 (2006).

Personal Information Protection and Electronic Documents Act (PIPEDA), SC 2000, c 5b.

P. Kosseim, Law in Canada-DLA Piper Global Data Protection Laws of the World 15 54 (2018).

P. Quinn, Is the GDPR and Its Right to Data Portability a Major Enabler of Citizen Science? 18 Global Jurist (2018).

P. Bender, The Canadian Charter of Rights and Freedoms and the United, 28 McGill.

P. Voigt and A. Von dem Bussche, The EU General Data Protection Regulation (GDPR) 38 (Springer ed. 2017). L. J. 56, 820 (1983).

Recommandation 16, Towards Privacy by Design: Review of The Personal Information Protection and Electronic Documents Act (2018).

Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). [2016] OJ L119/1.

Regulation (EU) 2018/1807 of the European Parliament and of the Council of

November 14, 2018 on a framework for the free flow of non-personal data in the EU. [2018] OJ L119/1.

Roger Parloff, The Deep-Learning Revolution, 174 Fortune 96, 106 (2016).

Ruth R. Faden et al., An Ethics Framework for a Learning Health Care System: A Departure from Traditional Research Ethics and Clinical Ethics, 43 Hastings Center Report S16, S27 (2013).

Riccardo Miotto et al., Deep Learning for Healthcare: Review, Opportunities and Challenges, 19 Brief Bioinform. 1236, 1246 (2018).

Roger A. Ford and W. Nicholson Price II, Privacy and Accountability in Black-Box Medicine, 23 Mich. Tech. L. Rev. 1 (2016); W. Nicholson Price II, Regulating Black-Box Medicine, 116 Michigan Law Review 421 (2017); T. Simonite, AI Experts Want to End "Black Box" Algorithms in Government | WIRED, Wired (2017).

S. Armstrong, What Happens to Data Gathered by Health and Wellness Apps? 353 BMJ 353 (2016).

Steven C. Bennett, The Right to Be Forgotten: Reconciling EU and US Perspectives, 30 Berkeley J. Int'l L. 161, 195, 161 (2012).

Stacey A. Tovino, The HIPAA Privacy Rule and the EU GDPR: Illustrative Comparisons, 47 Seton Hall L., Rev. 973, 994 (2016).

S. Gardner, High-Risk Processing Triggers EU Data Reg Obligations, Bloomberg (2016).

The Health Insurance Portability and Accountability Act of 1996 (HIPAA). P.L. No. 104-191, 110 Stat. 1938 (1996).

The National Committee on Vital and Health Statistics, Health Information Privacy Beyond HIPAA: A 2018 Environmental Scan of Major Trends and Challenges 68 2 (2017).

Tom L. Beauchamp and Y. Saghai, The Historical Foundations of the Research-Practice Distinction in Bioethics, 33 Theor. Med. Bioeth. 45, 56 (2012); See also G. Bertier, A. Cambon-Thomsen and Y. Joly, Is it

Research or Is It Clinical? Revisiting an Old Frontier Through the Lens of Next-Generation Sequencing Technologies, 61 Eur. J. Med. Genet. 634, 641 (2018).

V. J. Mar and H. P. Soyer, Artificial Intelligence for Melanoma Diagnosis: How Can We Deliver on the Promise? 29 Ann. Oncol. 1625, 1628 (2018).

W. Knight, The Dark Secret At The Heart of AI-MIT Technology Review (2017).

W. Glauser, Artificial Intelligence, Automation and the Future of Nursing, Canadian Nurse (2017).

Willem Sundblad, Data is the Foundation for Artificial Intelligence and Machine Learning Forbes (2018).

Z. Obermeyer and Ezekiel J. Emanuel, Predicting the Future-Big Data, Machine Learning, and Clinical Medicine, 375 N. Eng. J. Med. 1216, 1219 (2016).

<Abstract>

# Integrating artificial intelligence into health care through data access

## - can the GDPR act as a beacon for policymakers? -

Juhee Eom*·Jiwon Shim**·Hye kyung Kim***

In the field of health and medical care, artificial intelligence has made significant progress in areas such as precision medical care, diagnostic tools, psychological and mental treatment, decision-making support, and care services. Artificial intelligence in the health care sector relies on a significant portion of personal information, including health-related data and sensitive data extracted from research subjects. Considering the development of artificial intelligence integrated into health care, it is judged that regulation of data based on artificial intelligence has a significant impact on regulating health and medical artificial intelligence. The General Data Protection Regulations (hereafter referred to as the GDPR) enacted in the European Union(EU) made its first attempt to regulate artificial intelligence through data protection legislation. This is applies to data processors involved in the provision of goods or services to data subjects within the European Union, and when it relates to monitoring data subjects' behaviour within

* First Author: Ph.D Yonsei University Graduate School of Public Health, Research Professor. Email: juheelight@gmail.com
** Ph.D. Chung-ang University Human research institute, Research Professor
*** Corresponding Author: Dept. of Humanities, Director of HEF Institute, Inje University, Associate Professor
This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2019S1A5A2A03053179)

the European Union. In the U.S. and Canada, the rule of GDPR is putting pressure on the government to reform policies and legislation regarding data. The contribution and prospect of artificial intelligence to the health and medical field were reviewed at a glance, and the task of data and privacy protection due to the development of this field was explored. After this, key measures to improve policies in the United States and Canada was presented through implications of the GDPR.

**Key Words** : artificial intelligence, data protection, personal data, personal information, General Data Protection Regulation (GDPR), health care, privacy right, privacy