12. 디지털 헬스케어 시대의 개인정보 보호

[목 차]

1. 개요

▶ 디지털 헬스케어의 발전으로 의료정보 및 건강정보의 활용가치가 증대되면서 EU, 미국, 중국은 각기 다른 방식으로 의료정보를 보호하고 활용하기 위한 규제 체계를 구축하고 있음

▶ EU는 GDPR을 중심으로 eHealth Network Guidelines, MDR, NIS Directive, eIDAS Regulation, AI Act 등 다층적 규제 체계를 통해 건강정보를 '특별 범주'로 분류하여 강화된 보호를 제공하고, 정보 주체 정보 주체의 권리보호를 최우선시하는 보수적 접근방식을 취함

▶ 미국은 HIPAA, HITECH Act를 중심으로 한 연방법과 주법의 복합적 체계로 구성되어 있으며, 의료산업의 발전과 혁신을 저해하지 않는 범위 내에서 규제하는 실용적이고 산업 친화적인 접근방식을 보임

▶ 중국은 개인정보보호법, 데이터안전법, 네트워크안전법의 일반법 체계와 의료 빅데이터 관리방법 등 산업별 특별 규제가 결합된 형태로, 데이터 현지화 요구 등 국가 차원의 통제력을 강화하면서도 디지털 헬스케어 산업 육성과 개인정보 보호의 균형을 도모하는 국

가 주도의 하향식 규제체계를 운영

2. EU의 규제 동향

▶ EU의 디지털 헬스케어 관련 데이터 프라이버시 및 보안 규제는 GDPR, eHealth Network Guidelines, Medical Device Regulation(MDR), NIS Directive, eIDAS Regulation 등을 중심으로 하는 다층적 규제 체계를 구축하고 있음

• EU 차원의 주요 규제 프레임워크는 다음과 같이 구성됨

- **(GDPR)** ▲건강 정보의 특별 카테고리 분류 및 강화된 보호, ▲처리 목적의 명확한 특정, ▲데이터 최소화 원칙, ▲정보 주체의 권리 보장(열람권, 정정권 등), ▲안전한 처리를 위한 기술적·관리적 조치 의무화, ▲국외 이전 제한에 대하여 규정함

- **(eHealth Network Guidelines)** eHealth Network Guidelines(eHealth 네트워크를 통한 가이드라인)은 ▲국가 간 건강 정보 교환을 위한 보안 요구 사항, ▲환자 동의 관리 체계, ▲의료인 인증 체계, ▲데이터 표준화 요건에 대하여 규정함

- **(Medical Device Regulation(MDR))** Medical Device Regulation(MDR)(의료기기 규정)은 ▲의료기기 소프트웨어 보안 요구 사항, ▲사이버보안 위험 관리, ▲사후 모니터링 의무에 대하여 규정함

- **(NIS Directive)** NIS Directive(네트워크 및 정보 시스템 보안 지침)는 ▲의료서비스 제공자의 사이버보안 의무 규정, ▲보안사고 보고 체계 구축, ▲위험평가 및 관리 체계 수립, ▲사고 대응 및 복구 계획 수립에 대하여 규정함

- **(eIDAS Regulation)** eIDAS Regulation(전자식별 및 인증 서비스 규정)은 ▲디지털 헬스케어 서비스의 본인확인 체계, ▲전자서명 표준 및 요구 사항, ▲상호운용성 보장을 위한 기술표준에 대하여 규정함

• 회원국 차원의 국가별 보건 의료법을 규정하여 의료정보 처리 관련 특별 규정을 규율하거나, 국가별 특수성을 반영한 회원국별 GDPR 구체화 입법

▶ GDPR은 건강 정보처리의 기본 원칙을 규정하고 있음

• 건강 정보의 특별 카테고리 분류 및 강화된 보호

- 건강 정보를 포함한 특별 범주의 개인정보 처리는 원칙적으로 금지됨(제9조 제1항)

- 다만 ▲예방의학, 근로자의 근무적합성 평가, 의료진단, 건강·사회복지 서비스 제공 목

적 ▲공중보건 분야에서의 공익적 목적(중대한 건강 위협 예방, 의료기기 품질 안전 기준 등) ▲과학적 연구, 통계적 목적 등의 경우 예외적으로 처리 허용(제9조 제2항)

- 건강 정보를 처리하는 의료인 등은 직무상 비밀 유지 의무 부담(제9조 제3항)

• 처리 목적의 명확성

- 개인정보는 구체적이고 명시적이며 적법한 목적으로 수집되어야 하며, 그 목적에 부합하는 방식으로만 처리되어야 함(제5조 제1항 (b)호)
- ▲정보 주체의 명시적 동의 ▲법적 의무 준수 ▲정보 주체·제3자의 중대한 이익 보호 ▲공익적 업무 수행·공적 권한 등 행사와 같은 개인정보 처리의 법적 근거 필요(제6조 제1항)

• 데이터 최소화

- 목적 달성에 필요한 최소한의 정보만 처리(제5조 제1항 (c)호)
- 가명화 등 기술적 조치 적용 등 시스템 설계 단계부터 개인정보 보호 고려(제25조)
- ▲데이터 최소화 원칙 준수 ▲가능한 경우 가명 처리 실시 등 연구·통계 목적의 처리 시 적절한 안전조치 의무 준수(제89조 제1항)

• 정보 주체 정보 주체의 권리

- 자신의 건강 정보처리 여부 확인 및 사본 요청권(제15조)
- 부정확한 건강 정보의 정정 요청권(제16조)
- '잊힐 권리'-불필요해진 정보의 삭제 요청권(제17조)
- 정보의 정확성 등에 관하여 다툼이 있는 경우 처리 제한 요청권(제18조)
- 자신의 건강 정보를 다른 의료기관 등으로 이전을 요청할 권리(제20조)

• 안전조치 의무

- 암호화, 접근 통제 등 기술적·관리적 보호조치 의무(제32조)
- 건강 정보처리의 위험성 사전 평가 의무(제35조)
- 건강 정보 처리하는 기관의 DPO 지정 의무(제37조~39조)

• 국외이전 제한

- 적절한 보호수준 보장 없는 이전 금지 원칙(제44조)

- ▲EU 집행위가 해당 제3국이 적절한 수준의 개인정보보호를 보장한다고 적정성 결정(Adequacy Decision)한 경우(제45조) ▲표준계약조항 등 적정한 안전조치를 구비하고(제46조) ▲명시적 동의, 계약이행, 공익적 필요 등 예외사유 해당 시(제49조)에만 이전 허용

▶ GDPR은 건강정보를 제9조에서 '특별한 범주의 개인정보'로 분류하여 더 강화된 보호를 규정하고 있음

- 건강정보의 처리는 원칙적으로 금지되나, 명시적 동의나 공중보건 등 제한된 예외사유가 있는 경우에만 허용됨(제9조 제2항)
- 특히 의료 목적의 처리는 반드시 직무상 비밀유지의무가 있는 자에 의해서만 이루어져야 한다는 추가적인 안전장치를 두고 있음(제9조 제3항)

▶ eHealth Network Guidelines(eHealth 네트워크를 통한 가이드라인)는 EU 회원국 간 전자 건강 정보 교환에 있어 개인정보 보호를 위한 기본 원칙과 요구 사항을 규정하고 있음

- 위 가이드라인은 GDPR을 기반으로 하여 건강 정보의 처리, 저장, 교환 시 회원국들이 준수해야 할 의무 사항과 보안 조치를 상세히 다루고 있으며, 국가별 법적 프레임워크와의 조화를 통해 EU 전역에서 일관된 개인정보 보호 수준을 확보함

  - **(개인정보의 처리)** eHealth Network 가이드라인의 범위 내 개인정보는 GDPR 제9조의 특별 범주 개인정보에 해당하므로, 회원국은 개인정보의 처리와 저장이 적용가능한 개인정보 보호 요구 사항에 부합하도록 보장해야 함(제4조 제1항)

  - **(국가별 법적 프레임워크)** 국가 법적 프레임워크는 건강 정보 공유 조건을 추가로 정의할 수 있으며, 특정 보호조치를 규정할 수 있고, 회원국은 GDPR과 국가 규정 모두를 준수하는지 평가하고 보장하기위한 조치를 마련해야 함(제4조 제2항)

  - **(보안 조치)** 회원국과 시행자는 ▲개인정보의 기밀성, 무결성, 가용성, 부인방지[1]를 위한 보호 및 보안 조치(제14조 제1항) ▲설계 단계부터 개인정보 보호를 고려한 안전하고 신뢰할 수 있는 시스템 설계(제14조 제2항) ▲건강 정보의 무단 또는 불법 처리와 우발적 손실, 파괴, 손상 방지를 위한 예방 조치(제14조 제3항) ▲신뢰할 수 있는 조직이나 기관에만 건강 정보 전송 보장(제14조 제4항) ▲건강 정보 통신에 대

1) non-repudiation(부인 방지)란 메시지의 송수신이나 교환 또는 통신이나 처리가 실행된 후에 그 사실을 사후에 증명함으로써 사실 부인을 방지하는 공증과 같은 역할의 보안 기술임

한 보안 통신 및 종단 간(end-to-end) 보안 조치 적용(제14조 제5항)을 포함한 최고 수준의 보안 표준을 적용해야 함

▶ Medical Device Regulation(MDR)(의료기기 규정)은 의료기기에 대한 EU의 새로운 규제 프레임워크 제시

• '17. 5. 채택되어 '21 5. 26. 부터 전면 적용

- **(GDPR 기반의 개인정보 보호 체계)** 의료기기 관련 개인정보 처리는 GDPR의 원칙을 준수해야 하고(제110조), 열람권, 정정권, 삭제권 등 정보 주체의 권리를 보장해야 함(제33조 제7항)

- **(임상시험 관련 개인정보 보호)** 임상시험 참여자의 신체적 및 정신적 온전성, 프라이버시 권리, 개인정보 보호가 GDPR에 따라 보호되어야 하고(제62조 제4항 (h)호), 임상시험 참여자에게 임상시험의 성격, 목적, 영향, 위험 및 불편에 대해 고지해야 하며(제63조 제2항 (a)호), 임상시험 참여자에게 자신의 권리와 보호장치에 대한 정보를 제공해야 하고(제63조 제2항 (b)호), 임상시험 참여자는 불이익 없이 언제든지 동의를 철회할 수 있으며, 동의 철회 이전에 수집된 개인정보의 이용에는 영향을 미치지 않음(제62조 제5항)

- **(Eudamed 시스템 관련)** Eudamed(European Database on Medical Devices, EU 의료기기 규제 데이터베이스),는 MDR 제33조에 따라 설립된 EU 의료기기 데이터베이스로써 일반 대중과 의료전문가에게 시장의 의료기기에 대한 적절한 정보 제공 등을 목적으로 하는데 위 시스템과 관련하여 개인정보는 식별가능한 형태로 필요한 기간만큼만 보관되어야 하고(제33조 제6항), 접근권, 정정권, 삭제권 등 정보 주체의 권리를 보장하여야 하며(제33조 제7항), Eudamed 관련 개인정보 처리에서 위원회가 컨트롤러 역할 수행(제33조 제9항)

▶ NIS Directive(네트워크 및 정보 시스템 보안 지침)는 EU 전역에서 높은 수준의 사이버보안을 달성하기 위한 조치들을 규정

• 필수 및 중요 기관[2]들의 사이버보안 위험 관리 의무와 보고 의무를 규정하고 있으며, 회원

2) 필수기관(Essential entities)은 지침 제3조 제1항에 따라 ▲Annex I에 명시된 유형의 기관 중 중소기업 기준을 초과하는 기관 ▲자격을 갖춘 인증서비스 제공자와 최상위 도메인 등록기관 및 DNS 서비스 제공자(규모 무관) ▲공공 전자통신 네트워크/서비스 제공자 중 중소기업 규모의 기관 ▲중앙정부 공공행정기관 ▲회원국이 제2조 제2항 (b)~(e)에 따라 필수기관으로 지정한 기관 ▲중요 인프라 지침(CER Directive)에 따라 지정된 중요 기관 ▲이전 NIS 지침에 따라 필수 서비스 운영자로 지정된 기관(회원국 재량)을 의미하고, 중요기관(Important entities)이란 제3조 제2항에 따라 ▲위의 필수기관으로 분류되지 않는 Annex I 또는 II에 해당하는 기관 ▲회원국이 제2조 제2항 (b)~(e)에 따라 중요기관으로 지정한 기관을 의미하는데, 필수기관은 사전·사후 감독을 모두 받지만 중요기관은 사후 감독만 받고(제31조 제2항), 필수기관은 더 엄격한 보안 요구 사항과 보고 의무가 적용되며, 과징금 상한도 필수기관(최소 1천만 유로(약 150억 원) 또는 전세계 매출의 2%)이 중요기관(최소 7백만 유로(약 105억 원) 또는 전세계 매출의 1.4%)보다 높음(제34조 제4항, 제5항)

국 간 협력 체계도 마련하고 있음

- **(개인정보 처리의 법적 근거)** 필수·중요 기관은 네트워크 및 정보 시스템의 보안을 위해 필요한 범위 내에서 개인정보를 처리할 수 있고, 이러한 처리는 GDPR 제6조 제1항 (c)호에 따른 법적 의무 준수를 위한 것으로 인정됨(전문 제121조)
- **(CSIRT의 개인정보 처리)** CSIRT(Computer Security Incident Response Team, 컴퓨터 보안 사고 대응팀)는 GDPR에 따라 필수·중요 기관의 요청에 따른 네트워크·정보 시스템에 대해 사전 스캐닝을 수행할 수 있고(전문 제43조), 제3국과의 정보 공유 시 GDPR 제49조의 요건을 준수해야 함(전문 제45조)
- **(사고 보고와 개인정보 유출)** 사고로 인한 개인정보 유출 시 감독기관과 협력하여 필요한 정보를 제공해야 하고(제35조 제1항), GDPR에 따른 과징금이 부과된 경우 본 지침에 따른 추가 과징금은 부과하지 않으며(제35조 제2항), 다른 회원국의 감독기관이 관할하는 경우, 자국 감독기관에 통지해야 함(제35조 제3항)
- **(보안조치와 개인정보보호)** 암호화 등 보안기술 사용 시 프라이버시·보안 기본설정(Privacy·Security by Default) 원칙을 준수하여야 하고, 종단 간 암호화(End-to-End Encryption, E2EE)[3]는 필수적인 프라이버시·보안 보호 기술로 인정됨(전문 제98조)

▶ eIDAS Regulation(전자식별 및 인증 서비스 규정)은 EU 내 전자거래의 신뢰성 보장을 위한 전자식별 및 인증 서비스에 관한 법적 프레임워크를 제공

• 전자서명, 전자인감, 타임스탬프 등의 인증 서비스와 관련된 개인정보 보호 요구 사항을 규정

- **(전자식별 관련)** 전자식별 수단 발급 시 해당 자연인이나 법인을 고유하게 나타내는 개인식별정보를 기술사양·표준·절차에 따라 부여해야 하고(제7조 제d호), 당사자의 동의가 있는 경우에만 개인정보를 공개적으로 검색할 수 있도록 해야 함(제24조 제2항 제f호 (i)목)
- **(인증서비스 제공자의 의무)** 인증 서비스 제공자는 GDPR에 따라 개인정보를 적법하게 처리해야 하고(제24조 제2항 제j호), 보안사고나 개인정보 유출 시 24시간 내에 감독기관과 관련 기관(데이터보호당국 등)에 통지해야 함(제19조 제2항)
- **(감독 관련)** 감독기관은 개인정보보호 규정 위반이 의심되는 경우 데이터보호당국에

3) 통신의 양 끝점에 있는 사용자들만이 메시지를 읽을 수 있도록 하는 보안 통신 방식으로, NIS2 지침에서는 제98조에서 엔드투엔드 암호화와 관련하여, 공공 전자통신 네트워크와 서비스의 보안을 위해 암호화 기술, 특히 엔드투엔드 암호화의 사용을 권장해야 함을 규정함

감사 결과를 통보해야 하고(제17조 제4항 제f호), 감독기관은 보안사고 및 개인정보 침해 사고에 대한 요약 정보를 ENISA(European Union Agency for Network and Information Security, 유럽 네트워크 정보보안청)에 제공해야 함(제19조 제3항)

- **(전자서명·인감 인증서 관련)** 가명 사용 시 이를 명확히 표시해야 하고(제28조 제1항), 인증서에는 고유식별정보가 포함되어야 하며, 이를 통하여 자연인이나 법인을 명확히 식별할 수 있어야 함(부록 I, III)

▶ EU AI법(AI Act)는 '24년 8월 발효되고 '25년 2월부터 단계적으로 시행되는 AI 시스템의 개발·시장 출시·서비스 제공 및 사용에 관한 EU의 첫 번째 포괄적인 법적 프레임워크로서, 위험 기반 접근법을 채택하여 AI의 혁신을 촉진하면서도 개인을 보호하는 것을 목표로 함

- 의료분야 AI 시스템은 위험도에 따라 다음과 같이 분류되며, 각각 다른 규제가 적용됨[4)]
  - 고위험 AI 시스템에는 진단용 AI 도구, AI 의료기기(Class IIa 이상), 응급전화 평가 시스템 등이 포함되고, 이들은 엄격한 안전 및 품질 요구 사항을 준수해야 함
  - 특히 의료기기의 경우 MDR(Medical Device Regulation)에 따른 제3자 적합성 평가가 필요함
- AI 시스템 제공자(의료기관이 자체 개발한 AI 포함)의 주요 의무 사항은 다음과 같음
  - 위험관리 시스템 구축 및 데이터 거버넌스 확립
  - 기술문서 작성 및 보관, 인적 감독 조치 이행
  - 정확성, 견고성, 사이버보안 확보를 위한 품질관리 시스템 구축
- AI 시스템 사용자(의료전문가 및 공중보건당국)의 주요 의무 사항은 다음과 같음
  - AI 사용 인력에 대한 교육훈련 실시
  - 시스템 모니터링 및 중대사고 보고
  - 개인정보보호영향평가 및 기본권 영향평가 수행(단, 공공의료서비스 제공자에 한정)

4) Hannah van Kolfschooten, Janneke van Oirschot, "The EU Artificial Intelligence Act (2024): Implications for healthcare", Health policy 149 (2024)

▶ 규제 위반 시 GDPR과 MDR에 따른 제재가 적용됨

• GDPR에 따른 행정적 제재 및 민사상 손해배상 규정은 다음과 같음

- **(과징금)** 일반 위반의 경우 최대 1천만 유로(약 150억 원) 또는 전세계 연간 매출액의 2% 중 높은 금액(제83조 제4항), 중대 위반의 경우 최대 2천만 유로(약 300억 원) 또는 전세계 연간 매출액의 4% 중 높은 금액(제83조 제5항) 상당액의 과징금 부과 대상이 됨

- **(시정명령)** ▲위반 가능성에 대한 경고 발령(제58조 제2항 (a)호) ▲위반행위에 대한 견책(제58조 제2항 (b)호) ▲정보 주체 권리 행사 요청 이행 명령(제58조 제2항 (c)호) ▲처리 작업의 GDPR 준수 명령(제58조 제2항 (d)호) ▲개인정보 침해 사실의 정보 주체 통지 명령(제58조 제2항 (e)호) ▲처리에 대한 제한 명령(제58조 제2항 (f)호) ▲제3국으로의 정보 이전 중지 명령(제58조 제2항 (j)호)

- **(민사상 손해배상)** GDPR 위반으로 인한 물질적·비물질적 손해에 대한 보상 청구가 가능하고(제82조 제1항), 처리에 관여한 컨트롤러는 위반에 대한 전체 책임을 부담하고 프로세서는 GDPR 상 프로세서 의무 위반 또는 컨트롤러의 적법한 지시를 벗어난 경우에만 책임을 부담하며(제82조 제2항, 제4항), 동일 처리에 복수의 컨트롤러·프로세서가 관여한 경우 전체 손해에 대해 연대책임을 지고 전체 배상을 한 컨트롤러·프로세서는 다른 책임자에게 구상권 행사 가능(제82조 제4항, 제5항)

• MDR의 제재 관련 주요 조항은 아래와 같음

- **(행정적 제재의 기본 근거)** 회원국들은 이 규정 위반에 대한 처벌 규정을 수립하고, 이를 효과적이고 억제력 있게 적용해야 함을 규정(제113조)

- **(시장 감시 및 통제 조치)** 회원국의 권한 당국은 의료기기의 적합성 특성과 성능에 대한 적절한 점검을 수행하고, 필요한 경우 문서 검토와 함께 적절한 샘플을 바탕으로 한 물리적 검사 또는 실험실에서의 시험을 포함할 수 있고(제93조 제1항), 기기가 허용할 수 없는 수준의 위험을 나타내는 경우, 당국은 제조업체에 즉시 적절한 시정 조치를 취하도록 요구 가능(제95조 제1항)

- **(구체적인 제재 조치)** 제조업체가 적절한 시정 조치를 취하지 않을 경우 ▲해당 제품의 시장 출시 금지 ▲시장에서의 제품 회수 ▲제품의 철수 명령 가능(제98조 제4항)

- **(예방적 보건 조치)** 회원국은 공중보건 보호를 위해 특정 기기의 ▲시장 출시 금지 ▲시장 철수 ▲회수 등의 필요한 조치 가능(제98조 제1항)

- **(과징금)** 회원국들은 규정 위반에 대한 과징금을 포함한 처벌 규정을 자체적으로 수립하고 집행(제113조)
- **(시정조치 의무)** 제조업체는 시판 후 감시 시스템을 통해 필요한 예방적·시정 조치를 즉시 이행해야 하고(제83조), 중대한 사고나 현장 안전 시정 조치가 필요한 경우, 제조업체는 즉시 보고하고 조사를 실시해야 함(제89조)

3. 미국의 규제 동향

▶ 미국의 디지털 헬스케어 관련 개인정보 보호 및 보안 규제는 연방법과 주법의 복합적 체계로 구성되어 있으며, 각각의 법령이 상호보완적으로 운영되고 있음

• 연방 규제 사항은 다음과 같이 구성됨
- **(HIPAA)** 건강보험 정보의 이전 및 그 책임에 관한 법률(Health Insurance Portability and Accountability Act, 이하 HIPAA)은 ▲환자의 의료정보 접근권 보장 ▲의료정보 사용 및 공개에 대한 제한 ▲최소필요정보(Minimum Necessary) 원칙 적용 ▲보안위험 평가 및 관리 체계 구축 의무 ▲직원 교육 및 내부 정책 수립 의무를 주요 의무사항으로 하는 법률로써 ▲의료서비스 제공자(Healthcare Providers) ▲의료 보험사(Health Plans) ▲의료정보 중개기관(Healthcare Clearinghouses) ▲사업 관계자(Business Associates)를 적용 대상으로 함
- **(HITECH Act)** 경제 및 임상 건강을 위한 건강 정보 기술법(Health Information Technology for Economic and Clinical Health Act, 이하 HITECH Act)는 ▲전자건강기록(EHR) 시스템 보안 요건, ▲데이터 암호화 기준 ▲접근통제 요구 사항 ▲EHR에 관한 규정 ▲최대 벌금액 상향 조정 ▲고의성에 따른 차등 처벌 ▲시정조치 이행 의무화 ▲위반 사실 공개 의무 등 위반 시 처벌 강화 규정
- **(FDA 사이버보안 가이드라인)** 의료기기 수명 주기별 보안 요구 사항으로서 ▲설계 단계의 보안 고려 사항 ▲제조 과정의 품질관리 ▲시판 후 모니터링 체계 ▲취약점 관리 및 패치 정책 규정, 위험관리 프레임워크로써 ▲위험평가 방법론 ▲위험 완화 전략 ▲사고대응 체계 ▲복구계획 수립 등 규정
- **(FTC 소비자보호규정)** 개인정보 수집 및 이용과 관련하여, ▲투명성 확보 의무 ▲동의획득 절차 ▲목적 외 이용 제한 ▲제3자 제공 제한 규정, 소비자 권리보장과 관련하여 ▲정보접근권 ▲정정요구권 ▲삭제요구권 ▲이의제기권 규정

- **(PADFA)** 미국의 데이터를 외국 적대세력으로부터 보호하기 위한 법안(Protecting Americans' Data from Foreign Adversaries Act)은 미국 시민들의 민감정보를 보호하기 위한 법안으로써, ▲데이터 브로커의 외국 적대세력과의 거래 제한(데이터 브로커가 미국 개인의 민감한 개인정보를 외국 적대국가나 외국 적대세력이 통제하는 단체에 판매, 라이선스, 임대, 거래, 이전, 공개, 접근 제공 등 금지) ▲개인정보 보호(생체정보, 유전정보, 정확한 위치정보, 민감한 개인 통신 내용 등 다양한 민감정보 범주 정의) ▲적용 예외(정보기관 활동, 국제 의무 이행 및 법집행 활동) 등을 규정
- **(EO 14117)** 미국인의 민감한 개인정보 및 정부 관련 데이터 접근 제한에 관한 행정명령(Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern)은 외국의 위협으로부터 미국인의 개인정보와 정부 데이터를 보호하기 위한 포괄적 행정명령으로써 ▲위협 국가 정의 및 규제(우려 대상국의 정의와 해당 국가와의 데이터 거래 제한/금지) ▲민감정보 범위 설정(대규모 민감정보, 정부 관련 데이터, 생체정보, 위치정보, 건강정보, 금융정보 등 포함) ▲의료/연구 데이터 보호체계 구축(연방 지원 프로그램에 대한 보호조치 수립, 연구기관 지침 개발) ▲데이터 인프라 보안 강화(해저 케이블 허가 검토, 데이터 중개업체 규제), ▲기존 데이터 이전 위험 평가(국가안보 위험 평가 및 대응방안 수립) ▲생물학적 데이터 규제 검토(인체 유전체 데이터 외 추가 규제 필요성 평가) 등을 규정

• 주정부 규제사항은 다음과 같이 구체화됨

- **(주별 프라이버시법)** 이미 발효된 법률과 2024~2025년에 발효될 법률을 포함하여 적어도 15개 주가 소비자 프라이버시법을 보유하고 있고, 추가로 15개 주가 유사한 법안을 주 의회에 제출한 상태[5]로써, 주요 법령으로는 ▲일리노이 생체정보 프라이버시법(Illinois Biometric Information Privacy Act) ▲캘리포니아 소비자 프라이버시법(California Consumer Privacy Act, CCPA) ▲캘리포니아 유전정보 프라이버시법(California Genetic Information Privacy Act) ▲캘리포니아 프라이버시 권리법(California Privacy Rights Act) ▲버지니아 소비자 데이터 보호법(Virginia Consumer Data Protection Act)이 있음

5) Chambers and Partners, "Chambers Global Practice Guides" (2024), 286

▶ HIPAA는 개인의료정보 보호와 관련하여 제262조의 'Administrative Simplification'에서 규정하고 있으며, 세부적으로는 다음과 같이 구성됨

• 제262조(Administrative Simplification)는 사회보장법(Social Security Act)의 Title XI에 새로운 Part C를 추가하는 조항으로써, 추가된 Part C는 제1171조부터 제1179조까지의 하위 조항들로 구성됨

- **(보호대상 정보의 범위)** ▲의료제공자, 의료보험사, 의료정보 중개기관 등이 생성·수집하는 개인식별가능한 의료정보 ▲과거, 현재, 미래의 신체적·정신적 건강상태 정보, ▲의료서비스 제공 관련 정보 ▲의료비 지불 관련 정보가 포함됨(제1171조)

- **(정보보호 기준 수립 의무)** ▲정보의 전자교환을 위한 표준 수립 ▲데이터 요소에 대한 표준 수립 ▲정보보안을 위한 기술적·관리적·물리적 보호조치 기준 마련(제1172조, 제1173조)

- **(정보보안 요구 사항)** ▲정보 시스템의 기술적 능력 고려 ▲보안조치 비용 고려 ▲정보접근자에 대한 교육훈련 ▲감사추적 기록 유지 ▲중소규모 의료기관의 특수성 고려(제1173조 (d)항)

- **(정보 처리자의 의무)** ▲정보의 무결성과 기밀성 보장 ▲예상 가능한 위협으로부터 보호 ▲미승인 이용이나 공개 방지 ▲임직원들의 법규정 준수 보장(제1173조 (d)항 (2)목)

- **(개인정보 공개에 대한 처벌)** ▲고의적인 개인정보 유출·오용 시 최대 5만 달러(약 6,900만 원)의 벌금 또는 1년 이하의 징역 ▲상업적 이익 등을 위한 정보 유출 시 최대 25만 달러(약 3억 4천만 원)의 벌금 또는 10년 이하의 징역 ▲허위 명목으로 정보를 취득한 경우 최대 10만 달러(약 1억 4천만 원)의 벌금 또는 5년 이하의 징역(제1177조)

▶ HIPAA는 '보호대상 건강정보(Protected Health Information, PHI)'라는 개념을 통해 의료정보를 규제함

• **(PHI의 법적 정의)** PHI는 '개인을 식별할 수 있는 건강정보로써, 구두, 서면, 전자적 또는 기타 어떤 형태나 매체로 전송되거나 유지되는 정보'를 의미함(45 CFR § 160.103)

- 구체적으로 과거, 현재 또는 미래의 신체적·정신적 건강상태, 의료서비스 제공, 의료서비스 비용 지불과 관련된 정보를 포함함

• **(HIPAA 프라이버시 규칙)** 45 CFR Part 164, Subpart E의 제164.502조에서 PHI의 사용과 공개를 원칙적으로 제한하고, '24년 개정을 통해 생식건강 관련 PHI[6]의 사용/공개 제한 및 요청 시 서면증명 요구 사항 추가 등 보호를 강화함

- **(HIPAA 보안 규칙)** 45 CFR Part 164, Subpart C에서 PHI의 기밀성, 무결성, 가용성 보호를 위한 행정적, 기술적, 물리적 안전조치 의무를 규정함
- **(GDPR과의 차이점)** HIPAA는 EU의 GDPR과 달리 건강정보를 별도의 '민감정보' 범주로 분류하지는 않으나, 프라이버시 규칙과 보안 규칙을 통해 의료정보의 특수성을 반영한 독자적인 보호체계를 구축하고 있음
- **(제재 강화)** 2024년 HIPAA 위반에 대한 벌금 구조가 개정되어, 위반의 심각성과 고의성에 따라 4개 등급으로 구분하고 위반 건당 최소 141달러 (약 19만 원)에서 최대 2,134,831달러 (약 28억원)까지, 연간 총액 최대 2,134,831달러(약 28억 원)까지 부과할 수 있도록 함

▶ HITECH Act는 개인의료정보 보호와 관련하여 Title XIII의 Subtitle D(제13400-13424조)에서 규정하고 있음

- 제13400조는 정의 규정에 해당함
  - **(위반, breach)** 무단 획득·접근·사용·공개로 인해 보안이나 프라이버시가 침해된 경우를 의미하고, 다만 ▲수령인이 해당 정보를 실질적으로 보유할 수 없는 경우 ▲선의의 우발적 획득·접근인 경우 ▲동일 시설 내 권한 있는 자의 부주의한 공개의 경우 위반에 해당하지 않음
  - **(적용대상이 되는 기관, covered entity)** ▲의료서비스 제공자(Health care provider), ▲건강보험사(Health plan) ▲의료정보 중개기관(Health care clearinghouse) ▲이들과 계약관계에 있는 사업관계자(Business associates)[7] 포함
  - **(보호대상 건강 정보)** ▲보호대상 건강 정보(Protected health information) ▲개인건강기록 ▲의료서비스 제공자가 생성/수집/관리하는 정보 ▲건강보험과 관련된 정보
  - **(개인건강기록)** 여러 출처에서 수집되어 개인이 관리·공유·통제하는 전자건강 정보 기록

6) 개인의 생식 시스템과 그 기능 및 과정 관련 모든 건강 정보를 포함하고, 피임 및 응급 피임, 임신 전 검사 및 상담 등에 관한 정보가 포함됨
7) 45 CFR 160.103(정의 규정)에서 정의된 바와 같이 '적용대상 기관을 대신해 보호대상 건강 정보를 처리하는 자'를 의미함

- 제13401조는 보안 규정의 적용 관련 내용임
  - **(사업관계자 의무)** 45 CFR 164.308(관리적 보호조치), 164.310(물리적 보호조치), 164.312(기술적 보호조치), 164.316(정책·절차 및 문서화 요건)의 보안규정이 직접 적용되고, 적용대상 기관과의 계약에 보안 요구 사항 반영이 필요하며, 정기적인 보안평가 및 위험분석 실시 의무가 있음
  - **(처벌)** 사회보장법 제1176조와 1177조의 민사·형사 처벌 규정이 동일하게 적용되고, 위반 정도에 따라 건당 100~5만 달러(약 14만 원~6,926만 원)의 민사 제재금이 부과됨
  - **(연간 지침)** 보건복지부는 이해관계자 의견수렴 후 기술적 안전조치 지침을 발행하여야 하고, 이때 최신 보안위협 및 기술발전 사항을 반영하며 중소 규모 의료기관의 특수성을 고려해야 함
- 제13402조는 위반 통지 의무 규정으로, 적용대상 기관(covered entity)의 통지 의무는 아래와 같음
  - **(통지 대상)** 건강정보가 노출된 각 개인
  - **(발생 요건)** 보호대상 건강정보가 무단으로 접근, 획득 또는 공개되었다고 합리적으로 판단되는 경우
  - **(직접 통지)** 영향 받은 개인에게 직접 통지
  - **(매체 통지)** 500명 이상 영향 시 주요 매체 통지 필요
  - **(정부 통지)** 보건복지부 장관에게도 통지 필요
- 또한, 제13402조 중 사업관계자(business associate)의 통지 의무는 아래와 같음
  - **(통지 대상)** 위탁 관계에 있는 적용대상 기관
  - **(발생 요건)** 사업관계자가 접근·관리·보유·수정·기록·저장·파기하는 과정에서 보안되지 않은 보호대상 건강 정보의 위반 발견 시
  - **(통지 내용)** ▲영향 받은 각 개인의 신원 확인 정보 ▲위반과 관련된 모든 정보 ▲취한 조치나 향후 조치 계획 포함
  - **(후속 절차)** 적용 대상 기관이 최종적으로 개인에게 통지

• 제13405조는 정보 판매 제한, 접근권 보장, 최소 필요 원칙과 관련하여 개인정보 보호 강화에 대하여 규정하고 있음

- **(정보 판매 제한)** 원칙적으로 적용대상 기관이나 사업관계자는 보호대상 건강 정보를 직접 또는 간접적인 대가를 받고 교환할 수 없고, 정보 주체 정보 주체로부터 유효한 승인을 받은 경우에만 가능하며, 승인서에는 정보를 제공받는 기관이 해당 건강 정보를 대가를 받고 다시 교환/거래할 수 있는지 여부를 명시해야 하나, 예외적으로 ▲공중보건활동(45 CFR 164.512(b)) ▲연구목적(정보 준비/전송 비용만 반영) ▲치료 목적 ▲의료기관 인수합병 등 사업이전 ▲정보 주체 본인의 기록 사본 제공 ▲법령에 따른 필수적 공개 ▲사업관계자의 위탁업무 수행의 경우 예외적으로 허용됨(제13405조 (d)항)

- **(접근권 보장)** 적용대상 기관이 전자건강기록 보유 시 정보 주체의 전자적 형태 사본 요구권이 인정되고, 정보 주체가 지정한 제3자에게 직접 전송 요청은 가능하되 요청은 명확하고 구체적이어야 함(제13405조 (e)항)

- **(최소 필요 원칙)** 보호대상 건강 정보의 이용·제공·요청은 목적 달성을 위해 필요한 최소한의 범위로 제한되나 ▲치료 목적의 제공 ▲정보 주체에게 제공 ▲정보 주체의 승인을 받은 제공 ▲법령에 따른 필수적 제공은 원칙의 예외에 해당함(제13405조 (b)항)

• 제13410조는 처벌 강화에 대하여 규정하고 있음

- **(민사제재)** ▲과실(did not know)의 경우, 위반 당 100달러~5만 달러(약 14만 원~6천만 원), 연간 최대 2만 5천 달러(약 3천만 원) ▲상당한 과실(reasonable cause)의 경우 위반 당 1천~5만 달러(약 138만 원~6천만 원), 연간 최대 10만 달러(약 1억 4천만 원) ▲고의-시정(willful neglect-corrected)의 경우 위반 당 1만~5만 달러(약 1천만 원~6천만 원), 연간 최대 25만 달러(약 3억 4천만 원) ▲고의-미시정(willful neglect-not corrected)의 경우 위반 당 5만달러(약 6,923만 원), 연간 최대 150만 달러(약 20억 원)를 부과함(제13410조 (d)항)

- **(형사처벌)** ▲고의적 유출·획득의 경우, 5만 달러(약 6천만 원) 이하 벌금, 1년 이하 징역 ▲기망·사칭의 경우 10만 달러(약 1억 4천만 원) 이하 벌금, 5년 이하 징역 ▲영리목적의 경우 25만 달러(약 3억 4천만 원) 이하 벌금, 10년 이하 징역형 처벌(제13410조 (a)항)

- **(주 검찰총장 권한)** 주민의 이익을 대변하여 민사소송 제기, 금지명령 청구 가능, 민사제재금 상당의 손해배상 청구(제13410조 (e)항)

▶ PADFA 및 Executive Order 14117을 통해 민감정보의 범위를 구체적으로 정의하고 보호하는 체계를 구축

- PADFA 제2조 제c항 제7호는 '민감정보'를 ▲정부발급 식별자(사회보장번호, 여권번호, 운전면허증 번호) ▲건강정보 ▲금융정보(계좌번호, 신용카드번호 등) ▲생체인식 정보 ▲유전정보 ▲정확한 위치정보 ▲17세 미만 미성년자 정보 ▲인종, 피부색, 민족, 종교 정보 등으로 정의함

- Executive Order 14117 제7조 (l)항은 '민감한 개인정보(Sensitive Personal Data)'를 ▲개인식별자(Covered Personal Identifiers) ▲위치정보 및 관련 센서 데이터 ▲생체인식 정보 ▲인체 유전체 데이터(Human 'omic Data) ▲개인건강정보 ▲개인금융정보 ▲위 데이터들의 조합으로 정의함

- PADFA는 제2조 제a항에 따라 데이터 브로커의 외국 적대세력에 대한 민감 데이터 제공, 임대, 거래, 이전 등을 금지

- Executive Order 14117 제2조는 우려 국가의 민감정보 접근을 제한하는 금지거래(Prohibited Transactions)[8]와 제한거래(Restricted Transactions)[9] 체계를 구축하고, 제3조 제b항에서 의료데이터에 대한 특별 보호조치를 규정하며, 비식별화된 건강정보의 재식별 방지 등을 요구

  - 데이터가 익명화, 가명화 또는 비식별화되었더라도, 우려 국가(Countries of concern)[10]가 대규모 데이터셋에 접근할 경우 기술의 발전과 결합하여 데이터를 재식별하거나 익명성을 해제할 수 있는 위험성을 인식

  - 국제 협력과 협업을 통한 연구개발을 촉진하기 위해 과학 데이터와 샘플의 공개 공유는 지원하되, 미국인의 민감한 개인 건강정보와 인체 유전체 데이터에 대해서는 추가적인 보호조치를 의무화

  - 이를 위해 연방지원 연구기관의 데이터 보호조치 의무화 및 비식별화된 건강정보의 재식별 방지를 위한 구체적인 기술적·관리적 보호조치를 요구

▶ 미국의 디지털 헬스케어는 연방정부와 주정부의 이원화된 규제 체계를 가지고 있으며,

8) 제2조 제a항에 따라 국가안보에 용납할 수 없는 위험을 초래하는 거래 유형
9) 제2조 제c항 제ii호에 따라 국토안보부 장관이 정하는 보안요건을 충족하는 경우 허용되는 거래 유형
10) PADFA Division I의 제2조 제c항 제4호는 '외국 적대세력 국가'를 미국법전 제10편 4872(d)(2)에서 명시된 국가(▲북한 ▲중국 ▲러시아 ▲이란)로 정의

이는 의료서비스의 특수성과 지역별 특성을 고려한 효과적인 관리감독을 위한 것임

- 연방정부 차원의 주요 규제기관 및 역할은 다음과 같음
  - **(보건복지부)** 보건복지부(Department of Health and Human Services, HHS)는 ▲디지털 헬스케어 전반에 대한 국가 정책 수립 및 전략 방향 제시 ▲디지털 헬스케어 표준 및 가이드라인 개발 ▲연방정부 차원의 의료 데이터 표준화 추진 ▲디지털 헬스케어 관련 연구개발 지원 및 육성정책수립 ▲원격의료 확대를 위한 제도적 기반 마련을 담당
  - **(식품의약국)** 식품의약국(Food and Drug Administration, FDA)은 ▲디지털 헬스케어 관련 의료기기 및 소프트웨어의 안전성·유효성 평가 ▲의료기기 분류체계에 따른 차등 규제 적용 ▲소프트웨어의료기기(SaMD) 관련 특별 규제체계 운영 ▲사이버보안 가이드라인 제정 및 업데이트 ▲디지털 헬스케어 제품의 시판 전 승인 및 시판 후 안전관리 담당
  - **(메디케어·메디케이드서비스센터)** 메디케어·메디케이드서비스센터(Centers for Medicare & Medicaid Services, CMS)는 ▲원격의료 서비스의 메디케어·메디케이드 보험급여 기준 수립 ▲디지털 헬스케어서비스의 수가 책정 및 지불제도 설계 ▲원격의료 서비스의 품질 평가 및 모니터링 체계 운영 ▲취약계층에 대한 디지털 헬스케어 접근성 보장 정책 수립 ▲보험청구 및 지불 시스템의 디지털화 추진 담당
  - **(시민권리국)** 시민권리국(Office for Civil Rights, OCR)은 ▲HIPAA 프라이버시 규칙 및 보안 규칙 집행 ▲의료정보 보호 관련 법규 위반 시 조사 및 제재 ▲의료정보 보호 관련 가이드라인 개발 및 교육 제공 ▲환자의 의료정보 접근권 보장 ▲의료정보 유출 사고 조사 및 대응 담당
- 주정부 차원의 규제는 각 주의 특성을 반영하여 다음 사항을 중점적으로 관리함
  - **(의료면허 발급 및 관리)** ▲주 의료위원회를 통한 의료인 면허 발급 및 갱신 ▲타주 의료인의 원격의료 제공 자격 심사 ▲원격의료 제공자에 대한 특별 자격요건 설정 ▲의료인 징계 및 면허 취소 등 관리감독 ▲지속적 의료교육 요건 설정 및 관리 담당
  - **(기업의료행위 제한)** ▲영리법인의 의료기관 소유 제한 ▲의료인과 비의료인 간 고용관계 규제 ▲의료서비스 제공 주체의 자격요건 설정 ▲원격의료 서비스 제공기관의 설립 요건 규정 ▲의료기관 운영구조에 대한 규제 담당
  - **(소비자보호)** ▲주별 의료정보보호법 제정 및 시행 ▲원격의료 서비스 품질관리 기준 설정 ▲의료사고 피해구제 제도운영 ▲의료분쟁 조정제도운영 ▲의료광고 규제 담당

4. 중국의 규제 동향

▶ 중국의 디지털 헬스케어 데이터 보호 규제 체계는 일반법과 산업별 특별 규제가 결합된 형태로 구성되어 있음

• 일반 법률 체계는 다음과 같이 구성됨

- **(개인정보보호법)** '21년 11월 1일 시행된 개인정보보호법은 개인정보 처리에 대한 기본법으로서 의료분야를 포함한 전 산업에 적용됨
- **(데이터안전법)** '21년 시행된 데이터보안법은 데이터 보안과 관련된 기본 원칙과 요구 사항을 규정
- **(네트워크안전법)** 네트워크 운영자의 사이버보안 의무와 개인정보보호 의무를 규정하며, 네트워크 안전 등급 보호 제도 준수를 의무화함

• 산업별 특별규제는 다음과 같이 구성됨

- **(의료 빅데이터 관리 방법)** '18년 국가위생건강위원회가 발표하여, 의료 데이터의 활용과 보호에 대한 산업 특화 요구 사항을 규정
- **(의료정보보안 지침)** '20년 발표되어 의료정보보호를 위한 포괄적인 지침 제공
- **(인터넷진료 관리 방법)** '18년 국가위생건강위원회와 국가중의약관리국이 공동 발표하여, 인터넷을 통한 진료 행위 전반을 규율
- **(인터넷병원 관리 방법)** '18년 국가위생건강위원회와 국가중의약관리국이 공동 발표하여, 인터넷 병원의 설립과 운영에 관한 사항을 규율
- **(원격의료 서비스 관리 규범)** '18년 국가위생건강위원회와 국가중의약관리국이 공동 발표하여, 원격의료 서비스의 제공과 관리에 관한 사항을 규율

▶ 중국 개인정보보호법(中华人民共和国个人信息保护法)은 생체인식정보, 의료건강 정보 등 처리에 관한 기본 원칙을 규정하고 있음

• **(정보 주체 정보 주체의 권리보장)** 개인은 개인정보 처리에 대한 알 권리, 결정할 권리가 있으며, 타인의 처리를 제한하거나 거부할 권리 보유(제44조), 개인정보 열람권, 복사권 보장(제45조), 부정확하거나 불완전한 정보에 대한 정정·보완 요구권(제46조), 특정 상황(목적 달성, 동의 철회 등)에서의 삭제 요구권(제47조)

- **(개인정보처리 기본 원칙)** 적법성·정당성·필요성·신의성실의 원칙(제5조), 목적 제한 원칙 관련 명확하고 합리적인 목적 필요, 최소 수집 원칙 관련 최소한의 범위로 제한(제6조), 공개・투명성 원칙 관련, 처리규칙 공개, 목적·방식·범위 명시(제7조), 정확성 원칙 관련, 개인정보의 정확성과 ·완전성 보장(제8조), 안전보장 원칙 관련 필요한 보호조치 채택 의무(제9조)
- **(민감정보 특별 보호)** 민감정보란 유출 또는 불법 사용 시 개인의 인격 존엄성이나 신체・재산 안전이 침해될 수 있는 정보로서, 구체적으로 생체인식, 종교신앙, 특정 신분, 의료건강, 금융계좌, 행적 정보 및 14세 미만 미성년자의 개인정보가 포함됨(제28조)
  - **(처리요건)** 특정한 목적과 충분한 필요성이 있고, 엄격한 보호조치가 취해진 경우에만 처리 가능(제28조 제2항), 정보 주체의 별도 동의 필요하고, 법률・행정법규에서 서면동의를 요구하는 경우 해당 규정 준수(제29조)
  - **(처리자의 의무)** 민감정보 처리의 필요성과 개인의 권익에 미치는 영향을 정보 주체 정보 주체에게 고지할 의무(제30조), 14세 미만 미성년자의 정보처리 시 부모 또는 후견인의 동의 필요(제31조), 전문적인 개인정보 처리규칙 제정 의무(제31조), 사전영향평가 실시 및 처리상황 기록 의무(제55조)
  - **(행정규제)** 민감정보 처리 시 관련 행정허가나 기타 제한사항이 있는 경우 해당 규정 준수(제32조)
- **(국외이전 규제)** 중요정보기반시설 운영자와 개인정보 처리가 국가네트워크정보부문 규정 수량에 이르는 개인정보처리자는 중국 내 수집・생성된 개인정보를 반드시 국내 보관(제40조), 국외이전 시 ▲국가네트워크정보부문의 안전평가 통과 ▲전문기관의 개인정보보호 인증 획득 ▲국가네트워크정보부문이 제정한 표준계약 체결 ▲법률・행정법규 또는 국가네트워크정보부문이 규정한 기타 조건 중 하나 충족 필요(제38조)

▶ 중국 데이터안전법(中华人民共和国数据安全法)은 데이터 처리활동의 규범화, 데이터 안전 보장, 데이터의 개발·이용 촉진, 개인과 조직의 합법적 권익 보호를 위한 기본법으로서 다음과 같은 주요 내용을 규정하고 있음

- **(적용 범위)** 중국 내에서의 데이터 처리 활동 및 안전 관리·감독에 적용, 중국 외에서 중국의 국가안보, 공공이익, 개인·조직의 권익을 해치는 데이터 처리 활동도 법적책임 부과(제2조)
- **(데이터 안전)** 필요한 조치를 통해 데이터를 효과적으로 보호하고 합법적으로 이용하며 지속적 안전상태를 유지하는 능력을 의미(제3조)

- **(주무부서의 감독 책임)** 모든 지역과 부서는 각각 자신의 영역에서 수집·생성한 데이터와 그 안전에 대해 책임을 지며, 공업, 통신, 교통, 금융, 천연자원, 보건, 교육, 과학기술 등 각 분야의 주무부서는 해당 산업 및 분야의 데이터 안전 관리·감독을 책임짐(제6조)
- **(등급별 보호 체계)** 개인정보의 중요도와 유출·파괴 시 위험도에 따라 등급별 보호실시, 의료·건강 등 중요 민생 관련 데이터는 국가 핵심 데이터로 분류되어 더욱 엄격한 관리(제21조)
- **(처리자의 의무)** ▲전 과정 데이터 안전관리 제도 구축 ▲데이터 안전 교육훈련 실시 ▲필요한 기술적 조치 등 안전조치 이행을 포함한 안전관리 의무(제27조) ▲데이터 안전 결함·취약점 발견 시 즉시 보완조치 ▲데이터 안전사고 발생 시 즉시 처리조치 ▲규정에 따라 사용자에게 통지 및 관련 부서에 보고를 포함한 사고대응 의무(제29조)

▶ 중국 네트워크안전법(中华人民共和国网络安全法)은 네트워크 안전보장, 사이버 공간 주권 수호, 국가안전 보장, 개인과 조직의 합법적 권익 보호를 위한 기본법으로서 다음과 같은 주요 내용을 규정하고 있음

- **(네트워크 안전 등급 보호 제도)** 네트워크 운영자는 내부 안전관리제도와 운영매뉴얼을 제정하고, 네트워크 안전 담당자를 지정하여 네트워크 안전 책임을 이행해야 하며, 컴퓨터 바이러스, 네트워크 공격, 네트워크 침입 등을 방어하는 기술조치를 취해야 하고, 네트워크 운영상태와 보안사건을 모니터링하고 기록하는 기술조치를 실시해야 하며, 네트워크 운영일지를 최소 6개월 이상 보관해야 하고, 데이터 분류, 중요 데이터 백업, 암호화 등의 조치를 취해야 함(제21조)
- **(사전 고지 및 동의 의무)** 네트워크 제품·서비스가 사용자 정보를 수집하는 기능이 있는 경우, 해당 제공자는 사용자에게 이를 명시적으로 알리고 사용자의 동의를 얻어야 함(제22조)
- **(개인정보 수집 및 사용 원칙)** 적법성, 정당성, 필요성의 원칙 준수 의무, 수집·사용 규칙의 공개 의무, 수집·사용의 목적, 방식, 범위를 명시하고 정보 주체의 동의 획득 필요(제41조), 제공하는 서비스와 무관한 개인정보 수집 금지, 법률, 행정법규 및 쌍방 약정을 위반한 개인정보 수집·사용 금지(제41조)
- **(정보 주체의 열람·정정권)** 개인은 네트워크 운영자가 법률·행정법규 또는 쌍방 약정을 위반하여 개인정보를 수집·사용한 경우 삭제 요구 가능, 수집·저장된 개인정보에 오류가 있는 경우 정정 요구 가능, 네트워크 운영자는 이러한 요구에 따라 삭제 또는 정정 조치를 취해야 함(제43조)

- **(기술적·관리적 보호조치)** 네트워크 운영자의 수집 개인정보 유출·변조·훼손 금지, 정보 주체의 동의 없이 타인에게 개인정보 제공 금지, 기술조치와 기타 필요조치를 통한 개인정보 안전보장 의무, 개인정보 유출·훼손·분실 발생 또는 위험 시 즉시 ▲구제조치 실시 ▲사용자에게 통지 ▲관련 주관부문에 보고(제42조)

▶ 의료 빅데이터 관리방법(国家健康医疗大数据标准、安全和服务管理办法(试行))[11]은 '18. 7. 국가위생건강위원회(国家卫生健康委员会)가 발행한 규정으로 ▲의료정보의 표준화 ▲안전한 관리 ▲서비스 제공에 관한 전반적인 관리 체계를 규정하고 있으며, 특히 개인의 의료정보 보호에 중점을 두고 있음

- (정보 주체의 기본권리 보장) 국가가 공민(公民)의 알권리, 사용권 및 개인 프라이버시를 보장하는 기초 위에서 건강의료정보를 관리하고 활용한다고 규정하여 정보 주체의 기본권을 명시하고 있음(제2조)
- (개인정보 보호 의무) 각급 의료기관이 '일파수(一把手: 최고책임자) 책임제'를 실행하여 안전보장체계를 구축하고 의료 빅데이터의 안전을 보장해야 한다고 규정하고 있음(제17조)
- (기술적·관리적 보호조치) 데이터 분류, 중요 데이터 백업, 암호화 인증 등의 조치를 통해 건강의료 빅데이터의 안전을 보장해야 한다고 규정하고 있고(제18조), 서로 다른 등급의 사용자의 데이터 접근과 사용 권한을 엄격히 규범화해야 한다고 명시하고 있음(제22조)
- (개인정보 처리 원칙) 법률에 따라 건강의료 빅데이터 관련 정보를 안전하게 사용해야 한다고 규정하고 있고(제21조), 엄격한 전자실명인증과 데이터 접근통제를 시행하며, 모든 데이터 접근 행위가 관리 및 통제가능하며 서비스 관리 전 과정에서 흔적이 남아야 하고, 조회와 추적이 가능해야 한다고 규정(제23조)
- (국외 이전 제한) 건강의료 빅데이터는 반드시 국내의 안전하고 신뢰할 수 있는 서버에 저장되어야 하고, 국외 제공이 필요한 경우 관련 법률 및 요구 사항에 따라 안전평가심사를 진행해야 한다고 규정하고 있음(제30조)
- (정보 공개와 제한) 국가기밀, 상업비밀 및 개인 프라이버시를 누설해서는 안되며, 국가이익, 사회공공이익과 공민, 법인 및 기타 조직의 합법적 권익을 침해해서는 안된다고 규정(제35조)

11) http://www.nhc.gov.cn/mohwsbwstjxxzx/s8553/201809/f346909ef17e41499ab766890a34bff7.shtml

▶ 의료데이터보안지침(信息安全技术 健康医疗数据安全指南)[12]은 '20년 12월 국가표준화관리위원회(国家标准化管理委员会)가 발행한 지침으로, 의료정보 컨트롤러의 개인정보 보호를 위한 보안 조치 규정

- **(수집단계 보안통제)** 개인의 건강의료정보 수집 시 정보 주체의 동의 필요, 개인정보 수집 목적, 범위, 방법, 보유기간 등을 명확히 고지, 합법적이고 필요한 최소한의 범위 내 수집 원칙
- **(저장단계 보안조치)** 개인정보 저장 시 암호화 기술 적용 의무, 생체인증정보는 요약정보만 저장, 백업 및 복구 체계 구축
- **(사용·공개 단계 보안관리)** 정보 주체의 접근권·열람권·정정권 보장, 사용이력에 대한 6년간의 추적조회 권한 보장, 최소 사용·공개 원칙 준수
- **(국외이전 시 보안요구 사항)** 학술연구 목적의 경우 250건 이내는 비식별화 후 데이터 보안위원회 승인으로 가능, 해외 서버 저장 및 임대 금지
- **(조직구조 및 책임자)** ▲고위 관리자 및 각 사업부서장, 정보보안·윤리·법률 관련 전문가가 책임자로 포함 ▲최고책임자가 위원장 역임하여 의료정보보안위원회 설치 의무 ▲일상보안업무 수행 ▲보안전략 수립·갱신 ▲연간 보안점검 등 담당하는 의료정보보안사무실 설치
- **(위험평가 및 모니터링)** 보안위험 평가계획 수립, 정기적 모니터링 및 검사 수행, 개선계획 수립 및 이행
- **(비상대응체계)** 연 1회 이상 비상훈련 실시, 전담 비상대응 및 전문가팀 구성, 재해복구계획 수립, 사고 발생 시 서면보고 의무

▶ 인터넷 진료 관리방법(互联网诊疗管理办法), 인터넷병원 관리방법(互联网医院管理办法), 원격의료 서비스 관리규범(远程医疗服务管理规范)[13]은 '18년 7월 국가위생건강위원회(国家卫生健康委员会)와 국가중의약관리국(国家中医药管理局)이 공동 발표

- **(정보보안 등급 보호)** 의료기관은 제3급 정보보안 등급 보호를 실시해야 하고(인터넷

12) https://irb.sjtu.edu.cn/info/1039/1571.htm
13) https://www.gov.cn/gongbao/content/2019/content_5358684.htm

진료 관리방법 제13조), 인터넷 병원 정보 시스템은 국가 관련 법률법규와 규정에 따라 제3급 정보보안 등급 보호를 실시해야 함(인터넷 병원 관리방법 제15조)

- **(전자 실명인증)** 의료기관은 의료인력에 대해 전자 실명인증을 실시해야 하며, 생체인식 등 인체특징 식별기술을 통한 의료인력 관리 강화 권장(인터넷 진료 관리방법 제14조), 인터넷 병원은 의료인력에 대해 전자 실명인증을 실시하고, 생체인식 등 인체특징 식별기술을 통한 관리 강화 권장(인터넷 병원 관리방법 제16조)
- **(전자병력 관리)** '의료기관 병력관리규정'과 '전자병력 기본규범'에 따라 환자의 전자병력을 작성하고 관리해야 하고(인터넷 진료 관리방법 제17조), 환자는 온라인으로 검사결과, 진단치료방안, 처방전 등 병력자료 조회 가능(인터넷 병원 관리방법 제21조)
- **(정보보안 및 프라이버시 보호)** 의료기관은 정보보안과 의료정보 비밀보호 관련 법률법규를 엄격히 준수하고, 환자정보를 적절히 보관하며, 불법 매매·유출 금지(인터넷 진료 관리방법 제20조), 정보유출 발생 시 즉시 주관부서 보고 및 대응조치 실시(인터넷 병원 관리방법 제23조)
- **(개인정보 추적성 보장)** 의료기관은 인터넷 진료활동의 전 과정에서 추적가능성을 보장하고, 감독부서에 데이터 인터페이스 개방(인터넷 진료 관리방법 제24조), 각 참여기관은 정보보안과 환자 프라이버시 보호를 강화하고, 불법 전송·수정 방지, 개인정보 손실 방지, 개인정보보안 관리규정 수립(원격의료 서비스 관리규범 제4조 제1항)

▶ 규제 위반 시 개인정보보호법, 데이터안전법, 네트워크안전법, 의료 빅데이터 관리방법에 따른 제재가 적용됨

- 개인정보보호법에 따른 제재는 아래와 같음
  - **(기본 제재)** ▲시정명령·경고·부당이득 몰수 ▲위법한 앱에 대한 서비스 제공 중단·종료 명령 ▲시정 거부 시 100만 위안(약 1억 9천만 원) 이하 과징금 ▲책임자·관련자에게 1만~10만 위안(약 194만 원~1,940만 원) 과징금(제66조)
  - **(중대 위반 시 가중 제재)** ▲5천만 위안(약 97억 원) 이하 또는 전년도 매출액 5% 이하 과징금 ▲업무정지 및 영업정지 명령 가능 ▲사업허가 및 영업면허 취소 가능 ▲책임자·관련자에게 10만~100만 위안(약 1,940만 원~약 1억 9천만 원) 과징금 ▲일정기간 임원 취임 제한(제66조)
  - **(신용제재)** 위법행위는 신용조사서에 기재되어 공시됨(제67조)

- **(국가기관 관련 제재)** ▲상급기관·담당부서의 시정명령 ▲책임자·관련자에 대한 처분 ▲직무유기, 직권남용, 부패행위에 대한 처분(제68조)
- **(민사책임)** ▲개인정보 침해로 인한 손해배상 책임 ▲개인의 손실·처리자의 이익을 기준으로 배상액 산정 ▲산정 어려운 경우 실제 상황 고려하여 결정(제69조)
- **(집단소송)** 다수 피해자 발생 시 검찰, 소비자단체, 정부지정기관이 소송 제기 가능(제70조)
- **(형사책임)** 치안관리 위반행위 시 치안관리처벌, 범죄 구성 시 형사책임 추궁(제71조)

• 데이터안전법에 따른 제재는 아래와 같음

- **(행정처벌)** ▲일반 데이터 안전 의무 위반의 경우 5만~50만 위안(약 970만 원~9,700만 원)(제45조) ▲시정조치 불이행·중대결과 발생의 경우 50만~200만 위안(약 9,700만 원~3억 8천만 원)(제45조) ▲핵심 데이터 관리 위반의 경우 200만~1000만 위안(약 3억 8천만 원~약 19억 원)(제45조) ▲중요 데이터 무단 국외이전의 경우 일반 위반의 경우 10만 위안 이상 100만 위안(약 1,940만 원~1억 9천만 원) 이하의 벌금, 중대 사안의 경우 100만 위안 이상 1000만 위안(약 1억 9천만 원~19억 원) 이하의 벌금(제46조) ▲데이터 거래 중개의무 위반 관련, 불법소득이 있는 경우 불법소득의 1배 이상 10배 이하의 벌금, 불법소득이 없거나 10만 위안(약 1,940만 원) 미만인 경우는 10만 위안 이상 100만 위안(약 1,940만 원~1억 9천만 원) 이하의 벌금(제47조) ▲데이터 제공 협조의무 위반의 경우 5만~50만 위안(약 970만 원~9,700만 원)(제48조) ▲무단 해외제공 제재 시 일반적인 위반의 경우 기관에 대하여 경고, 10만 위안 이상 100만 위안(약 1,940만 원~약 1억 9천만 원) 이하의 벌금, 직접 책임자에 대하여 1만 위안 이상 10만 위안(약 194만 원~1,940만 원) 이하의 벌금, 중대한 결과 초래 시 기관에 대하여 100만 위안 이상 500만 위안(약 1억 9천 만원~9억 7천만 원) 이하의 벌금, 관련 업무 일시 정지, 영업 정지, 관련 업무 허가증 취소, 사업 자등록증 말소 가능하고, 직접 책임자의 경우 5만 위안 이상 50만 위안(약 970만 원~9,700만 원)이하의 벌금(제48조)
- **(민사 책임)** 본 법의 규정을 위반하고 타인에게 손해를 초래할 경우 민사 책임 부담 가능(제52조)
- **(형사 책임)** ▲핵심 데이터 관리제도 위반으로 국가주권, 안전 및 발전이익 위해 시(제45조) ▲치안관리처벌법 위반 시(제52조) ▲기타 형법상 범죄 구성 시(제52조) 형사책임 부과 가능

- 네트워크안전법에 따른 제재는 아래와 같음
  - **(일반 네트워크 운영자 관련 행정 제재)** ▲네트워크 안전 의무 미이행 시 1만~10만 위안 (약 194만 원~1,940만 원) 과태료 책임자 개인에게 5천~5만 위안(약 97만 원~970만 원) 과태료 부과(제59조) ▲악성 프로그램 설치, 보안결함 미조치, 유지보수 무단중단 시 5만~50만 위안(약 970만 원~9,700만 원) 과태료, 책임자 개인에게 1만~10만 위안(약 194만 원~1,940만 원) 과태료 부과(제60조) ▲이용자 신원확인 의무 위반 시 5만~50만 위안(약 970만 원~9,700만 원) 과태료, 업무정지·영업정지·허가취소 가능(제61조)
  - **(핵심 정보 인프라 운영자 관련 행정 제재)** ▲안전의무 미이행 시 10만~100만 위안 (약 1,940만 원~약 1억 9천만 원) 과태료, 책임자 개인에게 1만~10만 위안(약 194만 원~1,940만 원) 과태료 부과(제59조) ▲승인되지 않은 제품·서비스 사용 시 구매금액의 1~10배 과태료(제65조), 데이터를 해외에 저장하거나 안전평가 없이 해외에 제공하는 규정 위반 시 5만~50만 위안(약 970만 원~9,700만 원) 과태료, 영업정지·허가취소 가능(제66조)
  - **(개인정보 보호 관련 제재)** ▲개인정보 보호의무 위반 시 불법소득 몰수 및 1~10배 과태료, 소득이 없는 경우 100만 위안(약 1억 9천만 원) 이하 과태료(제64조) ▲정보 불법 취득·판매 시 불법소득 몰수 및 1~10배 과태료, 소득이 없는 경우 100만 위안 (약 1억 9천만 원) 이하 과태료(제64조)
  - **(형사 처벌)** 네트워크 안전 위해활동이 형사처벌 조항에 해당하는 경우 형사책임 부과(제74조), 특히 중대한 위반행위에 대해서는 치안관리처벌(구류)과 함께 과태료 병과 가능하고 ▲일반적인 경우 5일 이하 구류와 5만~50만(약 970만 원~9,700만 원) 위안 과태료 ▲중대한 경우 5-15일 구류와 10만-100만 위안(약 1,940만 원~약 1억 9천만 원) 과태료(제63조)
  - **(민사 책임)** 타인에게 손해를 초래한 경우 민사상 손해배상책임 부담(제74조)
- 의료 빅데이터 관리방법 위반 시 위반한 단위와 개인에 대해 "면담, 감독 시정, 경고, 통보 비평, 처분 등의 조치를 취할 수 있으며, 위법을 구성하는 경우 사법기관에 이송하여 법적 책임을 추궁함(제40조)

5. EU, 미국, 중국의 의료정보 활용 현황 및 개인정보 보호 이슈

▶ 디지털 헬스케어 시대에서 의료정보 및 건강정보의 활용은 진단 정확성 향상과 개인 맞춤형 치료 계획 수립, 운영 효율 최적화에 크게 기여하고 있음

- **(AI 진단 도구)** AI 기반 진단 도구를 통해 의료 영상을 높은 정밀도로 분석하여 암과 같은 질병의 조기 발견을 지원함
- **(맞춤형 치료)** AI가 개개인의 환자 데이터를 기반으로 질병 진행을 예측하고 맞춤형 치료 계획을 추천하는 것이 가능함
- **(원격 모니터링)** 웨어러블 기기를 통해 체온, 맥박, 혈압, 호흡 등 기본적인 건강 상태를 원격으로 관찰할 수 있음
- **(의료 효율성)** AI 기술이 의료서비스의 운영 효율을 최적화하고 비용 절감에 기여함

▶ 의료정보 활용이 확대됨에 따라 다음과 같은 개인정보 보호 문제들이 제기되고 있음

- **(데이터 품질)** AI 시스템의 정확성과 신뢰성 확보를 위해 대표성을 가진 양질의 데이터 확보가 필요함
- **(투명성)** 의료전문가와 규제기관의 관리·감독을 위해 AI 시스템의 작동 방식, 한계점, 의사 결정 과정을 명확히 기록해야 함
- **(보안 위험)** 의료기기나 시스템이 해킹될 경우 환자 정보 유출과 치료 시스템 마비 등 심각한 피해가 발생할 수 있음
- **(개인정보 보호)** 민감한 건강정보를 다루는 과정에서 개인정보보호법 등 관련 법규를 준수하고 데이터의 정확성을 유지해야 함
- **(인적 요소)** 의료진이 AI 시스템을 제대로 활용할 수 있도록 체계적인 교육과 훈련이 필요함
- **(차별 방지)** 의료 데이터의 편향으로 인한 의료 격차가 발생하지 않도록 주의해야 함
- **(보안 모니터링)** 의료기관은 보안 위험을 실시간으로 감지하고 대응할 수 있는 지속적인 관리 체계를 갖춰야 함
- **(데이터 접근 통제)** 환자의 의료정보 접근 권한을 철저히 관리하고 무단 접근을 차단하는 위험 체계 구축이 필요함

▶ 한편, 디지털 헬스케어의 발전으로 의료정보 및 건강정보의 활용가치가 증대되면서 EU, 미국, 중국은 각기 다른 방식으로 의료정보를 활용하고 있으며, 이에 따른 개인정보 보호 이슈도 다양하게 대두되고 있음

▶ EU는 EHDS(European Health Data Space)[14]를 통해 회원국 간 의료데이터 공유 체계를 구축하여 연구·혁신을 지원하고 있으며, 개인 맞춤형 치료와 희귀질환 연구, 예방의료 강화 등을 추진하고 있음

- **(개요 및 목적)** EU의 보건 연합(Health Union)의 핵심이자 유럽 데이터 전략의 첫 공통 데이터 공간으로, 2024년 3월 유럽 의회와 이사회가 EHDS 도입에 합의함
- **(주요 기능)** ▲EU 전역에서 개인의 의료정보 자기결정권 강화 및 데이터 교환 활성화(데이터 1차 활용) ▲전자건강기록(EHR) 시스템을 통한 단일 시장 구축 ▲연구, 혁신, 정책 수립을 위한 안전하고 효율적인 데이터 재활용 체계 마련(데이터 2차 활용)
- **(법적 프레임워크)** ▲GDPR ▲Data Governance Act(데이터 거버넌스 법) ▲Data Act(데이터 법) ▲Network and Information Systems Directive(네트워크 및 정보 시스템 지침)을 기반으로 하되, 건강정보의 민감성을 고려한 부문별 규칙 제공
- **(정보 제공 거부권)** EHDS는 데이터 활용 목적에 따라 1차 활용과 2차 활용에 대한 차등적인 거부권(opt-out) 적용
  - **(1차 활용)** 진료, 처방, 치료 등 직접적 의료서비스 제공을 위한 경우, 회원국 국민들에게 EHDS 참여 거부권을 전적으로 부여
  - **(2차 활용)** 연구, 정책 수립, 통계 작성 등 기타 목적의 경우, 개인의 정보 자기결정권과 공익적 필요성을 고려해 제한적 거부권 부여
- **(당면 과제)** ▲의료영상 등 신기술 발전으로 데이터 익명화가 더욱 어려워져 민감정보 판단 기준 설정에 기술적 한계 존재 ▲회원국별로 정보 제공 거부권(opt-out) 도입과 민감정보 처리절차를 자율적으로 결정할 수 있어 데이터 동의체계의 분절화 우려 ▲복잡한 동의절차로 인한 데이터 수집의 편향 발생이 시스템 목적 달성을 저해할 수 있는 문제 ▲EU 회원국 간 윤리적 가치와 법 해석 차이로 데이터 공유가 제한됨에 따라 투명성·보안·형평성에 기반한 시스템 설계로 신뢰 확보 필요

14) EU 의회와 이사회가 '24년 3월 합의한 유럽의 의료데이터 공유를 위한 새로운 규제 프레임워크

▶ 미국은 EHR(전자건강기록) 도입과 정밀의료 계획을 통해 의료 혁신을 추진하고, 실제임상데이터를 활용한 신약개발과 의료기기 혁신, 원격의료 확대 등을 적극 추진하고 있음

- 연방법과 주법의 혼재, HIPAA의 제한적 적용 범위, 데이터 브로커에 의한 무분별한 정보 활용 등이 주요 개인정보 보호 이슈로 제기되고 있음
- '24년 HIPAA 개인정보 보호 규칙이 업데이트되어 생식 건강정보에 대한 보호를 강화함

▶ 중국은 인터넷병원과 AI 의료기기 개발을 통한 디지털화, 의료 빅데이터 산업 육성, 의료자원 분배 최적화 등을 추진하면서 의료정보 활용을 확대하고 있음

- 이와 함께 개인정보보호법 등 관련 법제를 정비하고 데이터 국외이전 제한, 보안평가 의무화, 기업 책임 강화 등 강력한 규제를 실시하고 있음

6. 시사점

▶ 각국의 디지털 헬스케어 관련 개인정보 규제는 각국의 법체계와 접근방식에 따라 서로 다른 특성을 보이므로, 이러한 각국 규제 특성을 고려한 차별화된 대응 전략 수립이 필요

- EU는 GDPR을 통해 건강정보를 특별 범주로 분류하고 정보 주체 정보 주체의 동의권과 통제권을 강조하는 등 개인의 권리보호를 최우선시하는 보수적 접근방식을 취하고 있으며, 개인정보 보호를 디지털 헬스케어 발전의 필수 전제조건으로 인식하고 있음
- 반면 미국은 의료산업의 발전과 혁신을 저해하지 않는 범위 내에서 규제하고, 연방법과 주법의 이원화된 체계를 통해 유연성을 확보하는 등 실용적이고 산업 친화적인 접근방식을 보이고 있음
- 중국은 데이터 현지화 요구 등 국가 차원의 통제력을 강화하면서도 디지털 헬스케어 산업 육성과 개인정보 보호의 균형을 도모하는 등 국가 주도의 하향식 규제체계를 운영하고 있음

▶ 또한, 공통적인 규제 준수 사항에 대한 우선적 대응이 요구되는데 ▲건강 정보 수집·이용에 대한 명시적 동의 획득 ▲데이터 최소화 원칙 준수 ▲기술적·관리적 보호조치 이행 ▲국외이전 시 엄격한 안전성 확보 조치실시가 필요함

▶ 법규 위반 시 고액의 과징금과 형사처벌 등 강력한 제재가 부과되므로, 규제 준수를 위한 상시 모니터링 체계 구축과 정기적인 내부 감사 실시가 요구됨

[참고 자료]

- 최선미, 김경진, "데이터 3법 기반 디지털 헬스케어 산업에서 안전한 데이터 활용에 관한 연구", 한국융합학회논문지 Vol.13 (2022)
- 연미영, "디지털 헬스케어 정책 현황: 소비자 참여 기반의 디지털 헬스케어 활성화를 위한 검토", 소비자정책동향 제130호 (2023)
- Chambers and Partners, "Chambers Global Practice Guides" (2024)
- eHealth Network GUIDELINE on the electronic exchange of health data under Cross-Border Directive 2011/24/EU
- REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
- Hannah van Kolfschooten, Janneke van Oirschot, "The EU Artificial Intelligence Act (2024): Implications for healthcare", Health policy 149 (2024)
- REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC
- DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)
- European Commission, "Study on Health Data, Digital Health and Artificial Intelligence in Healthcare", 2021. 7.
- 인천연구원, "중국 디지털 헬스케어 산업의 발전전략과 시사점", 한중Zine INChinaBrief Vol.389 (2020)
- 선종수, "중국의 디지털 헬스케어 현황과 시사점", 대외경제정책연구원 (2022)
- 백서인 · 박동운 · 손은정 · 김영진 · 윤여진 · 김병국 · 곽기호 · 이제영, "2021년 중국(중화권) 첨단기술 모니터링 및 DB 구축 사업: 스마트 에듀·디지털 헬스케어", 과학기술정책연구원 (2021)
- 中华人民共和国个人信息保护法
- 中华人民共和国数据安全法
- 中华人民共和国网络安全法
- 国家健康医疗大数据标准、安全和服务管理办法

- 信息安全技术 健康医疗数据安全指南
- 互联网诊疗管理办法, 互联网医院管理办法, 远程医疗服务管理规范
- Health Information Technology for Economic and Clinical Health Act
- Health Insurance Portability and Accountability Act
- The Health Sector Cybersecurity Coordination Center, "An advisory on the rise of voice phishing attacks in the healthcare sector", 2022. 8.
- The European Union Agency for Cybersecurity, Cybersecurity in the healthcare sector during COVID-19 pandemic, 2020. 5.
- The Maxim Healthcare Group, Notice of Data Privacy Incident, 2021. 11.
- Michael Borrelli, "EU: The impact of the EU AI Act on the healthcare sector", 2024. 7.
- Hannah Petit, "International: Risks of AI for the healthcare sector", 2024. 8.
- FDA, FDA informs health care providers, facilities and patients about potential cybersecurity vulnerabilities for certain GE Healthcare Clinical Information Central Stations and Telemetry Servers, 2020. 1.
- 21st Century Cures Act
- Emmanuel Pernot-Leplay, "China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?", Penn State Journal of Law & International Affairs, 2020. 5.
- Yu Yao, Fei Yang, "Overcoming personal information protection challenges involving real-world data to support public health efforts in China", Frontiers, 2023. 9.
- Xinyuan Shi, "Reducing privacy risks of China's healthcare big data through the policy framework", Frontiers, 2024. 7.
- Andreas Ruediger, "The European Health Data Space – What lies ahead?", 2024. 6.
- Jaisalmer de Frutos Lucas, Hans Torvald Haugo, "Moving forward with the European health data space: the need to restore trust in European health systems", 2024. 4.