사이버보안 강화를 위한 체외진단 의료데이터 분류 및 보호방안 연구

연세대학교 대학원

의료기기산업학과

이 나 경

사이버보안 강화를 위한 체외진단 의료데이터 분류 및 보호방안 연구

지도교수 한 승 환

이 논문을 석사 학위논문으로 제출함

2025 년 06 월

연세대학교 대학원

의료기기산업학과

이 나 경

사이버보안 강화를 위한
체외진단 의료데이터 분류 및 보호방안 연구

이나경의 석사 학위논문으로 인준함

심사위원장 한 승 환

심사위원 김 성 환

심사위원 정 호 넌

연세대학교 대학원
의료기기산업학과

2025년 06월

차 례

표 차례

그림 차례

국 문 요 약

사이버보안 강화를 위한
체외진단 의료데이터 분류 및 보호방안 연구

최근 체외진단(In Vitro Diagnostics, IVD) 시장은 인공지능(AI), 사물인터넷(IoT), 원격의료 등의 기술 발전에 힘입어 급속히 성장하고 있으며, 이에 따라 의료데이터의 양과 복잡성 또한 급증하고 있다. 그러나 이러한 기술 발전은 사이버 위협 증가로 이어져 보안 취약성에 대한 우려가 커지고 있다. 특히, 체외진단 의료기기에서 생성되는 의료데이터는 환자의 유전자 정보, 감염병 검사 결과 등 고도의 민감 정보를 포함하고 있어, 유출, 위·변조 시 환자의 안전 및 사회적 신뢰에 심각한 영향을 미칠 수 있다.

본 연구에서는 체외진단 분야에서 생성되는 의료데이터를 민감도와 유출 시 피해 규모인 위험도를 기준으로 분류하고, 등급별로 암호화, 다중 인증, 접근 제어 등 차등화 된 보안 대응방안을 제시한다. 이를 통해 사이버 위협으로 인한 데이터 유출 및 오남용 위험을 최소화하고, 체외진단 분야의 보안 체계 강화에 기여하고자 한다.

체외진단 의료데이터의 민감도·위험도 기반 분류 및 보안 전략은 의료기관 및 관련 기업의 보안 정책 수립을 지원하고, 환자 안전과 의료 서비스 신뢰성 향상에 도움이 될 것으로 기대된다.

핵심 되는 말: 체외진단, 의료데이터, 사이버 보안

I. 서론

1. 연구 배경

가. 체외진단 시장

최근 질병 진단의 패러다임은 조기 진단 및 예방의학 중심으로 변화하고 있다. 정보통신기술과 의료기기의 융합은 혁신적인 의료 서비스를 가능하게 하며, 예방 중심의 산업 구조로 변화하고 있다. 이에 따라 체외진단 시장의 수요는 지속적으로 증가할 것으로 전망된다. 진단의 효율성과 정확성을 높이기 위해 인공지능(AI) 기술이 적용된 소프트웨어 및 웨어러블 기기, 신종 감염병 진단, 유전자 정보를 활용한 개인 맞춤형 진단의 확대 등으로 체외진단 의료기기의 적용 범위는 점차 확대되고 있으며, 이에 따라 시장의 성장이 가속화될 것으로 보인다.

시장조사기관 Frost&Sullivan 의 시장 자료에 따르면, 체외진단 시장은 2021 년 992 억 2,000 만 달러에서 연평균 6.9%의 성장률을 보이며 2026 년까지 지속적으로 성장할 것으로 전망된다. 즉, 글로벌 체외진단 시장은 2021 년 기준 992 억 2,000 만 달러에서 연평균 6.9% 성장하여 2026 년에는 약 1,383 억 달러 규모에 이를 것으로 예측된다. [1] 또한, 리서치 기관인 Knowledge Sourcing Intelligence 에서 발표한 전 세계의 체외진단(IVD) 시장 예측(2024-2029 년) 자료에 따르면 2024 년 1,034 억 1,500 만 달러에서 2029 년 1,390 억 8,400 만 달러에 달할 것으로 예상된다.[2]

표 1 체외진단 시장 성장 요인

구분	성장요인
1	인구 고령화로 인한 만성질환자 증가
2	개인 맞춤형 의료 인식 개선, 소비자(환자)가 직접 진단하는 산업 구조로 전환

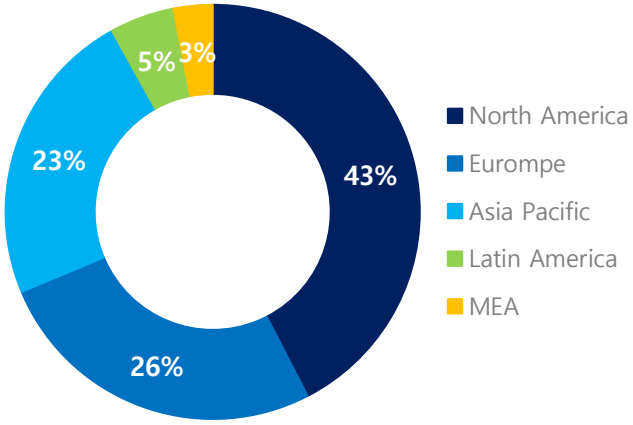
3	원격 의료 및 디지털 기술 발전에 따른 직접 진단 비즈니스 모델 성장 가속화
4	사물인터넷(IoT) 기술, 인공지능 기반 분석, 의료기기 간 연결을 통한 자동화

(출처: Frost and Sullivan, 한국 IR 협의회 기업리서치센터)

Precedence Research 에 따르면, 지역별 체외진단 시장 점유율은 북미에서 가장 큰 비중을 차지하고 있으며, 높은 의료 수준과 만성질환의 증가로 향후 시장 점유율도 지속적으로 확대될 것으로 전망된다. 아시아 태평양 지역은 빠른 경제 성장과 향상된 의료 솔루션에 대한 수요 증가로 인해 예측 기간 동안 가장 높은 연평균 성장률을 기록할 것으로 예상된다. 고령 인구 증가와 감염성 및 만성질환의 유병률 상승, 정밀 진단이 가능한 체외진단 시스템의 발전이 시장 성장의 주요 요인으로 작용하고 있다.

전 세계적으로 체외진단 시장의 성장을 이끄는 핵심 요인으로는 고령 인구 증가, 면역분석 기반 검사의 수요 증가, 맞춤형 의료 서비스 발전에 따른 개인 맞춤형 진단에 대한 인식 확대, 현장 진단(Point-of Care) 검사 수요 증가 등을 들 수 있다.[3]

표 2 In Vitro Diagnostics Market Share, By Region, 2023 (%)



(출처: Precedence Research, 『In Vitro Diagnostics Market Size to Hit USD 132.18 Billion by 2034』)

국내 체외진단 시장의 경우, 현장진단(Point-of-Care Testing, POCT) 시장의 성장으로 기존 중앙검사실에서 대형 장비를 이용하여 수행되던 면역화학검사와 분자진단이 점차 현장진단 방식으로 전환되고 있다. 현장진단기기는 신속한 진단 결과를 제공할 수 있어 선호도가 높아지고 있는 추세이다. 그러나 현장진단기기의 진단 프로세스는 약 50% 이상이 수동으로 이루어지고 있어, 정보기술(IT)과의 융합을 통한 기술 발전 가능성이 크다. 이러한 다양한 성장 요인에 따라, Allied Market Research 자료에 따르면 국내 체외진단 시장 규모는 2027 년에 약 1.7 조원(13.1 억 달러)에 이를 것으로 전망된다.

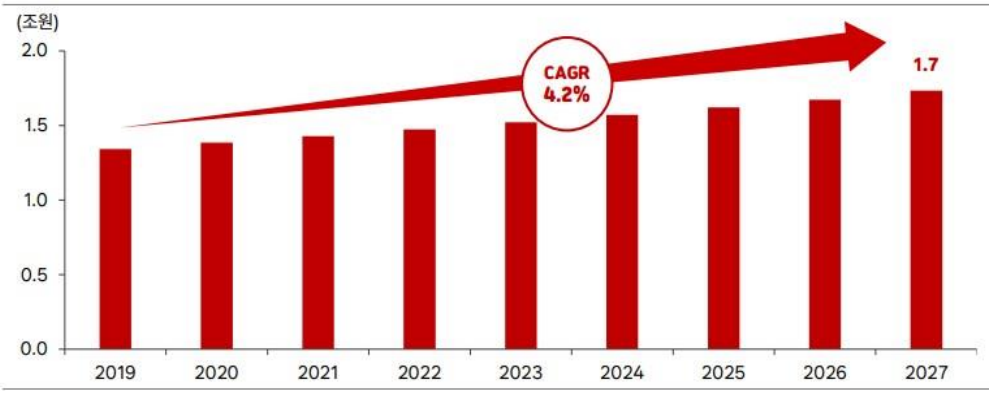


그림 1 국내 체외진단 시장 규모 및 전망

(출처: 수젠텍, 한국IR협의회 기업리서치센터)

체외진단 산업은 매우 세분화되어 있으나, 크게 중앙검사실(Central Lab)과 현장진단(Point-of-Care Testing, POCT)으로 구분할 수 있다. 중앙검사실에서 사용되는 제품은 장비와 시약류로 구성되며, 현장진단은 사용자가 원하는 장소에서 간편한 조작으로 빠르게 검사가 가능한 제품군을 포함한다. 또한 체외진단은 진단 기술 및 대상 검체에 따라 면역화학, 임상미생물, 조직진단, 지혈진단, 혈액진단, 분자진단, 자가혈당측정, 현장진단으로 분류된다.[4]

표 3 체외진단 기술 분류

분류	설명
면역화학적 진단 (Immunochemistry)	– 항원–항체 반응의 원리 이용 – 각종 암마커, 감염성질환, 감상선 기능, 빈혈, 알레르기, 임신, 약물남용 등 다양한 질환 진단과 추적에 이용
자가혈당측정 (Self-Monitoring Blood Glucose)	– 당뇨 환자가 직접 혈액으로 혈당 진단

현장진단 (POCT, Point of Care Testing)	– 면역화학적, 임상화학적 방식으로 검사하던 것을 소형 및 신속화, 즉각 검사 가능하도록 한 진단 방법 – 감염질환의 신속진단, 심근경색 검사 등에 이용
분자진단 (Molecular Diagnostics)	– 병원체나 세포의 유전정보물질(DNA, RNA)을 분석하여 질병 유무 검사 – HIV, 인유두종 바이러스(HPV)등을 검사하거나 암유전자, 유전질환 검사 등에 이용
혈액진단 (Hematology)	– 혈액이나 골수로 적혈구, 백혈구, 혈소판, 헤모글로빈 등 혈액세포 검사 – 백혈병, 빈혈, 항응고 등을 진단하거나 치료 모니터링에 이용
임상미생물학진단 (Clinical Microbiology)	– 바이러스, 세균, 진균 등을 배양 및 동정, 세균의 항생제 감수성 검사해 감염원 찾기 – 치료 약재의 가이드라인 제공, 각종 감염에 의한 질병과 진단, 추적에 이용
조직진단 (Tissue Diagnostics)	– 유리판 위에 체액을 도말, 생체조직 염색 후 현미경을 통해 분석 – 암 조직, 세포를 관찰해 진단
지혈진단 (Hemostasis)	– 혈액응고 진단 – 출혈성 질환 및 혈소판 장애, 자가면역 상태 진단

(출처: 수젠텍, 한국IR협의회 기업리서치센터)

2021 년 연구개발특구진흥재단 자료에서 Allied Market Research 가 발표한 “Global In-Vitro Diagnostics Market, 2021”을 보면 각 진단 기술에 따라 2027 년에는 더 성장할 것을 확인할 수 있다.[5] 2019 년부터 2027 년까지 면역진단 연평균

성장률 6.2%, 혈액 연평균 성장률 3.0%, 분자진단 연평균 성장률 6.7%, 조직진단 연평균 5.2%, 임상화학 분석 연평균 3.6% 증가, 기타 기술은 연평균 4.2% 증가한 시장 규모를 예상한다.[6]

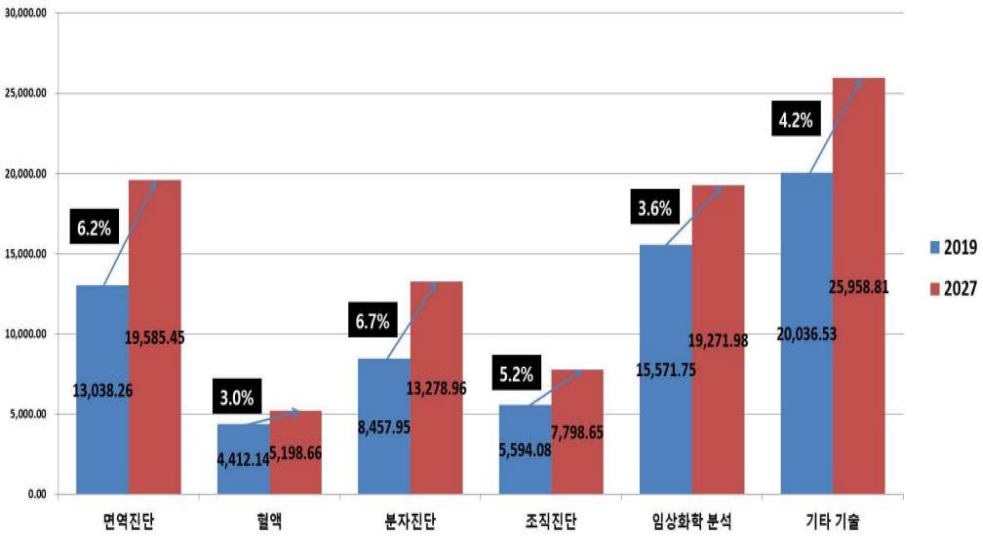
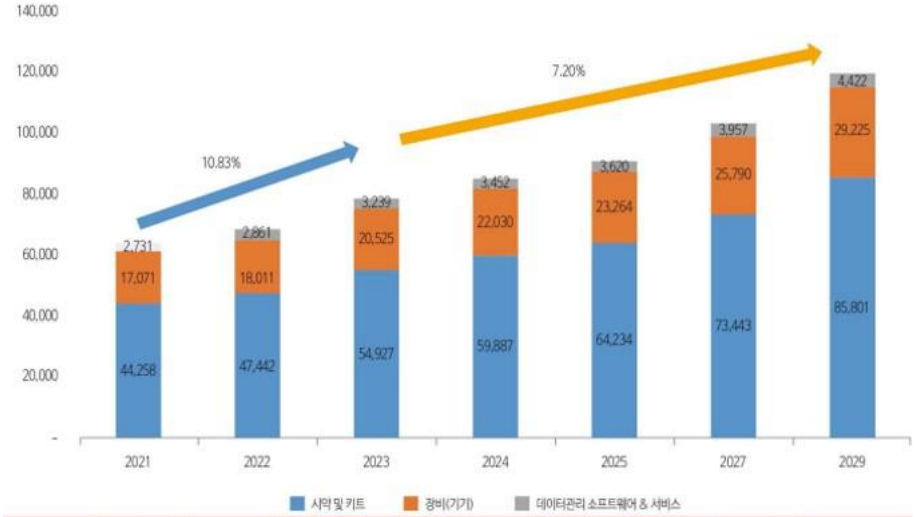


그림 2 글로벌 체외진단 시장의 기술별 시장 규모 및 전망 (단위: 백만 달러)

(출처: Allied Market Research, 『Global In-Vitro Diagnostics Market, 2021』, 연구개발특구진흥재단, 『유망시장 Issue Report : 체외진단』,2021)

체외진단 시장은 제품과 서비스에 따라 시약, 기기, 소프트웨어 및 서비스로 분류된다. 각 요인이 복합적으로 작용되어 체외진단 시장을 구성하고 있는 시약, 기기, 소프트웨어 및 서비스의 분야의 성장을 기여하고 있다. [그림 3]과 같이 각 분야의 성장률을 보면 시약 및 키트 분야는 시장에서 가장 큰 부분을 차지하고 있다. 감염병 유병률 증가, 예방 검사에 대한 인식, 질병 조기 진단에 대한 수요 증가 및 환자의 요구에 따른 다양한 진단 요구로 29년까지 연평균 7.72% 성장이 예상, 지속적으로 증가할 전망을 보인다.



	2021	2022	2023	2024	2025	2027	2029	비중('23)	CAGR ('23-'29)
시약 및 키트	44,258	47,442	54,927	59,887	64,234	73,443	85,801	69.8%	7.72%
장비(기기)	17,071	18,011	20,525	22,030	23,264	25,790	29,225	26.1%	6.07%
데이터관리 소프트웨어 & 서비스	2,731	2,861	3,239	3,452	3,620	3,957	4,422	4.1%	5.33%
Total	64,059	68,314	78,691	85,369	91,117	103,190	119,448	100.0%	7.20%

그림 3 시장 분류별 체외진단의료기기 시장 현황(단위: 백만달러, %)

(출처: 한국보건산업진흥원. 『In-Vito Diagnostics markets, global forecast to 2029, markets and markets』)

최근에는 검사 자동화의 도입과 디지털 진단 환경의 확산에 따라 데이터관리 소프트웨어 및 서비스 분야의 성장이 두드러진다. 시장조사기관의 예측하고 한국보건산업진흥원이 가공한 자료를 보면 해당 분야는 29 년까지 연평균 약 5.33%의 성장률을 나타낸다.[7] 이와 같은 증가는 단순한 장비 활용을 넘어 진단 과정에서 생성된 데이터를 실시간으로 저장하고 분석해 통신하는 기능이 핵심 역량으로 부각되고 있음을 말한다. 이러한 흐름은 의료데이터의 양적 증가, 정보의 민감도와 복잡성이 심화되고 있음을 보여준다. 더불어 소프트웨어 기반

체계는 네트워크, 클라우드, 외부 분석 플랫폼 등 다양한 정보기술 환경과 연결될 수 있어 진단의 정밀성과 효율성을 높이는 동시에 이에 상응하는 수준의 의료데이터 사이버보안 확보가 필요함을 보여준다.

나. 체외진단 분야에서의 사이버 보안 필요성

의료 산업 분야는 정보통신기술(ICT)의 발달에 따라 유·무선 통신 기반 의료기기, 디지털 헬스케어 서비스, 원격 진료 등 다양한 디지털 의료 환경으로 빠르게 전환되고 있다. 이러한 변화는 의료 서비스의 효율성과 접근성을 향상시켰으며, 특히 체외진단(In Vitro Diagnostic, IVD) 분야에서도 중요한 영향을 미치고 있다. 체외진단은 유전자 검사, 혈당 측정, 감염병 진단 등 질병의 조기 발견과 예측에 필수적인 기술로, 의료 패러다임이 치료 중심에서 예방 중심으로 이동하는 과정에서 중심적 역할을 하고 있다.

최근 웨어러블 기기, 사물인터넷(IoT), 현장진단기기(POCT), 유전자 예측 기기 등의 발전으로 체외진단의 범위가 확대되고 있으며, 이로 인해 의료 현장에서 생성되는 데이터의 양도 증가하고 있다. 그러나, 대부분의 체외진단 장비 및 관련 네트워크는 와이파이(Wi-Fi), 블루투스(Bluetooth) 등 무선 통신 기술에 기반하고 있어 외부 공격에 상대적으로 취약한 구조를 가지고 있다. 디지털 진단 기술의 확산은 진단의 정밀도와 효율성을 높이는 데 기여하고 있으나, 동시에 민감한 의료데이터에 대한 보안 위협도 함께 증대되고 있다. Secureframe 에서 발표한 2003 년부터 2023 년까지 산업별 데이터 유출 건수를 살펴보면, 의료 분야에서 데이터 침해 사례의 증가 폭이 큰 산업으로 나타났다.[8]

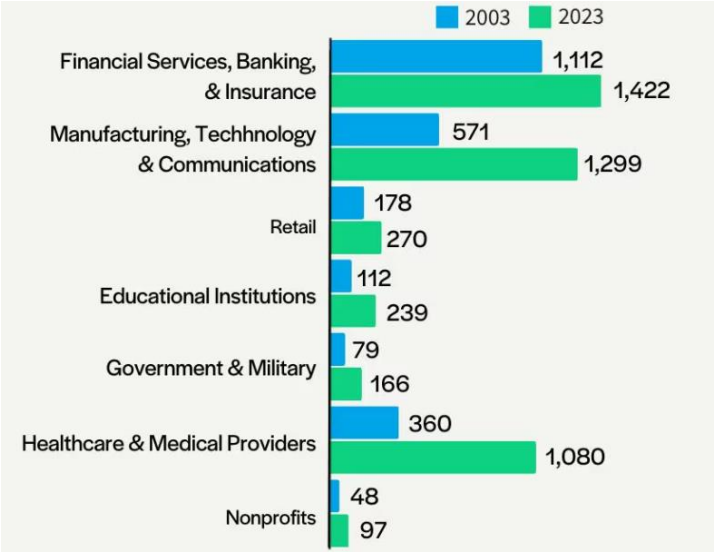


그림 4 산업별 데이터 침해 건 수(2003-2023)

(출처: Privacy Rights Clearinghouse, 2023)[8]

진단 기술 발전과 디지털 진단 환경 확산으로 체외진단 분야의 시장 규모는 지속적으로 성장하고 있다. 그러나 이와 동시에 디지털 환경에서 생성되는 의료데이터의 양이 급증함에 따라, 데이터 침해 사례 또한 증가하고 있어 산업의 성장과 더불어 사이버 위협에 노출되는 빈도도 높아지고 있다.

현재 의료 현장에서는 인슐린 펌프, 혈당 측정기, 유전자 검사 장비 등 다양한 장비들이 환자의 생체 정보를 수집하고, 이를 네트워크를 통해 전송 및 저장하고 있다. 이러한 데이터가 변조되거나 유출될 경우, 환자 프라이버시 침해는 물론, 잘못된 진단과 치료로 이어질 수 있는 심각한 문제를 초래할 수 있다. 특히 체외진단 장비는 진단의 정확도와 신속성이 중요한 만큼, 데이터 무결성이 보장되지 않을 경우 진단의 신뢰성에 중대한 영향을 미칠 수 있다.

표 4 체외진단 의료기기 사이버보안 필요성

구분	사이버 보안 필요성
1	환자 안전 보장
2	민감한 의료 정보 보호
3	의료기관 운영 연속성 확보
4	규제 준수
5	기관 신뢰도 유지

특히 체외진단 분야에서 발생하는 의료데이터는 단순한 개인 정보 수준을 넘어 질병 유무나 유전자 정보와 같이 매우 높은 민감성을 가진다. 이러한 특성으로 인해 보다 체계적인 보안 체계가 요구된다. 국내에서는 의료기기 사이버보안 규제 도입 초기에는 개인 의료정보를 송수신하거나 원격으로 기기를 제어하는 경우에 한해 보안 적용이 이루어졌으나, 현재는 통신 기능이 탑재된 모든 의료기기로 사이버보안 적용 범위가 확대되고 있다. 또한 국제 의료기기 규제 포럼(International Medical Device Regulators Forum, IMDRF)에서 요구하는 국제적 사이버보안 기준을 도입하여 글로벌 수준의 보안 체계를 확보했다.

미국 식품의약국(FDA)은 의료기기 보안의 중요성을 강조하며, 설계 단계에서부터 사이버보안을 고려하도록 요구하고 있다. 환자 안전, 개인정보 보호, 의료기기 신뢰성 유지를 위해 시판 전 단계와 시판 후 단계를 모두 포함한 의료기기 전주기 수명 전반에 걸쳐 사이버보안 해결을 위한 명확한 지침을 발표했다. 유럽연합(EU)의 의료기기 규정(MDR/IVDR) 역시 이와 유사한 방향으로 보안 요구 사항을 강화하고 있다.

주요국에서 의료기기 사이버보안에 대한 인식과 규제는 점차 강화되고 있음에도 불구하고, 의료데이터 자체에 대한 보안 인식은 상대적으로 부족한 실정이다. 특히 체외진단 분야는 커넥티드 진단 장치의 발전으로 임상적 유용성과 운영 효율성이 높아지고 있으나, 동시에 사이버 보안 취약점도 증가하고 있어, 실질적 적용 가능성을 고려한 종합적 보안 전략 수립이 요구된다.

표 5 사이버 보안이 필요한 의료기기

의료기기 품목	예시
네트워크 연결 기기	유전자 검사 장비, 혈당 측정기, 감염병 진단 장비
고위험 분류 기기	HIV 진단 키트, 혈액 선별 검사 장비, 암 진단 기기
소프트웨어 기반 기기	독립형 소프트웨어 의료기기(SaMD), 내장형 소프트웨어 의료기기(SiMD), 의료영상 분석 소프트웨어, 진단 알고리즘 기반 소프트웨어
환자 모니터링 기기	환자 생체신호 모니터, 심장박동기, 제세동기
의료데이터 관련 기기	전자 건강 기록 시스템과 연동되는 진단 기기, 환자 식별 정보 저장 기기, 유·무선 통신으로 환자 정보를 송수신/제어 가능한 의료기기, 원격 업데이트 가능한 기기

다. 체외진단 의료데이터 보안 현황과 규제

현재 의료데이터는 관리 주체 및 활용 환경에 유전체 정보, 개인건강정보(Personal Health Record, PHR), 전자의무기록(Electronic Medical Record, EMR), 국민건강정보로 구분된다. 이 중 전자의무기록(EMR)과 국민건강정보는 병원과 정부기관 중심의 관리가 이루어지고 있지만, 유전체 염기쌍 서열인 유전체 정보는 과거에 병원에서만 다뤄지는 의료정보였으나 민간 유전자 분석 기업에서 수집되는 경우도 있으며, IoT 기반의 헬스 디바이스 및 모바일 앱에서도 의료데이터가 생성 및 관리되고 있다. 특히 웨어러블 기기나 모바일 기반 진단 도구에서 발생하는 데이터는 의료기관 외부에서도 수집·이용되며, 병원과의 연계성을 바탕으로 의료정보 체계에 통합되어 활용되고 있다.

하지만 이러한 환경 변화에 비해 의료데이터 보안을 위한 법적·제도적 규제는 불균형한 상황이다. 미국의 경우 건강 정보의 프라이버시를 규제하려는 최초의 시도로 1974 년의 개인정보 보호법(Privacy Act)이 있지만, 의료제공자들에게 영향을 주지 않았다. 이후 1996 년 Health Insurance Portability and Accountability Act(HIPAA)가 제정되어 개인 정보 보호 및 보안 규정이 포함되었다. HIPAA 는 의료 프라이버시와 관련해 가장 중요한 법률로, 의료기관이 환자 데이터를 처리하고 공유하는 방식과 기준을 만들어 기밀성을 보장하고자 했지만, 유전자정보 데이터베이스나 웨어러블 기기와 같은 새로운 기술은 HIPPA 에서 다루지 않았다. 이에 따라 데이터 프라이버시에 대한 새로운 위험을 초래하고 있어 정보가 침해, 공유 또는 제 3 자에게 판매될 수 있는 상황에 노출되기 쉽다.[9]

최근 백악관은 미국 보건복지부(The Department of Health and Human Services, HHS)가 제안한 HIPAA 보안 규칙 개정을 승인했으며, 이는 약 10 년 넘게 이루어지지 않았던 HIPAA 보안 규칙의 첫 대규모 개정이다.[10] 2025 년 1 월, 미국 보건복지부 산하 민권국(Office for Civil Rights, OCR)은 기존 HIPAA 보안 규칙을 개정하는 내용인 규칙 제정 예고안(Notice of Proposed Rule Making, NPRM)을 발표했다. 이 예고안은 사이버 보안 강화를 목적으로, 위험 식별 및 대응역량에 중점을 두는 내용을 포함한다. 주요 제안 사항으로는 모바일 기기, 태블릿 등 휴대용 장치에 기술적 보호 조치를 적용하고, 전자 건강 정보(electronic PHI, ePHI)는 저장과 전송 시 모두 암호화, 다중 인증(MFA) 필수 도입, 해커가 시스템 내에서 이동하는 것(Lateral movement)을 막기 위한 네트워크 세분화, 악성코드 방지 소프트웨어 설치 등이 포함된다.[11]

한편, 2024 년, 미국 의원들이 의료데이터 관련 두 가지 법안인 의료 사이버 보안법(the Healthcare Cybersecurity Act of 2024)과 의료 인프라 보안 및 책임법(the Health Infrastructure Security and Accountability Act of 2024, HISAA)을 발의했지만 아직 법으로 제정되지 않은 상태이다.[12]

PIPEDA 는 캐나다의 민간 부문에 중점, 정보의 민감성에 따라 적용되고, GDPR 은 유럽 연합 내 개인 데이터를 처리하는 모든 조직에 적용된다. 미국의 HIPAA, 캐나다의 PIPEDA, 유럽연합의 GDPR, 일본의 APPI 등 각국의 개인정보

보호법에서 의료정보를 포함하고 있지만, 의료기기에서 생성되는 데이터에 대한 기술적 보안 기준이나 민감도 기반 분류 체계가 미비하다. [표 6]와 같이 개인정보에 관한 규제는 있으나 의료기기 사이버 보안의 법률, 규제처럼 의료데이터의 민감도나 위험도에 따라 지정되지 않았다.

표 6 국가별 개인정보 보호 규정

국가	규정	내용
미국	HIPAA (Health Insurance Portability and Accountability Act)	– 1996 년, Health Insurance Portability and Accountability Act(HIPAA) 제정 – 의료, 데이터의 개인정보 보호와 보안 규정, 보호된 건강정보(PHI)를 다루는 방법에 대한 표준을 설정
	HISSA (Health Infrastructure Security and Accountability Act)[13]	– 2024 년 발의 – 모든 HIPAA 대상 기업 및 비즈니스 협회에 대해 최소한의 보안 요구사항 설정 규정 요구(매년 사이버 보안 위험 평가 실시)
	CHIPPA (Consumer Health Information Privacy Protection Act) [14]	– 워싱턴 DC(Washington, DC), 2024 년 CHIPPA 도입 – HIPAA 의 적용을 받지 않는 건강 데이터의 보호를 개선하기 위해 도입됨 – 소비자 건강 데이터의 수집, 공유, 사용 또는 판매에 관한 강화된 개인정보 보호 규정을 준수하도록 요구 및 강화된 개인정보 보호 정책 수립
캐나다	PIPEDA	– 2000 년, 캐나다 연방 개인정보 보호법으로 제정

	(Personal Information Protection and Electronic Documents Act)[15]	– 10 가지 원칙으로 민간 부문에서 개인정보를 수집, 사용, 공개하는 데 있어 기준 제시
	PHIPA (Personal Health Information Protection Act)[16]	– 온타리오 주에서 의료 정보를 위한 법률 – 의료정보 수집, 사용, 공개에 대한 규정을 설정
유럽연합 (EU)	GDPR (General Data Protection Regulation)[17]	– 2016 년 4 월, 개인 데이터 보호 규정(의료데이터도 포함) 제정, 2018 년 5 월 시행 – 개인정보 보호 조치 개선, 데이터 유출에 관해 조직의 책임을 강화하도록 함.[18]
영국	DPA 2018 (Data Protection Act 2018)[19]	– EU 의 GDPR 을 기반으로 영국 내 데이터 보호, 개인 정보 관리 규정 – 개인 데이터의 수집, 저장, 처리, 공유에 대한 명확한 기준을 제시 – 민감한 데이터 별도 분류, 더 높은 수준의 보호 요구
한국	개인정보 보호법[20]	– 개인정보 보호 규정
일본	APPI (Act on the Protection of Personal Information)[21]	– 아시아 최초의 데이터 보호 규정 중 하나로 2003 년 5 월 30 일 공포 – 일본의 기본적인 개인정보 보호법

체외진단 분야는 인공지능(AI), 머신러닝 등 고도화된 분석 기술이 도입되면서 방대한 양의 정밀 의료데이터가 수집·활용되고 있다. 이는 의료의 정확성과 개인 맞춤형 치료에 기여하는 긍정적인 효과를 가져오지만, 동시에 의료기기와 의료기관 간 데이터 송수신 과정에서의 노출 위험, 클라우드 및 네트워크 기반의

해킹 · 침해 가능성 등 다양한 보안 위협을 증가시킨다. 의료 사물인터넷(Internet of Medical Things, IoMT)을 기반으로 환자 모니터링, 원격 진단, 치료 지원이 가능해지는 환경에서 기술적 진보와 함께 사이버 보안 리스크에 대한 체계적인 대응이 요구된다. 따라서 체외진단 의료데이터의 민감도와 활용 환경을 종합적으로 고려한 데이터 등급 분류 체계와 각 등급에 적합한 차등 보안 전략의 수립이 필요한 시점이다. 이는 단순한 법적 규제 준수를 넘어, 디지털 헬스케어의 신뢰성과 지속 가능성을 확보하고 환자의 권리를 보호하기 위한 중요한 의의를 지닌다.

본 연구는 의료데이터를 고위험, 중위험, 저위험으로 분류하고, 각 등급별 특성에 부합하는 보안 방법을 제안함으로써, 체외진단 분야에서 실질적이고 실행 가능한 보안 체계 구축의 방향을 제안하고자 한다.

2. 연구 목적

본 연구의 목적은 급속히 성장하고 있는 체외진단(In Vitro Diagnostics, IVD) 분야에서 발생하는 의료데이터 보안 위협에 체계적으로 대응하기 위한 분류 및 보안 대응 방안을 제시하는 데 있다. 최근 체외진단 기술은 인공지능 기반의 분석, 원격 진료, 사물인터넷(IoT) 연동 진단기기 등 기술 융합을 통해 진단의 정확성과 효율성을 향상시키고 있다. 이에 따라 다양한 형태의 의료데이터의 생성과 활용 범위가 증가하고 있다. 그러나 이러한 연결성과 디지털화는 편의성과 효율성을 높이는 동시에 사이버 위협 노출이라는 문제를 야기할 수 있다.

의료데이터는 일반 산업 데이터에 비해 개인 식별 가능성이 높고 민감한 정보를 포함하고 있어, 데이터 유출, 위·변조, 악성코드 감염 등의 위협 발생 시 환자의 생명과 건강은 물론 사생활 침해, 사회적 신뢰에까지 중대한 영향을 미칠 수 있다. 이는 의료 서비스에 대한 신뢰 저하와 사회적 혼란을 초래할 위험이 크다.

이에 본 연구는 체외진단 의료기기에서 수집·전송·저장되는 의료데이터의 특성과 발생할 수 있는 사이버 위협 요소, 침해 사례를 확인한다. 데이터의 민감도와 위협 발생 시 위험도에 따라 유형별 위험 등급(고위험, 중위험, 저위험)을 분류하고, 각 위험 등급에 적합한 보호 방안을 제시하여 의료의 신뢰성과 데이터 보안 방안에 기여하고자 한다.

II. 연구범위 및 방법

1. 연구 범위

본 연구는 체외진단 분야에서 생성되는 의료데이터의 사이버 보안 현황과 사례를 중심으로 다룬다. 연구 대상은 체외진단 의료기기에서 발생하는 의료데이터의 생성, 전송, 저장 과정 전반에 걸친 보안 취약점과 위협 요소를 포함하며, 관련 규제 및 정책, 기술적 보안 대책을 조사한다.

미국의 HIPAA, 유럽연합의 GDPR 등 주요 국가별 의료데이터 보호 규제를 검토해 현재 적용되고 있는 보호 조치와 규제 준수 현황을 확인한다. 또한, 정보보호학회지, 국내외 사이버보안 관련 논문 및 자료, 산업 보고서, 최신 기사 등 사례를 검토하여 체외진단 의료데이터와 관련된 사이버 침해 사례를 분석하고, 의료 및 금융 산업을 포함한 여러 산업에서 데이터 보호를 위한 보안 기술을 확인한다.

의료데이터의 특성과 민감도, 위험도에 기반해 고위험, 중위험, 저위험으로 분류하고 각 등급별 필요한 보안 기술을 고찰한다. 이를 통해 효과적인 사이버 보안 전략 수립 방향을 제시하는 데 목적이 있다.

2. 연구 방법

본 연구는 자료 조사를 통해 체외진단 의료기기로부터 생성되는 의료데이터가 직면한 사이버 보안 현황을 확인하고, 의료데이터를 민감도와 위험도에 따른 분류 체계(저위험, 중위험, 고위험)를 수립하여 각 등급에 적합한 보안 방안을 제시하는 것을 목적으로 한다.

이를 위해 국내외 주요 공공기관 및 민간 연구기관에서 발간한 산업 보고서, 기술 문서, 학술 자료를 기반으로 체외진단 시장과 데이터 보안 현황을 조사한다.

특히, 한국보건산업진흥원, 식품의약품안전처 등 국내 기관의 자료뿐만 아니라, 미국 HIPAA, 유럽연합의 GDPR 등 국가별 보호 규제를 비교·분석한다.

체외진단 기술의 특성과 검사 방식에 따라 생성되는 의료데이터의 민감도와 위험도에 따라 분류하고, 국내외 사이버 위협 사례를 통해 데이터가 노출되는 경로 및 유형별 위협을 분석한다. 해킹, 정보 유출, 시스템 침해 등 구체적인 침해 사례를 통해 보안 취약성을 파악한다.

다중 인증(Multi-Factor Authentication, MFA), 역할 기반 접근 제어(Role-Based Access Control, RBAC), 데이터 암호화, 네트워크 분리(Network Segmentation) 등 다양한 산업 분야에서 활용되는 정보보안 기술 적용 가능성을 검토한다. 이러한 분석을 바탕으로 체외진단 의료데이터 보호를 위한 효과적인 보호 방안을 제시하고자 한다.

III. 결과

1. 체외진단 의료기기 및 의료데이터 특성

가. 체외진단 의료기기 정의

『체외진단의료기기법』 제 2 조(정의)에 따르면, 체외진단의료기의 정의는 다음과 같다. “체외진단의료기기”란 사람이나 동물로부터 유래하는 검체를 체외에서 검사하기 위하여 단독 또는 조합하여 사용되는 시약, 대조·보정 물질, 기구·기계·장치, 소프트웨어 등 『의료기기법』 제 2 조 제 1 항에 따른 의료기기로서 해당하는 제품을 말한다.

생리학적 또는 병리학적 상태를 진단할 목적으로 사용되는 제품, 질병의 소인을 판단하거나 질병의 예후를 관찰하기 위한 목적으로 사용되는 제품, 혈액, 조직 등을 다른 사람에게 수혈하거나 이식하고자 할 때 안전성 및 적합성 판단에 필요한 정보 제공을 목적으로 하는 제품, 치료 반응 및 치료 결과를 예측하기 위한 목적으로 사용되는 제품, 치료 방법을 결정하거나 치료 효과 또는 부작용을 모니터링하기 위한 목적으로 사용되는 제품을 말한다.[22]

나. 체외진단 의료기기 분류

체외진단의료기기는 『체외진단의료기기 품목 및 품목별 등급에 대한 규정』에 따라 4 등급(1~4 등급)으로 분류된다. 이 등급은 개인과 공중보건에 미치는 잠재적 위해성, 사회적 영향력 및 파급 효과를 고려하여 분류된다. [23]

표 7 등급별 체외진단의료기기

등급	잠재적 위험성	품목 예시
1 등급	개인과 공중보건에 미치는 잠재적 위해성이 낮은 경우	핵산추출시약,혈당측정기, 세포및조직병리검사장치 등
2 등급	개인에게 중증도의 잠재적 위해성, 공중보건에 미치는 잠재적 위해성이 낮은 경우	요화학검사시약, 당뇨질환관련검사시약, 질환진단검사소프트웨어 등
3 등급	개인에게 고도의 잠재적 위해성, 공중보건에 중증도의 잠재적 위해성	개인용혈당검사지, 개인용임신내분비물검사지, 혈액응고검사시약, 개인용혈당측정기 등
4 등급	개인과 공중보건에 미치는 잠재적 위해성이 높은 경우	ABO·RhD 혈액형면역검사시약, HIV·HBV·HCV·HTLV 유전자검사시약 등

(출처: 한국의료기기산업협회 의료기기광고심의위원회, 심의대상)

국내를 포함한 주요 국가들은 의료기기를 사용 목적과 위해성에 따라 등급별로 분류하고 있으며, 그에 따라 규제와 안전관리 체계를 운영하고 있다. 미국은 의료기기를 위해성 및 관리로 3 개 등급(1 등급, 2 등급, 3 등급)으로, 유럽연합(EU)은 사용 목적과 위해성에 따라 4 개 등급(I등급, IIa 등급, IIb 등급, III등급)으로 분류, 일본은 3 개 등급(고도관리 의료기기, 관리 의료기기, 일반 의료기기)으로 분류되어 있다.[24]

의료기기의 경우, 현재 국내에서는 의료기기산업의 활성화 및 국제환경변화에 부합하는 의료기기 관리체제를 구축하기 위해 2004 년부터 별도로 『의료기기법』을 제정·시행하여 독립적인 규제 체계를 갖추게 되었고, [25] 체외진단 의료기기 시장의 확대에 발맞춰 2020 년 5 월부터는 별도로 『체외진단의료기기법』을 시행하고 있다. 의료기기는 사용 목적과 위해성을

기준으로 등급을 나누어 체계적으로 관리되고 있으나, 의료데이터의 경우 민감성, 활용 범위, 잠재적 위해성 등에 따라 등급별로 보호하거나 차등 관리하는 제도는 국내외적으로 명확히 마련되어 있지 않다. 정밀의료, AI 기반 진단기술, 원격의료 등 데이터 중심의 의료 환경이 고도화되고 있는 시점에서, 의료기기와 마찬가지로 의료데이터 또한 위험 기반의 등급 분류 체계를 마련해 체계적인 보호 관리가 필요성이 크다.

한편, 체외진단 기술의 활용 범위가 넓어지면서 최종사용자 관점에서도 시장이 세분화되고 있다. 특히 [그림 5]에서 독립형 실험실이 2019년 대비 2027년까지 연평균 3.9%의 성장률이 예상되는 등 의료기관 외에서 의료데이터가 생성·관리되고 진단검사 수요 증가와 더불어 의료데이터 생성 환경도 빠르게 확대되고 있다. 이러한 시장 확대는 정밀의료와 맞춤형 진단의 중요성, 편리성이 높아지는 동시에 의료데이터 보호와 안전한 관리의 필요성을 더욱 부각시키고 있다.

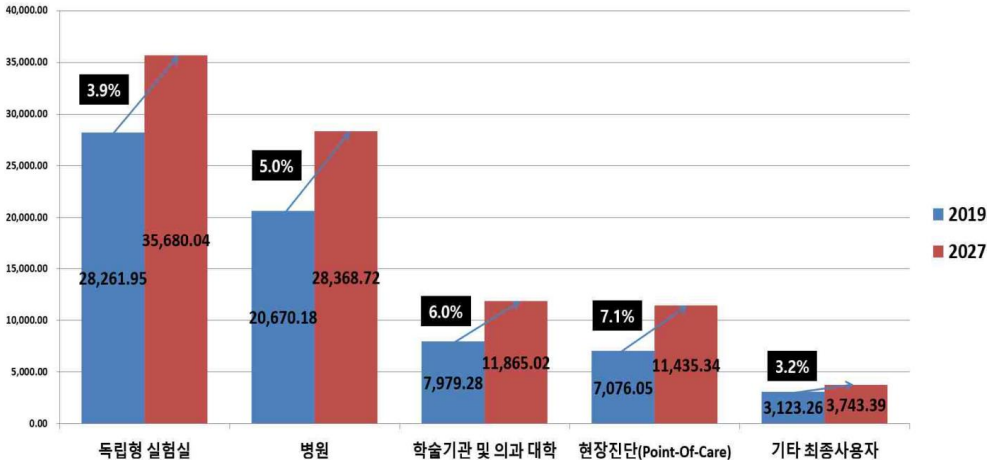


그림 5 글로벌 체외진단 시장의 최종사용자별 시장 규모 및 전망

(단위: 백만 달러)

(출처: Allied Market Research, 『Global In-Vitro Diagnostics Market, 2021』, 연구개발특구진흥재단, 『유망시장 Issue Report : 체외진단, 2021』)

다. 의료데이터

체외진단 의료기기의 기술 고도화와 보급 확산은 의료 현장에서 다양한 유형의 의료데이터가 빠르게 축적되고 활용되는 환경을 만들고 있으며, 이에 따라 해당 데이터의 보호와 관리 체계에 대한 중요성이 더욱 부각되고 있다.

국가법령정보센터에서 확인한 『보건의료기본법』 제 3 조(정의)에 따르면 "보건의료"란 국민의 건강을 보호·증진하기 위하여 국가, 지방자치단체, 보건의료기관 또는 보건의료인 등이 행하는 모든 활동을 말하며, "보건의료정보"는 보건의료와 관련한 지식 또는 부호, 숫자, 문자, 음성, 음향, 영상 등으로 표현된 모든 종류의 자료를 말한다.[26] 이러한 보건의료정보는 다양한 형태로 구성되며, 일반적인 개인정보와는 구별되는 특성을 가진다. 미국의 경우, 1974 년 개인정보 보호법(Privacy Act) 이후 HIPAA(Health Insurance Portability and Accountability Act)가 제정되어 개인식별정보(Personally Identifiable Information, PII))와 보호 대상 건강 정보(Protected Health Information, PHI)가 구분되었다.

표 8 HIPAA 에서 개인식별정보(PII), 의료정보(PHI) 구분

구분	PII	PHI
적용범위	개인을 식별할 수 있는 모든 정보	개인을 식별할 수 있는 건강 및 의료 관련 정보
관련 법률	일반 개인정보 보호법(PII 에 대한 규제)	HIPAA 규정에 따라 보호
포함 항목 예시	이름, 주소, 주민등록번호 등	의료 기록 번호, 검사 결과, 보험 청구 정보 등
익명화 여부	익명화되지 않은 모든 개인 정보	익명화되지 않은 건강 및 의료데이터

(출처: HIPAA Secure Now, 『PHI or PHI? What's the Difference?』)[27]

현행 개인정보 보호법은 의료데이터도 보호 대상으로 포함하고 있으나, 건강정보 특유의 민감성과 잠재적 위해성을 고려할 때 보다 정교한 보호 체계가 요구된다. 의료데이터는 사람으로부터 생성되는 데이터로 환자의 진료, 처방 정보로부터 개인이 일상생활에서 생성하거나 유전적으로 확보되는 정보까지 다양한 범위를 포함해 분석이나 식별화 조치가 어려운 특징이 있다.

표 9 의료데이터의 종류

구분	설명
개인유전정보	1 인당 약 30 억 개의 유전자 염기서열 정보 존재
개인건강정보	수면패턴 등 스마트폰 앱 또는 IoT 디바이스로 수집되는 Life-log
전자의무기록	의료기관에서 관리하며 환자의 모든 진료정보를 전산화하여 입력, 저장, 관리하는 형태(진단정보, 처방자료, 처방결과 등)
국민건강정보 (공공의료데이터)	공공기관에서 관리하며 자격 및 보험료, 진료내역, 건강검진 결과, 의료급여 등

(출처: 보험연구원, 『연구보고서 2022-10 중 III 의료데이터의 이차적 활용』)

의료데이터는 개인의 정보이기 때문에 데이터 유출 시 사회적 불이익, 불합리한 차별 등으로 피해 규모가 매우 크다. 이 의료데이터의 개념 및 활용가능 범위는 [표 10]과 같다.

표 10 개인정보, 가명정보, 익명정보의 개념 및 활용 가능 범위

구분	개념	활용 가능 범위
개인정보	특정 개인에 대한 정보 혹은 개인을 알아볼 수 있게 하는 정보	사전에 구체적인 동의를 받은 범위 내에서 활용 가능

가명정보	추가정보 없이는 특정 개인을 알아볼 수 없도록 처리한 정보	통계작성, 과학적 연구, 공익적 기록보존 목적에 있어서는 동의 없이 활용 가능
익명정보	더 이상 개인을 알아볼 수 없는 정보	개인정보가 아니기 때문에 제한 없이 자유롭게 활용 가능

(출처: 보험연구원, 『연구보고서 2022-10 중 III 의료데이터의 이차적 활용』)

현재 전 세계적으로 의료데이터의 대용량 전산화가 활발히 진행되고 있다. 각 의료기관에 정보시스템 도입됨으로써 정보를 데이터베이스에 보관해 전자의무기록(EMR)이 가능하다. 독립적으로 관리된 EMR 은 다른 의료기관과 공동으로 활용할 수 있는 EHR 로 발전했다. 의료기관이 정보시스템을 도입함으로써 다양한 의료정보시스템이 존재한다.

표 11 의료정보시스템 종류

구분	내용
병원정보시스템 (Hospital Information System, HIS)	– 병원의 전반적인 관리 업무를 전산 시스템으로 자동화한 시스템, 병원의 인사 관리 및 급여 관리, 환자의 외래와 입·퇴원관리, 의료 수가 관리, 급식 관리 – 병원의 시설 및 의료 장비 관리 등 병원의 종사자를 위한 시스템
전자의무기록 (Electronic Medica Record, EMR)	– 의료인이나 의료기관 개설자가 진료기록부 등을 전자서명법에 따른 전자서명이 기재된 전자문서
처방전달시스템	– 의료기관에서 컴퓨터망을 통해 의사의 처방을 각종 진료 지원부에 전달, 처방 내역을 컴퓨터에

(Ordering Communication System, OCS)	저장해 환자 진단 시에 조회할 수 있는 의료정보시스템
임상정보시스템 (Laboratory Information System, LIS)[28]	– 진단검사의학과의 진단검사처방부터 검체 획득, 검체 접수, 검사 결과 입력까지 모든 과정이 전산화 되어 운영

(출처: 보건복지부, 한국사회보장정보원, 『의료분야 랜섬웨어 예방·대응 안내서 2020.7』)

의료기록의 전산화 및 정보화, 의료기기의 발달로 대용량의 의료데이터가 생성되고 보관되면서 의료데이터 시스템은 AI, 원격의료, 의료사물인터넷(IoMT), 전자의무기록(EMR) 시스템 등 첨단 기술의 융합으로 빠르게 발전하고 있다. 의료 서비스 품질, 효율성을 높이고 환자 중심의 맞춤형 치료를 가능하게 하지만, 의료데이터에 대한 접근성, 효율성, 편의성이 높아질수록 데이터 노출에 대한 위험도 커진다. 최근 의료기관, 의료데이터 서비스 업체 등 다양한 곳에서 랜섬웨어 공격, 바이러스 감염, 해킹 등 사이버 침해 사례가 늘고 있다. 의료데이터 유출의 위험성을 확인하고 예방 및 대응 방안을 통해 보호하는 것이 필수적이다.

2. 의료데이터 사이버보안 환경과 규제 현황

가. 의료데이터 사이버보안 위협 및 공격 유형

의료 산업의 디지털화는 클라우드 저장, 원격진료, 인공지능 진단 등 효율성을 높이는 기술 발전을 가져왔지만, 사이버 보안 측면에서 새로운 위협 요소도 함께 증가하고 있다. 병원, 연구소, 보험사 등 다양한 기관 간 네트워크 환경이 확산되면서 개인건강정보(PHI)를 포함한 민감한 의료데이터가 사이버 공격에 노출되고 있다.

2016 년 1 월부터 2021 년 12 월까지 미국 내 의료기관을 대상으로 한 코호트 연구(Cohort Study)에 따르면, 374 건의 랜섬웨어 공격으로 약 4,200 만 명의 환자 개인건강 정보(PHI)가 유출되었으며, 연간 랜섬웨어 공격 건수는 43 건에서 91 건으로 두 배 이상 증가한 것으로 보고되었다.[29] 의료데이터가 사이버 범죄에 주요 공격 대상이 되는 이유는 경제적 가치 때문이다. 의료정보는 신용카드 정보보다 암시장에서 더 높은 가격으로 거래되며, 이를 악용한 보험 사기, 도용, 불법 거래가 발생할 수 있다.

의료데이터 보호는 의료기관 내 정보 시스템뿐만 아니라, 해당 데이터를 수집·전송하는 장치의 보안과도 직결된다. 최근 네트워크 연결 기반 의료기기 사용이 보편화되면서, 의료기기 보안 취약점은 단순한 장비 문제를 넘어 환자 데이터의 유출, 변조, 접근 통제 실패 등으로 이어질 수 있다. 예를 들어, 체외진단 의료기기와 같은 장비는 병원정보시스템과 연동되며, 진단 결과를 전송하거나 외부에서 원격 제어되는 과정에서 데이터 무결성 손상이나 암호화 취약점에 따른 정보 가로채기, 인증 미비로 인한 무단 접근 등이 발생할 수 있다.

의료기기 보안을 포함한 다양한 경로를 통해 의료데이터가 유출될 수 있는 사이버 위협을 확인하고, 대표적인 사이버 공격 유형을 [표 12]에 정리한다.

표 12 10 가지 유형의 사이버 공격

사이버 공격 종류	내용
Phishing	– 이메일 등 대량 메시지를 통한 사이버 공격
Denial of Service (Dos)	– 시스템 사용 차단 목적 – 네트워크 과부화로 인해 응답 및 접근 불가능, 트래픽으로 네트워크 마비
Privilege escalation	– 권한 확대로 일반 로그인 계정을 관리 계정으로 변환
Man in the middle (MITM)	– 네트워크 연결 취약점을 악용해 통신 전송 중간에 정보 도청 및 수정 가능
Malware	– 일정 기간 동안 시스템 통제 – 컴퓨터나 장비에 심어진 승인되지 않은 소프트웨어로 소유자의 결정과 달리 시스템의 활동이나 성능 변경
Cryptographic	– 암호화 공격 – 환자 기록 수정, 삭제, 손상시킬 수 있음
Injections exploits	– 인터넷 서버, 데이터베이스 시스템에서 이루어짐 – 시스템의 취약성을 파악해 불안정하거나 접근할 수 없는 시스템 기능, 잠재적으로 노출된 데이터 생성
Spoofing	– 의료기기에 외부 신호를 수신하도록 시도해 데이터, 운영 설정, 기타 시스템 구성 요소에 접근하거나 조정할 수 있도록 하는 방법 – 휴대용 의료기기 해킹에 가장 많이 사용됨
Destructive software	– 파일 손상

Drone-specific	– 무인항공기(unmanned aerial vehicles, UAV)라고도 불리며 해커가 모든 시설의 네트워크에 접근할 수 있도록 가깝게 접근 가능 – MITM 공격의 일종

(출처: Front Digit Health,『Hospital cybersecurity risks and gaps: Review (for the non-cyber professional)』, 2022)

의료데이터 유출과 보안 위협은 다양한 사이버 공격 유형으로 나타난다. [표 12]에 정리된 대표적인 사이버 공격 중 피싱(Phishing)은 이메일 등을 통해 대량으로 전송되는 가장 흔한 공격으로, 2020 년 의료 사이버 사고의 57%를 차지했다. Phishing 은 환자의 개인 건강 정보(PHI)를 노출이나 해커가 의료 시스템에 접근할 수 있도록 하여, 의료기기 조작이, 데이터 변조, 악성 소프트웨어 설치를 유발한다. 이로 인해 의료 서비스 지연, 투약 오류, 오진 등의 심각한 위험이 발생할 수 있다. 중간자 공격(Man in the middle, MITM)은 민감한 환자 정보 유출 및 의료데이터 조작에 사용된다. 드론 기반 공격(Drone-specific)은 접근하기 어려운 위치에서도 병원 네트워크 해킹이 가능한 것으로 알려져 있으며. 사용자를 속여 병원 네트워크가 아닌 드론의 네트워크에 로그인하도록 유도하는 이블 트윈(evil twin) 공격 방식을 사용한다. 사용자가 네트워크를 접속하기 위해 감염된 페이지에 로그인 정보를 입력하면, 이 과정에서 와이파이 피싱(wifi phishing)이 발생한다. 이러한 절차를 통해 의료 서비스 자격 증명이 해커에게 노출되고, 병원 네트워크에 접속하여 악성 소프트웨어 설치, 데이터 탈취, 암호화, 시스템 손상 등이 발생할 수 있다. 이 공격은 드론-중간자 공격(Drone-in-the-Middle, DITM)이라고 하며 MITM 공격의 일종이다. 악성 소프트웨어(Malware)는 일정 기간 동안 시스템을 통제해 데이터를 변경할 수 있는 위협을 발생시킬 수 있다.[30]

나. 의료데이터 유출 및 규제 현황

의료데이터는 민감성과 활용 가치가 높아 해킹, 랜섬웨어, 내부 유출 등 다양한 경로를 통해 지속적으로 침해되고 있다. HIPAA Journal 에 따르면, 2009 년부터 2023 년까지 의료데이터 유출은 5,887 건에 이르며 5 억 1,993 만 5,970 건의 의료기록이 노출되거나 무단으로 공개되었다. 이는 미국 인구의 1.5 배 이상의 수치로, 14 년간 증가하는 추세를 보였다. 특히 2023 년 한 해 동안 미국 보건복지부(Department of Health and Human Services) 산하 민권국(Office for Civil Rights)에 보고된 의료데이터 유출만 500 건 이상이었다.[31]

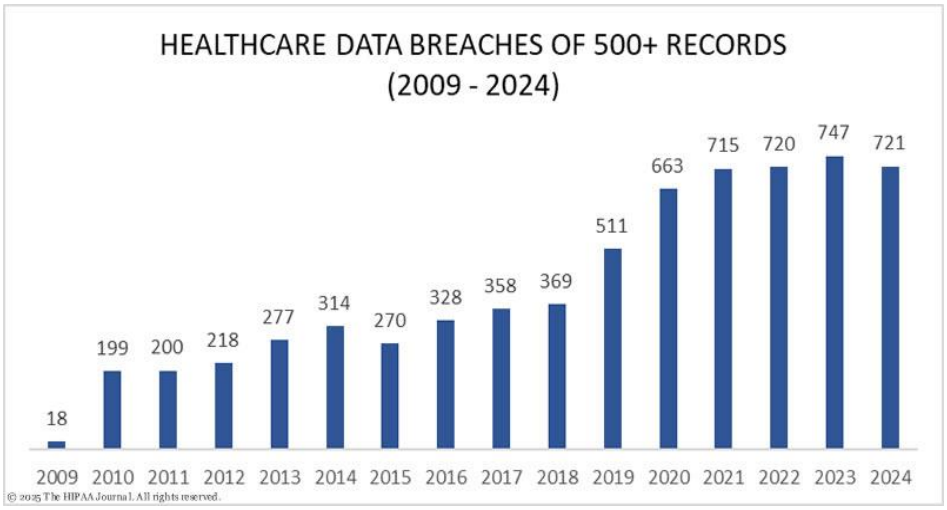


그림 6 OCR 에 보고된 의료데이터 유출 건수 (2009-2024)

(출처:THE HIPAA Journal,『THE HIPAA Journal, Healthcare Data Breach Statistics』, 2025)

매년 노출되는 기록수는 전반적으로 증가하는 추세를 보였다. 2024 년에는 2 억 7,677 만 5,457 명의 개인 건강 정보가 노출되거나 도난당한 것으로 보고되었다. 특히 2015 년은 세 번의 대규모 의료 보험 데이터 유출이 있었으며, 2015 년부터

2023 년까지 1 억 1,200 만 건 이상의 기록이 노출되거나 허가 없이 공개되어 의료 기록이 유출되었다.[31]

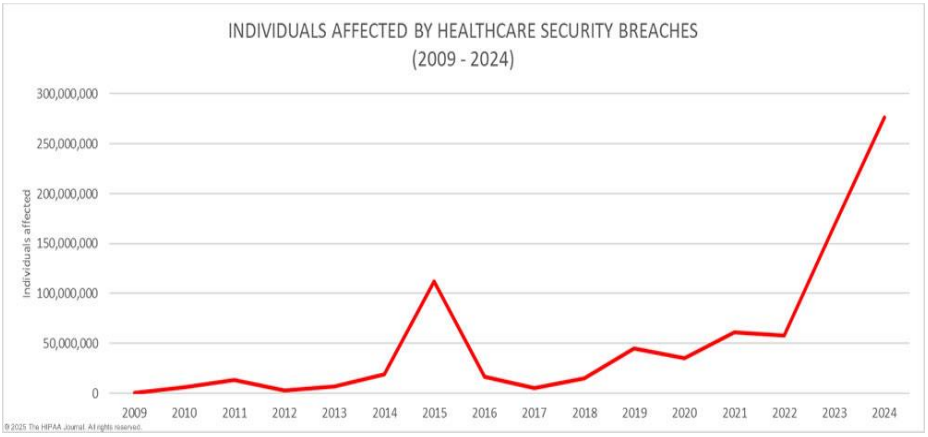


그림 7 의료데이터 유출된 개인의 수(2009−2024)

((출처:THE HIPAA Journal,『THE HIPAA Journal, Healthcare Data Breach Statistics』, 2025)

의료데이터 유출의 주요 원인으로 해킹이 지목되고 있다. 랜섬웨어 공격, Malware 등 외부 침입뿐만 아니라, 내부자의 부주의나 고의적 유출도 큰 비중을 차지한다. 의료데이터는 신용카드 정보보다 암시장에서 더 높은 가치를 가지며, 도난당한 정보가 장기간 악용될 수 있다는 점에서 그 중요성이 더욱 부각된다. 이에 따라 의료기관 및 의료기기 간 데이터 송수신 시 암호화, 이중 인증, 네트워크 접근 제어 등의 기술적 보호조치가 필수적이며, 데이터의 민감도 및 위험도에 따라 보안 수준을 차등화 하는 접근이 필요하다.

각국은 의료데이터 보호를 위한 법적·제도적 체계가 상이하다. 대표적으로 미국은 의료 정보 보호를 위한 연방법으로 1996 년 미국 의회에서 통과된 HIPAA 가 있다. 개인의 의료 정보를 열람할 수 있는 사람에 대한 규정, 전자 의료 정보에 대한 보안 통제, 개인정보 보호 관행의 의무화, 민감한 환자 건강 정보가 환자의 동의 없이 공개 금지 등을 규정하고 있다. HIPAA 규정 준수를

통해 사이버 위협 노출을 줄이고 잠재적인 데이터 침해 가능성을 줄이고 있으며, 증가하는 사이버 위협에 따라 2025 HIPAA 개정 사항이 있었다. 사이버 위협 증강에 대응한 ePHI 보호를 강화하며, 규제 준수에 의무를 두고 있다. 의료 기관, 관련 업체 및 기관에서 더욱 엄격한 보안 조치를 갖추고 환자의 데이터 관리에 존중하도록 요구하고 있다. 이런 규정을 준수하기 위해서 기술적, 운영적 준비가 필요해 보인다.

미국 연방거래위원회에서 Health Breach Notification Rule(HBN Rule)에서 침해의 정의 개정을 제안하고 헬스케어 앱까지도 규제 범위를 확대했다. HBN Rule 을 개정하고 있으며 HIPAA 가 적용되지 않은 개인 건강 기록(Personal Health Records, PHRs) 및 관련 기관, 건강 데이터 유출을 미디어에 통지하도록 했다. 디지털 헬스케어 기업들의 건강 정보 공유에 대한 제재가 들어가며 의료데이터 관련 규제 환경이 더욱 강화되고 있다.[32] 의료 기관 및 관련 기관은 PHI 를 더 잘 보호하고, 위반 위험을 줄이며, HIPAA, HBN Rule 등 규정을 따르는 것은 단순한 규제 의무에 준수하는 것뿐만 아니라 점점 더 디지털화되는 의료 환경에서 환자의 안전과 기밀을 보호하는데 필요하다.

표 13 각 국가별 의료데이터 보호 법률 및 규제

국가	법명	내용
미국	Health Insurance Portability and Accountability Act (HIPAA)	– 데이터의 기밀성, 무결성, 가용성 보호하기 위해 설계된 법률로 전자 건강 기록(ePHI)에 대한 보안 요구 사항 포함
유럽연합 (EU)	European Health Data Space Regulation (EHDS)[33]	– 2025 년 1 월 유럽연합 이사회에서 채택됨 – 개인의 건강 데이터에 대한 접근성과 통제성 강화

		– 유럽연합 회원국 간 건강 데이터의 원활한 교환 목표
중국	Network Data Security Management[34]	– 24 년 9 월 발표되어 2025 년 1 월 1 일부터 시행됨 – 개인정보 보호를 위한 규칙, 네트워크 데이터 처리 활동에 대한 명확한 지침 제공
캐나다	PHIPA (Personal Health Information Protection Act)[35]	– 온타리오 주에서 의료 정보를 위한 법률 – 의료정보 수집, 사용, 공개에 대한 규정을 설정

3. 체외진단 의료기기, 의료데이터 사이버 침해 사례

가. 사이버 보안 침해 사례

법적·제도적 대응에도 불구하고 의료데이터는 여전히 여러 경로를 통해 사이버 위협에 노출되고 있으며, 실제로 다수의 침해 사례가 보고되고 있다. 특히 체외진단 의료기기와 같이 네트워크 및 디지털 기반 기술을 활용하는 장치는 해킹, 악성코드 감염, 시스템 침투 등의 공격에 취약하다. 의료정보는 센서, 스마트기기, 의료정보시스템 등 다양한 접점에서 탈취될 수 있으며, 유출 시 환자 개인의 민감한 정보가 포함되어 대규모 피해로 이어질 수 있다. 이에 따라 의료데이터는 다른 분야의 정보보다 높은 수준의 보안이 요구된다.

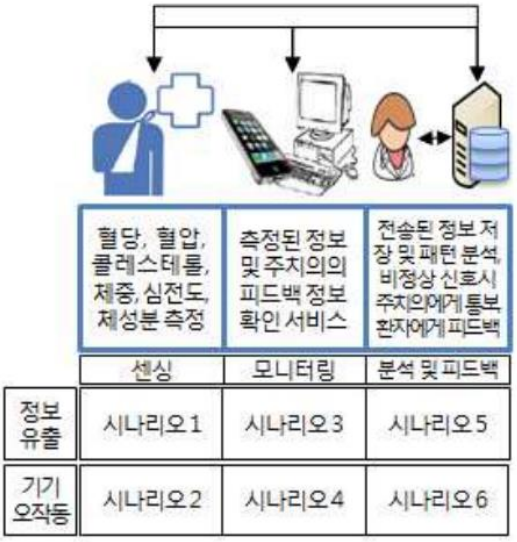


그림 8 헬스케어 시스템의 보안위협에 대한 분류[36]

(출처: 한국멀티미디어학회지,
『u-헬스케어(Healthcare) 환경에 따른 의료 정보 보안이슈』, 2015)

체외진단 의료기기는 병원뿐만 아니라 유전자 검사 기관, 연구소 등 다양한 기관에서 활용되며, 의료데이터를 자동으로 생성·처리하고 병원정보시스템과 연동되는 특성을 지닌다. 이에 체외진단 의료기기에 대한 사이버 보안 위협은 단순히 장비 기능의 장애를 넘어 의료데이터의 유출, 변경 또는 오용과 같은 심각한 문제로 확대될 수 있다. 의료기기 보안과 의료데이터 보호는 개별적인 대응이 아니라 통합적이고 포괄적인 관점에서 접근해야 하며, 관련 기관 전반에 걸친 보안 강화가 필수적이다. 다음 [표 14]는 체외진단 분야에서 발생한 주요 사이버 보안 침해 사례를 정리한 것이다.

표 14. 의료기기 사이버 보안 취약 및 사고사례[37]

사건	원인	내용
태아 모니터링 시스템 악성코드 감염	악성코드 감염	고위험 임신 여성을 위한 태아 모니터링 시스템이 악성코드 감염으로 환자 모니터링 방해
대학부속 병원 의료기기 바이러스 감염	의료기기 바이러스 감염	1000 건의 악성프로그램 발견된 의료 장비와 다른 종류의 기기로 바이러스 확산돼 진료 업무에 영향을 끼침
의료기기를 겨냥한 악성코드 발표	악성코드 감염	2013 년 6 월 FDA 에서 네트워크에 연결된 의료기기가 악성 코드에 감염된 사례 발표(환자의 정보 및 모니터링 시스템, 임플란트 장비에 무선으로 연결되는 모바일 기기)
네트워크 취약점을 통한 인터넷에서 의료기기 접근	네트워크 취약점	ICS-CERT Monthly Monitor (2012 년 8 월호)에서 의료기기 원격 모니터링에 대한 경고 발표, 실제 인터넷에서 접근할 수 있는 의료기기 발견
인슐린 펌프 해킹	해킹에 의한 인슐린 양 조절 가능성	2011 년, 당뇨병 환자의 인슐린 펌프에 무선 기능의 취약점을 이용해 투여되는 인슐린의 양을 외부에서 조작할 수 있는 것을 발표

(출처: 정보보호학회지, 『국외 의료기기 보안위협 사례 및 보안 동향 조사』,2015)

또한, 체외진단 장비에 포함된 특정 DNA 염기서열 분석 소프트웨어에서 보안 취약점이 발견된 사례도 있다. 미국 FDA 는 해당 기기의 소프트웨어에서 사이버 보안 취약점으로 인해 유전체 데이터 결과가 변경될 가능성이 있다고 경고하였다. 이 사례는 체외진단 의료기기의 소프트웨어적 취약점이 의료데이터 무결성에 직접적인 위협이 될 수 있음을 보여준다.

의료기기의 사이버 보안 위협은 단순한 기기 장애를 넘어, 해당 기기가 생성·처리하는 데이터의 유출, 변조, 진단 오류 등으로 이어질 수 있다. 체외진단 장비는 환자의 민감 정보를 병원정보시스템과 연계하여 처리하므로, 보안 침해는 곧 환자 안전에 직결된다. 이에 따라 사이버 위협 사례는 단순한 사건으로 그치지 않으며, 의료기기 보안과 데이터 보안은 통합적으로 고려되어야 한다.

다음 [표 15]는 의료기관 및 관련 기관에서 발생한 의료데이터 유출 사례를 정리한 것이다.

표 15 사이버 침해로 인한 의료데이터 유출 사례

사건	침해 유형	발생 시기	내용
호주 민간 건강보험사 네트워크 해킹[38]	해킹	2022 년 7 월	민간 건강보험사의 네트워크가 공격 받아 고객 약 970만 명의 개인정보 및 의료데이터(이름, HIV 양성 반응 결과, 마약 치료 및 간염 등의 의료기록) 유출
유전자 분석 서비스 회사 계정 접근 시도[39]	해킹	2023 년 10 월	Credential Stuffing 공격으로 유출된 계정을 통해 DNA 관련 정보 접근 시도

헬스케어 소프트웨어 솔루션 회사 고객 데이터 유출[40]	해킹	2021 년 2 월	데이터 마이그레이션 중 고객 개인정보, 의료정보(HIV, 암, 유전 질환, 임신, 환자의 약물치료, 유전 데이터 등) 인터넷에 대규모 유출
인슐린 펌프 의료기기 제조업체 임상 데이터 유출[41]	피싱	2020 년 1 월	Phising 공격으로 권한이 없는 사용자가 직원 이메일 계정에 접근. 당뇨병 관련 임상 데이터 및 고객 연락처 정보 일부 유출
C형 간염 데이터 노출[42]	데이터 노출	2019 년 10 월	미국 필라델피아 공중보건부에서 약 23,000명의 C형 간염 환자 데이터 노출됨
유전자 검사 연구소 직원 계정 무단 접근[43]	무단 접근	2020 년 1 월	직원 계정에 무단 접근, 약 233,000명의 고객의 개인 건강 정보(의료 정보, 유전자 실험실 서비스 관련 내용, 사회보장번호) 노출됨
의료기관 직원 이메일 계정 무단 접근[44]	무단 접근	2024 년 11 월	알레르기, 천식, 면역 질환 치료 의료기관 직원 이메일 계정에 무단 접근, 데이터(이름, 사회보장번호, 보험 정보, 치료 관련 정보) 유출

해킹 공격이나 권한이 없는 사용자의 무단 접근으로 인해 의료기관 및 서비스 제공업체의 네트워크에서 유전정보, HIV 결과 노출시킨 사례가 발생하고 있다.

나. 의료데이터 유출 경로 및 규제·제도 대응 현황

HIPAA Journal 에 따르면, 의료정보 유출 경로 중 네트워크 서버를 통한 유출이 가장 높은 비중을 차지하며, 다음으로는 이메일 관련 유출이 따른다.

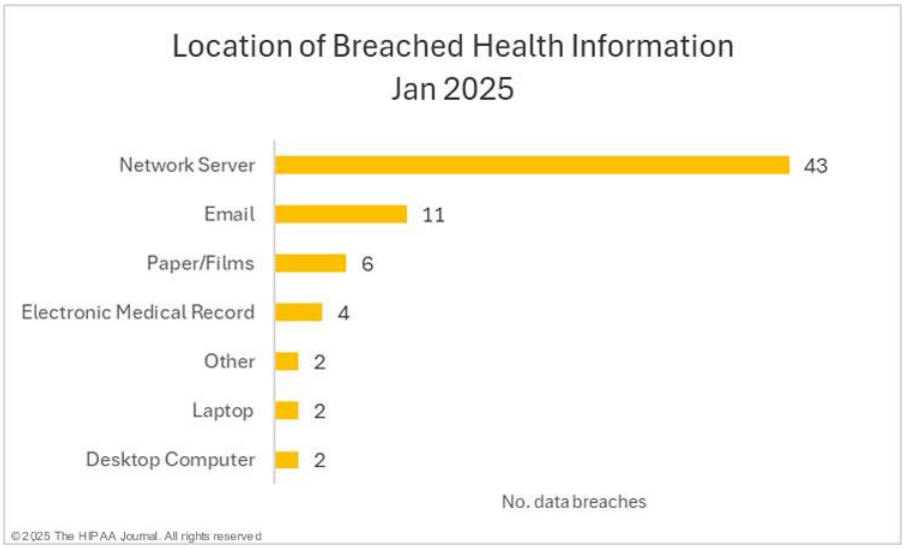


그림 9 의료 정보가 유출된 경로

(출처: HIPAA Journal,『January 2025 Healthcare Data Breach Report』)

정보가 유출이 발생한 경우 비밀번호 재설정이나 이메일 2 단계 인증 의무화 등 즉각적인 대응이 이루어졌으나,[45] 이는 근본적인 해결 방법이 아니며, 다중 인증, 세분화된 접근 제어와 같은 구조적인 보안 조치의 필요성이 지속적으로 제기되고 있다. 또한 소프트웨어 마이그레이션 상황에서도 의료데이터 해킹

사례가 발생한다. 프랑스 매거진 ZATAZ 는 2021 년 2 월, 데이터베이스 유출로 인해 다크웹에서도 특정 데이터의 결과가 판매되고 있다고 보도했다.[46] 데이터 유출 원인으로는 소프트웨어에서 다른 툴로 마이그레이션하는 상황에서 필요 이상의 데이터 추출, 보안 조치의 부족, 제 29 조 GDPR(Processing under the authority of the controller or processor) 미준수, 제 32 조 GDPR(Security of processing)의 개인 데이터의 보안을 보장하지 않은 점이 있다.

표 16 General Data Protection Regulation(GDPR) Chapter 4[47]

구분	내용
Section 1 (General obligations) 제 1 절: 일반적인 의무	Article 24 – Responsibility of the controller (제 24 조–개인정보 처리자의 책임)
	Article 25 – Data protection by design and by default (제 25 조–설계 및 기본 설정에 의한 개인정보 보호)
	Article 26 – Joint controllers (제 26 조–공동 개인정보 처리자)
	Article 27-Representatives of controllers or processors not established in the Union (제 27 조–EU 에 설립되지 않은 개인정보 처리자 또는 수탁자의 대리인)
	Article 28 – Processor (제 28 조–개인정보 처리자)
	Article 29 – Processing under the authority of the controller or processor (제 29 조–개인정보 처리자의 권한 내에서의 처리)
	Article 30 – Records of processing activities (체 30 조–개인정보 처리 활동 기록)

	Article 31-Cooperation with the supervisory authority (제 31 조−감독기관과의 협력)
Section 2 (Security of personal data) 제 2 절: 개인정보의 보안	Article 32-Security of processing (제 32 조−개인정보 처리의 보안)
	Article 33-Notification of a personal data breach to the supervisory authority (제 33 조−개인정보 침해 발생 시 감독기관에 대한 통지)
	Article 34-Communication of a personal data breach to the data subject (제 34 조−정보주체에 대한 개인정보 침해 사실의 통지)
Section 3 (Data protection impact assessment and prior consultation) 제 3 절: 개인정보 영향 평가 및 사전 협의	Article 35-Data protection impact assessment (제 35 조−개인정보 영향 평가)
	Article 35-Prior consultation (제 36 조−사전 협의)
Section 4 (Data protection officer) 제 4 절: 개인정보 보호책임자	Article 37-Designation of the data protection officer (제 37 조−개인정보 보호책임자의 지정)
	Article 38-Position of the data protection officer (제 38 조−개인정보 보호책임자의 지위)
	Article 39-Tasks of the data protection officer (제 39 조−개인정보 보호책임자의 임무)
Section 5 (Codes of conduct and certification) 제 5 절: 행동강령 및 인증	Article 40-codes of conduct (제 40 조−행동강령)
	Article 41-Monitoring of approved codes of conduct (제 41 조−승인된 행동강령의 모니터링)
	Article 42-Certification

(제 42 조-인증)
Article 43-Certification bodies
(제 43 조-인증 기관)

(출처: Regulation (EU) 2016/679, 『General Data Protection Regulation』)

해킹, 무단 접근, 소프트웨어 취약점 등으로 의료데이터가 노출될 수 있으며 유출된 정보(HIV, 암, 유전 질환 등)는 피싱, 사기 등의 2 차 피해로 이어질 수 있다. 의료기관이나 서비스 업체에서는 2중 인증 로그인, 이메일 보안 통제 시행, 사용자 인증 및 인증 절차 강화, 이메일 전송 가능 데이터 유형 제한, 직원 교육 등 다양한 방법을 통해 의료데이터를 보호하거나 사후 조치를 진행하고 있다.

이러한 사이버 공격 사례뿐만 아니라, 의료기관에서 사용하는 전자의무기록(EMR) 시스템에서도 유출되는 사례가 있다. 한국보건의료정보원에 따르면 2024 년 9 월 기준으로 전체의료기관 3 만 8,012 개소 중 91%인 3 만 4,421 개소가 EMR 을 도입했다.[48] 국내 병·의원에서 랜섬웨어 공격으로 개인정보나 상담 내역이 유출되는 사례가 증가하고 있으며 개인정보보호위원회와 보건복지부가 협력하여 의료기관 개인정보 보호 강화에 노력하고 있다. 개인정보위원회는 의료기관의 환자 정보 유출 이후 보건복지부의 협조를 받아 2023 년 6 월부터 9 월까지의 전자의무기록(EMR) 시스템을 제공하는 소프트웨어를 조사했다. 그 결과 [표 17]와 같이 시스템에서 개인정보 보호에 필요한 기능이 미흡한 점을 확인했고, 의료기관이 사용하는 EMR 시스템의 보호 수준을 향상하기위해 EMR 인증기준과 청구소프트웨어 적정성 검사 기준을 강화하고 구체적인 방안을 마련하고자 했다.[49]

표 17 EMR 의 개선 필요 사항[49]

구분	필요사항
1	개인정보취급자 계정에 대한 접근권한 관련 기록
2	비밀번호 제한 해제 시 확인

3	외부에서 접속 시 안전한 접속·인증수단
4	안전한 암호화 알고리즘
5	취급자 접속기록 중 처리한 정보주체 정보 기록
6	개인정보 다운로드 사유 입력·확인
7	삭제 기능 제공

(출처:개인정보보호위원회 기관 소식, 정부 24)

국내외 병원 정보 해킹으로 인한 개인정보 유출 사례로 인해 병원 내 EMR 도 보안 강화에 대한 필요성이 증가하고 있다. 2021 년 EMR 랜섬웨어 공격 기사에 따르면 의료기관이 보안사고 대응 시 상급종합병원 59.5%, 300 병상 이상 종합병원 53.6%, 300 병상 미만 종합병원 55.5%, 병원 59.6%가 보안 기술과 같은 전문성 미흡 문제로 어려움을 겪고 있는 것으로 나타났다.[50] 이는 환자 데이터를 관리하는 핵심 시스템인 EMR 에서 보다 높은 수준의 보안 역량이 요구되고 있음을 보여준다.

의료데이터 유출 사례를 분석해 보면, 해킹의 주요 동기는 의료기관에 대한 랜섬웨어 공격뿐만 아니라 보험 사기, 신분 도용 목적의 개인 건강 정보 탈취, 불법 데이터 마켓에서의 건강정보 매매, 내부자 실수 등이 있다. 특히, 생체 정보, 유전 정보, 질병 이력 등은 일반적인 개인정보보다 훨씬 높은 시장 가치를 지니며, 해커들의 주요 표적이 되기 쉽다. 이러한 현실을 고려할 때, 의료데이터 보호는 단순히 환자의 사생활을 지키는 것을 넘어, 의료기관에 대한 사회적 신뢰, 공공 안전, 그리고 국가 차원의 경제적 안정성과도 직결되는 문제임을 인식할 필요가 있다. 의료데이터 유출은 병원 내 전자의무기록(EMR) 시스템뿐만 아니라 데이터의 기밀성, 무결성, 가용성을 보장할 수 있는 사이버 보안 체계가 필요하다.

의료기기의 경우, 사이버 보안 위협에 대응하기 위해 [표 18]과 같은 사이버보안 가이드 제시나 기술적 대책이 국내외에서 제안되고 마련되고 있다. 이에 준하는 구체적이고 체계적인 보안 대책이 의료데이터에도 적용되어야 할 것이다.

표 18 의료기기 사이버보안 가이드

대책 및 기술	내용
물리적 접근 제어	권한이 있는 담당자에게만 의료기기에 대한 접근 허용, USB 드라이브 등 이동식 매체 사용 제한
네트워크 격리	의료기기를 병원 네트워크에서 격리, 필요한 네트워크 통신만 허용하도록 방화벽 설정
지속적인 모니터링 및 업데이트	지속적인 모니터링, 데이터 백업, 보안 취약점을 해결하기 위해 정기적으로 소프트웨어 업데이트
보안 내재화	의료기기 설계 단계부터 보안 고려하여 개발

(출처: 한국방송통신전파진흥원, 『ICT 산업 Hot Clips vol.83』, 2022
한국인터넷진흥원, 『의료분야 ICT 융합 제품·서비스의 보안 내재화를 위한 스마트의료 사이버보안 가이드』, 2018)

4. 체외진단 의료데이터 분류와 데이터 등급별 보안 방법 제시

가. 체외진단 의료데이터 보호를 위한 기술적 보안 방안

체외진단 의료데이터는 진단의 정확도와 개인의 건강 상태를 반영하는 민감한 정보로, 데이터의 민감도와 및 활용 목적에 따라 체계적인 분류와 맞춤형 보안 전략이 필요하다. 해킹, 내부 유출, 시스템 침해 등 다양한 위협에 노출된 현실을 고려할 때, 데이터를 효과적으로 보호하기 위한 기술적 대응 방안이 필요하다. 이에 따라 체외진단 의료데이터를 위험 등급별로 분류하고, 각 등급에 적합한 보안 대응 방안을 기술 중심으로 정리했다.

의료데이터 보호를 포함해 데이터 보호에 사용될 수 있는 기술 요소들은 전송 과정에서의 보안, 인증 방식, 접근 통제, 네트워크 구조 등 여러 분야의 기술이 활용된다. HTTPS 또는 가상 사설망(virtual private network, VPN)과 같은 안전한

전송 프로토콜은 사이버 보안을 위한 기본 조건으로, 데이터가 외부로 노출되지 않도록 한다. 다중 인증(Multi-factor authentication, MFA)은 민감한 의료 IT 시스템을 비인가 사용으로부터 보호하는 데 중요한 역할을 하고 있고, 비대칭 암호화 기술인 공개 키 인프라(Public Key Infrastructure, PKI)는 가장 신뢰받는 인증 방식 중 하나로 평가받는다. 또한, 신원 접근 관리(Identity access management, IAM)는 인증되지 않은 사용자의 접근을 차단함으로써 시스템 오용을 효과적으로 방지한다.[51] 이러한 기술을 포함해 [표 19]에서 의료 분야에서 사용될 수 있는 사이버 보안 기술을 정리했다.

표 19 사이버 보안을 위한 기술

기술	내용
암호화 및 인증	– End to end 암호화: 데이터 전송 및 저장 시 모든 수준에서 암호화를 적용하여 기밀성 보장 – 다중 인증(MFA): 공개 키 기반구조(PKI)를 활용한 비대칭 암호화 기술로 안전한 인증 제공
네트워크 보안	– 제로 트러스트 보안: 모든 사용자와 기기를 지속적으로 인증하는 IT 보안 프레임워크 – 네트워크 분할: 의료기기 네트워크를 분리하여 취약점 진단, 격리 용이
AI 및 머신러닝	– AI 기반 이상 탐지: 사이버 공격에 대한 효과적인 방어 메커니즘으로 활용 – 실시간 위협 탐지: AI 와 머신러닝을 이용해 데이터 패턴 분석, 잠재적 보안 위협 식별
블록체인	– 환자 데이터를 안전하게 처리 가능, 투명한 데이터 교환 가능 – 개인의 건강과 관련된 모든 데이터의 기록, 저장, 유통에 대한 소유권 확보 가능해 안전하게 데이터 활용 가능[52]

클라우드 기술	– 가상 저장소를 통해 위치에 상관없이 여러 기기에서 접근 가능 – 개별 사용자 권한 설정으로 보안 강화

(출처: COMPAMED, 『Technologies for maximum cybersecurity in medical technology』,2025)

보안 기술은 국제 규제 기준에서도 중요성이 강조되고 있다. EU 의 GDPR 에 따르면 건강 및 환자 데이터는 전송 중 암호화 또는 익명화를 통해 보호해야 한다. 미국의 HIPAA 규정은 데이터 저장 및 전송 시에 암호화가 필요한 이유를 설명함으로써 암호화 방식은 의료데이터 보안에 있어 중요한 것을 알 수 있다. 이처럼 대칭 키 암호화 알고리즘 암호화 방식, 비대칭 키 암호화 방식 등 의료데이터 보안을 위해 사용되는 암호화 기술은 의료데이터 보안에 핵심으로 활용되어야 한다. 이러한 기술 외에도, 의료기관이나 관련 기관, 기업은 데이터 암호화, 접근 제어 및 인증, 네트워크 분리, 사고 대응 계획이나 정기적인 보안 교육 등 포괄적인 보안 조치를 마련해야 한다. 보안의 목적과 사용 환경에 따라 적절한 기술을 선택하고 조합하는 것이 중요하다고 생각한다.

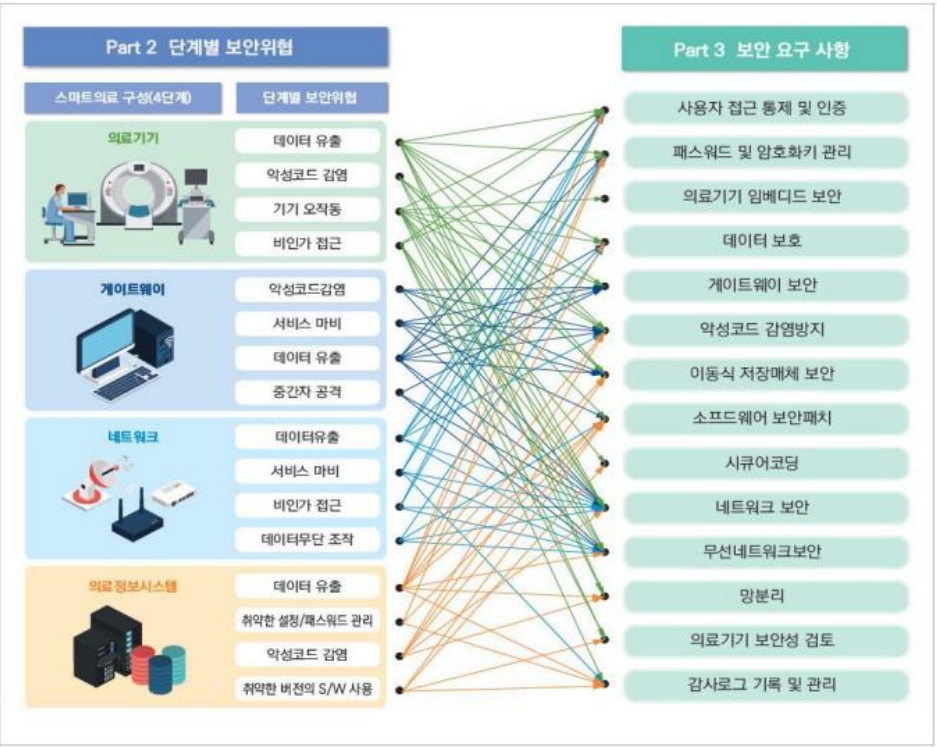


그림 10 스마트 의료 보안위협 및 보안요구사항

(출처: 한국인터넷진흥원,『스마트의료 사이버보안 가이드』,2018)

사례적으로, 한 헬스케어 기술 기업에서 사이버 보안 프로토콜을 개편한 후 사이버 위협에 대한 취약성을 크게 줄였다. 모든 데이터 전송에 대해 end-to-end 암호화를 구현해 환자 정보를 안전하게 보호했고, 플랫폼에 다중 요인 인증(MFA)을 채택해 사용자의 신원을 검증했다. 또한, Phishing 공격을 방지하기 위한 이메일 필터링 기술을 도입하고, VPN 인프라와 실시간 사이버 보안 모니터링 센터를 구축해 보안 체계를 구축했다.[53] 이 사례는 헬스케어 분야에서 사이버 보안의 중요성과 신뢰성이 예방 및 보안에 긍정적인 영향을 끼친 것을 확인할 수 있다.

따라서 체외진단 의료데이터 보호를 위해서는 의료 분야에 특화된 기술뿐만 아니라 다른 산업 분야에서 검증된 보안 기술을 도입·활용할 필요가 있다. 이와

관련하여 보안 대응 방안은 데이터 보호 방법, 네트워크 보안 방법, 사이버 위협 대응, 직원 교육 관리, 규제 준수 등으로 분류될 수 있다.

표 20 의료데이터 보호를 위한 보안 기술 분류 및 활용 예시

구분	보안 방법	주요 목적	활용 예시 및 특징
인증 방법	이중 인증(2FA)	비밀번호 외 두 번째 인증 계층	문자 인증, 인증 앱 등
	다중 인증 (MFA)	세 가지 인상 인증 요소로 강화	생체 정보+기기+PIN
	생체 인증	고유 생체 특성으로 본인 확인	지문, 홍채, 얼굴 인식 등
	적응형 인증	실시간 위험 평가 기반 동적 인증	위치, 시간, IP 기반 맞춤 인증
암호화 방법	데이터 암호화	데이터 전송 및 저장 시 보호	AES, RSA, ECC
접근 제어	RBAC (역할 기반 접근제어)	직무에 따라 정보 접근 권한 제한	차등 접근 제어
네트워크 보안	SIEM	보안 이벤트 통합 모니터링 및 대응	로그 분석, 실시간 경고
	방화벽	네트워크 출입 통제	승인된 트래픽만 허용
	네트워크 세분화	내부망 분리로 민감 데이터 보호	환자정보망, 업무망 분리 등

(1) 이중 인증(Two-Factor Authentication, 2FA)

단순한 PIN 이나 비밀번호 외에 계정 접근을 위한 추가 보안 계층이 요구된다. 휴대폰으로 전송된 코드를 입력하거나 인증 앱 사용, 생체 인식 데이터를 제공하는 것이 포함될 수 있다.

(2) 다중인증(Multi-Factor Authentication, MFA)

다중인증은 비밀번호 외에 추가 인증 단계를 요구해 사용자 계정에 보안 계층을 더하는 방법이다. 이중 인증은 2 단계 인증, 다중인증은 2 단계 이상 인증을 의미한다. 비밀번호와 함께 두 사지 이상의 독립적인 인증 수단을 결합해 신원을 확인한다. 다중인증에는 생체 인식, 토큰, 일회용 비밀번호 등 다양한 방식이 있으며, 사용자 선호에 따라 선택할 수 있다.[54] 다중인증은 승인되지 않은 사용자나 해커가 리소스(예: 계정, 디바이스, 네트워크, 데이터베이스 등)에 접근하지 못하도록 다층 방어 시스템을 사용해 다층 방어 체계를 구축할 수 있다. 비밀번호만 사용하는 경우에 비해 보안 침해 위험을 크게 줄일 수 있다. 사용자가 로그인 시 지식 기반, 소유물, 생체 특징, 시간 정보를 바탕으로 신원이 검증된다.[55] [표 21]에서는 다중 인증의 인증 요소별 유형과 예시를 정리했다.

표 21 다중 인증(MFA)의 인증 요소별 유형 및 예시

유형	내용	예
지식 기반	지식 기반 검증을 위해 사용자는 보안 질문에 답해야 함	– 보안 질문에 대한 답변(출생지, 좋아하는 색, 음악 등) – OTP(One-Time Password) – 비밀번호 – PIN
소유물	로그인 시 사용자가 소유한 개체 필요	– 전자 열쇠 – 휴대전화

		– 스마트 카드 – 물리적/소프트 토큰
생물학적 특성	사용자의 신원 확인을 위한 사용자의 생물학적 특성 확인 필요	– 얼굴 인식 – 지문 스캔 – 망막/ 홍채 스캔
시간	특정 시간, 특정 시스템, 위치에 대해 사용자의 존재를 감지, 사용자 신원확인 필요	– 특정 시간 활동 감지 – 시간에 따른 위치 감지

(출처: SailPoint,『What is multi-factor authentication(MFA)』)

(3) 생체 인증(Biometric Authentication)

생체 인식 보안은 단독이나 2FA, MFA 의 단계로 사용될 수 있다. 생체인증은 개인의 고유한 생체 특성(예: 지문, 홍채, 얼굴, 음성)을 기반으로 신원을 식별 및 인증하는 기술로 다양한 보안 분야에서 보호 제공을 하고 있다. 특히 모바일 기기에서 보편화 된 방법으로 금융 거래나 기업 접근 통제에서 여러 가지의 생체 인식 방식을 병행해 단일 생체 인증 방식의 취약점을 보완하고 있다. 높은 신뢰성 제공, 강화된 보안성을 갖추고 있어 다중 인증이 필요한 고위험 분야에서 보안성 강화에 중요한 역할을 한다.[56]

(4) 적응형 인증(Adaptive Authentication)

적응형 인증은 위험 기반 인증이라고도 하며, 로그인 시도와 관련된 다양한 위험 요소를 실시간으로 평가하는 단계별 인증 방식이다. 위치, 장치, 사용자 행동, 위험 수준 등 상황별 정보를 고려해 사용자 접근 권한을 결정한다.[57] 금융,

의료, 전자상거래 등 민감한 데이터를 다루는 고위험 산업 분야에서 더 많이 활용되고 있다.

표 22 기존 인증과 적응형 인증 방식 비교

요소	기존 인증	적응형 인증
접근 방식	고정적 (예: 다단계 인증의 경우 고정된 다단계 절차로 인증 진행)	동적 및 상황 인식
위험 평가	없음	인증 시도와 관련된 위험 평가
보안 수준	자격 증명 일치 여부 확인 고정 수준의 인증	다중 요인 고려, 위험 분석을 통한 보안 강화
사용자 경험	모든 활동, 사용자에 대해 동일한 인증 요구	위험 수준에 따라 맞춤형 절차
유연성	고정된 보안조치로 제한적	환경과 행동에 따라 조절 가능

(출처: Silverfort, 『Adaptive Authentication』)

기존 인증은 모든 사용자에게 동일한 보안 수준을 적용하는 반면, 적응형 인증은 사용자 행동과 환경 정보를 바탕으로 위험을 분석해 필요에 따라 추가 보안 조치를 적용한다. 예를 들어, 로그인 위치, 장치 정보, 행동 패턴, 로그인 시간을 분석해 비정상적인 접근 시도 시 추가 인증을 요구한다.

과거 금융 기관은 직원과 고객의 데이터 접근을 위해 이중인증과 다중인증을 도입했으나, 비밀번호 재사용 문제로 인해 한계가 있었다. 이를 보완하기 위해 적응형 인증이 새로운 표준으로 자리잡았으며, 포털이나 애플리케이션 접근 시 SSO 와 이중 인증에 추가 보안 계층을 더하는 방식으로 적용했다.[58]

적응형 인증은 위험 점수에 따라 보안 수준을 조절할 수 있다. 예를 들어, 저위험 시에는 비밀번호만 요구하고, 중위험의 경우 다단계 인증을, 고위험의 경우 추가 인증 프로세스를 진행하는 방법으로 최적화된 인증 방법을 제공한다.

표 23 적응형 인증 적용 시 고려 요소 및 예시

요소	예시
디바이스	사용자가 승인되지 않은 디바이스를 사용해 로그인 시도 여부 확인
IP 주소	사용자가 리소스에 로그인할 때 일반적으로 사용하는 IP 주소와 동일한지 확인
위치	– 사용자가 짧은 시간 내에 다른 위치에서 계정에 로그인 시도 여부 확인 – 로그인 위치 확인 – 회사(병원) 네트워크, 공용 네트워크에서 로그인 시도 여부 확인
민감도	민감한 정보에 접근 여부 확인
로그인 시간	로그인 시간이 사용자의 일반적인 로그인 시간과 관련있는지 확인

(출처: SailPoint,『What is multi-factor authentication(MFA)』)

(5) 데이터 암호화(Data Encryption)

그림 11 데이터 암호화

(출처: AppSealing News,『데이터 암호화는 안전한 디지털 생태계에 어떻게 기여하는가?』,2022)

데이터는 저장 중(at rest)과 전송 중(in transit) 모두 암호화 알고리즘을 사용해 보호되어야 한다. 데이터 암호화는 수학적 알고리즘을 통해 데이터를 암호문으로 변환하여 해킹을 방지하는 기술로, 올바른 키를 가진 사람만이 데이터를 복호화해 원래 상태로 복원할 수 있다. 이 과정은 기밀성, 무결성, 인증이라는 세 가지 보안 요소를 보장하며, 권한 없는 접근을 막는다.[59]

데이터 암호화 알고리즘은 기본적으로 암호화 프로세스를 제어하는 규칙 및 명령이다. 암호화 시스템의 키 길이, 특징, 기능에 따라 효율성과 보안 수준이 달라지며, 대칭키 암호화와 공개키 암호화로 나뉜다. 대칭키 암호화는 데이터를 암호화하고 복호화하는 데 동일한 키를 사용하는 방식이고 공개키 암호화는 공개키와 개인키를 사용해 데이터를 암호화하고 복호화하는 방식이다 암호화 알고리즘은 수년 동안 악성 공격에 대응하기 위해 발전해 왔다. 다양한 보안 요구를 충족하는 수많은 암호화 알고리즘이 있으며, 그 중 일반적으로 사용되는 알고리즘은 다음과 같다.

표 24 데이터 암호화 알고리즘 종류 및 특성

암호화 방식	특징
AES (Advanced Encryption Standard)	– Rijndael 알고리즘 기반으로 한 대칭 키 암호화. – 미국 정부 암호화 표준으로 제정 – 하드웨어와 소프트웨어에 모두 이용되어 메시징 앱을 암호화하는데 사용
RSA (Rivest-Shamir-Adleman)	– 전송 중 데이터를 보호하기 위해 사용되는 비대칭 암호화 – 처리 능력이 큰 경우에만 해동할 수 있으며 길이가 긴 키에 많이 사용
3DES/ TDES (Triple DES)	– 금융 서비스에서 하드웨어 암호화 용도로 사용됨

	– 암호화, 복호화, 재 암호화 세 가지 단계로 작동
ECC (Elliptic Curve Cryptography)	– 보안을 보장하는 향상된 버전의 RSA – 메모리를 적게 사용해 모바일 기기에서 사용 시 유용
Twofish Encryption	– 복잡한 키 구조를 가진 가장 빠른 알고리즘 중 하나 – 하드웨어 및 소프트웨어 환경 사용에 이상적

(출처: AppSealing News,『데이터 암호화는 안전한 디지털 생태계에 어떻게 기여하는가?』,2022)

(6) 역할 기반 접근 제어(Role-based access control, RBAC)

네트워크 접근 제어(Network Access Control, NAC)가 보안 표준을 충족하는지 확인하는 데 중점이 있다면 역할 기반 접근 제어(RBAC)는 사용자에게 부여된 역할(Role)에 따라 접근 권한을 설정하는 데 초점을 둔다.

RBAC 는 사용자에게 사전에 정의된 역할을 기반으로 시스템, 애플리케이션 및 데이터에 대한 접근 권한을 부여하는 보안 모델로, 조직 내 직무와 책임에 기반한 접근 제어를 제공해 보안성과 관리 효율성을 동시에 향상시킬 수 있다.

RBAC 은 1992 년 미국 국립표준기술연구소(National Institute of Standards and Technology, NIST)에 의해 발표되었다. 특히 의료 정보 시스템(HIS)에서 널리 적용되고 있으며, [60] 보안관련 시스템과 컴퓨터 시스템에서 적용되고 있는 정보보호 기술 중 하나로 보안관리의 용이성, 비용감소에 효과가 있어 다양한 환경에서 적용되고 있다.[61]

다양한 산업 환경에서 요구되는 보안 정책에 유연하게 대응할 수 있도록 설계된 RBAC 은 접근 관리를 간소화하고 데이터 센터 정보 보안 유지 및 권한 관리의 일관성을 확보하는 데 기여한다. 특히 금융, 의료 등 고도화된 정보 보호가 요구되는 분야에서 역할 기반 권한 부여를 통해 내부자의 위협, 직원의 실수, 외부 위협 등 다양한 보안 위협으로부터 효과적으로 방어할 수 있다.

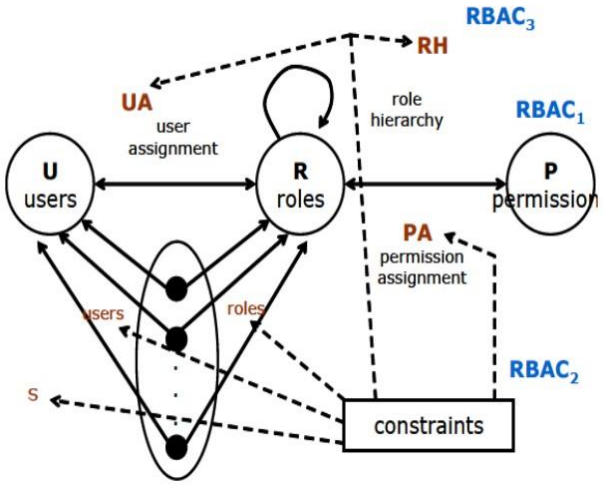


그림 12 RBAC(Role-Based Access Control) 모델

(출처: 한국산학기술학회논문지,『 RBAC에 기반한 개인 맞춤형 건강 정보 제공 헬스케어 서비스 플랫폼』. 2014)

RBAC 모델 구성요소는 다음과 같다. 의료인 혹은 사용자, 디바이스는 User에 해당되며 할당된 역할(Role)에 따라 권한(Permission)이 부여된다. 의료인·사용자·디바이스-역할(User-Role, UR) 관계, 역할-권한(Role-Permission, RP) 관계, 역할-역할(Role-Role ,RR) 관계가 존재한다.[62]

표 25 역할 기반 접근 제어(RBAC) 모델의 구성요소

구성 요소	내용
사용자 (User)	시스템에 접근하는 개별 엔티티 (예: 사람, 디바이스, 애플리케이션 등)
역할	특정 직무나 책임과 관련된 권한 집합

(Role)	(예: 관리자, 직원, 게스트 등)
권한 (Permission)	사용자가 시스템 내에서 수행할 수 있는 작업 (예: 데이터 읽기(Read), 쓰기(Write), 삭제(Delete) 등)

특히 의료분야에서 환자 데이터 보호를 위해 의료진별로 접근 가능한 정보 범위를 제한하기 위해 사용되기도 한다. 또한 클라우드 기반 애플리케이션에서 특정 역할에 따라 데이터 저장소, API 에 대한 접근을 제한해 금융 산업에서는 고객 데이터 보호, 내부 위협 및 외부 공격을 방지를 위해 활용된다.

표 26 의료기관에서의 역할 기반 접근 제어(RBAC) 적용 사례 예시

순서	내용
1	병원 IT 관리자가 “간호사”에 대한 RBAC 역할 생성
2	관리자는 약물 확인이나 전자 건강 기록(HER) 시스템에서 간호사 역할에 “데이터 입력” 권한 설정
3	병원의 간호사에게는 RBAC 간호사 역할 할당
4	간호사 역할에 할당된 사용자가 로그인하면 RBAC 는 사용자에게 부여된 권한 확인, 해당 세션에 대한 접근 권한 부여
5	“약물 처방”, “검사 주문”과 같이 다른 시스템 권한은 간호사에 대한 권한이 없으므로 사용자 거부

(출처: IBM,『What is role-based access control (RBAC)?』)

RBAC 는 구성요소들을 확장하거나 정의함으로써 다양한 조직 환경에 맞춰 유연하게 적용할 수 있다. 사용자가 직접 권한을 가지는 대신, 역할을 통해 간접적으로 권한을 받는다. 사용자의 역할에 따라 의료정보에 대한 접근 권한을 제한함으로써 정보보호와 프라이버시 침해를 최소화할 수 있으며, 민감 정보에 대한 통제를 강화할 수 있다.

(7) SIEM(Security Incident and Event Management) 시스템

Security Information Management (SIM)와 Security Event Management (SEM)을 결합하여 SIEM 으로 만들어졌다. SIEM 시스템은 애플리케이션과 네트워크, 하드웨어에서 생성된 보안 경고를 실시간으로 수집, 분석해 통합적으로 관리할 수 있는 통합 솔루션이다. SIM 은 로그 데이터의 수집, 분석, 보고에 중점을 두고 SEM 은 실시간 모니터링과 사고 관리에 중점을 둔다. 실시간 이벤트 모니터링, 위협 탐지, 로그 분석, 사고 대응 및 보고를 포함하여 전반적인 보안 태세를 강화해 보안 위협을 효율적으로 대응할 수 있다.[63]

시스템, 네트워크 장비, 보안 장비 등에서 생성되는 로그에는 사용자 접근기록, 활동기록, 외부침투기록, 장애의 흔적 등 각 기기가 동작된 모든 흔적이 남아있다. SIEM 은 기기의 모든 로그를 수집해 흔적을 분석한다. 어디에서 위협을 받고 있는지, 이상 사례가 발생되는지 빠르게 분석, 파악해서 관리자에게 알려줄 수 있으며 미리 위협 행위를 차단해 사고를 예방할 수 있도록 도와준다.

표 27 SIEM 시스템이 적용되는 주요 산업 분야

구분	내용
민감한 데이터 보유한 조직	금융 기관, 의료 제공업체, 정부 기관 등 민감한 데이터를 취급하는 조직은 보안 위협을 실시간으로 감지, 잠재적인 보안 사고를 모니터링
대규모 IT 인프라를 갖춘 기업	여러 시스템, 네트워크 및 장치를 포함한 광범위한 IT 인프라를 갖춘 기업 및 이벤트 로그를 중앙 집중식으로 분석해야 하는 경우
위협 정보 관련 조직	보안 서비스 제공업체, 사이버 보안 회사나 정부 기관 등은 다양한 출처의 위협 정보를 수집·분석하여 사전에 위협을 감지하고 대응할 수 있음

사고 대응 전담 조직	위협 탐지 자동화로 사고 조사, 억제, 복구 등 일련의 보안 사고 관리 프로세스 효율화
규정 준수 중심 산업	금융 부문(PCI DSS), 의료 부문(HIPAA), 데이터 프라이버시(GDPR) 등 엄격한 규제가 요구되는 분야는 보안 사고 모니터링 및 보고 기능 필요

(출처: SECURIUM SOLUTIONS. 『Security Incident Event Management(SIEM SECURITY)』)

(8) 네트워크 세분화

네트워크 세분화는 컴퓨터 네트워크를 더 작고 관리 가능한 세그먼트 또는 하위 네트워크로 나누는 것으로 세그먼트 간 트래픽 흐름을 제한해 민감한 데이터를 분리하고 사용자 접근을 효과적으로 관리할 수 있다. 데이터 유출 가능성을 줄이고, 데이터 개인정보 보호 및 GDPR, HIPAA, PCI DSS 와 같은 보안 규정에 준수할 수 있는 환경을 만들 수 있다. 또한, 데이터 암호화, 모니터링 프로토콜과 같은 규제 요구 사항에 맞는 특정 보안에 적용할 수 있다.

표 28 네트워크 세분화 적용 사례

적용 분야	내용
의료기관	– 대형 의료 제공업체가 HIPAA 규정 준수를 위해 네트워크 세분화 구현 – 세그먼트(네트워크 내에서 논리적 또는 물리적으로 여러 개의 작은 영역으로 나누는 것)에서 환자 데이터 분리해 접근 제어 시행 – 정기 감사 결과 데이터 유출 감소 및 세분화로 사고 대응 시간 단축, 잠재적 위협에 효과적 대응 가능

금융기관	– 대형 은행에서 사이버 공격 이후 보안 강화를 위한 네트워크 세분화 도입 – 내부 운영, 고객 데이터, 거래 처리를 위한 별도 세그먼트 생성 – 노출이 제한되어 맞춤형 보안 조치 시행 가능
소매 회사	– 판매 시점 시스템 세분화, 고객 결제 데이터 보호를 위한 네트워크 세분화 구현 – 세분화 후 감사 결과 보안 표준 준수, 보안 사고 감소 확인

(출처: EasyChair Preprint .『The Role of Network Segmentation in Enhancing Data Privacy and Meeting Security Standards』. 2024)

표 29 네트워크 데이터 유출 사례

피해 사례	내용
신용카드 정보 노출 (2013 년)	– 수백만 명의 고객 신용카드 정보 데이터 유출 – 내부 네트워크 접근을 위한 약해진 네트워크 세분화 악용
데이터 유출 (2017 년)	– 취약점 놓침, 세분화 불충분으로 데이터 유출 – 공격자는 네트워크 간 이동으로 소비자 데이터에 접근
고객 기록 노출 (2019 년)	– 잘못 설정된 방화벽이 공격당해 고객 기록 노출 – 데이터 저장 시 세분화가 불충분한 경우 위험을 초래할 수 있음을 확인

(출처: EasyChair Preprint .『The Role of Network Segmentation in Enhancing Data Privacy and Meeting Security Standards』. 2024)

이러한 사례를 통해 확인할 수 있듯, 네트워크 세분화는 외부 공격이나 침입이 발생하더라도 피해를 제한하는 데 효과적임을 알 수 있다.[64] 보안 위협을

격리함으로써 민감한 데이터에 대한 접근을 제한해 데이터 프라이버시 보호와 지속적인 모니터링을 통해 보안 강화에 기여한다.

나. 의료데이터 분류에 따른 보안 방법 고찰

체외진단 기기에서 해킹되어 악성 소프트웨어가 테스트 결과를 조작하거나 잘못된 진단, 치료 지연, 체외진단 기기를 대상으로 랜섬웨어 공격, 체외진단 장비로부터 만들어진 의료데이터가 의료 기관과 관련 기관의 네트워크 상에서 해킹되는 경우 등 다양한 방법으로 사이버 침해의 위협에 노출되어 있다. 개인정보보호법이나 데이터 보호를 위한 규정, 보안 방법은 있으나 상황에 따라 제시되는 보안 방법은 구체적이지 않다. 의료데이터 해킹 방지를 위해 기술적, 조직적 접근법을 통해 효과적인 보안 방법이 필요하다고 생각되어 의료데이터 노출 사례를 바탕으로 데이터의 민감도, 위험도에 따라 분류해보고자 한다.

민감도는 데이터가 개인의 사생활, 신체적 및 정신적 상태, 정체성 등에 대한 민감한 정보를 포함하고 있는 정도이며 위험도는 의료데이터가 유출되거나 악용되었을 때, 개인에게 발생할 수 있는 피해의 심각도와 가능성을 종합적으로 평가한 척도이다

표 30 민감도, 위험도 비교

구분	민감도	위험도
의미	사적인/민감한 정보의 정도	유출 시 피해 발생 정도
초점	데이터의 내용 자체	데이터 유출 후의 결과
기준	사생활 침해 가능성, 사회적 낙인	금전적 피해, 차별, 법적 불이익 및 기술적, 사회적 악용의 파급력

체외진단 분야에서 생성되는 의료데이터는 진단 목적, 질병 관련성, 개인 식별 가능성 등에 따라 위험도와 민감도의 수준이 상이하게 나타난다. 따라서 제시하려는 의료데이터 등급은 의료데이터 자체 또는 다른 정보와 결합해 특정 개인 식별 여부, 민감정보 여부(유전자 정보, 감염병 정보 등), 임상 영향력(진단, 치료, 처방에 직접적인 관련 여부), 유출 시 피해 규모(생명, 사회적 및 프라이버시 침해 가능성 등)를 기준 요소로 분류하고자 한다.

일부 데이터는 상대적으로 민감도와 위험도가 낮은 저위험 데이터로 분류될 수 있다. 저위험의 경우, 일반 진료 이력, 키와 몸무게 등 비질환성 생체정보나 직접적인 피해 가능성이 낮은 의료데이터로 분류했다. 또 다른 예로 자가혈당측정은 환자가 일상적으로 혈당을 측정해 질병을 관리하는데 활용되며, 단일 혈당 수치는 특정 질병 유무나 개인의 정체성을 직접적으로 드러내지 않기 때문에 민감도가 낮은 데이터로 생각된다. 그러나 장기적으로 수집된 혈당 수치가 누적될 경우, 당뇨병 이력이나 건강 상태의 추정이 가능해져 보험사 등 제 3 자에 의해 차별적 의사결정의 근거로 활용될 위험이 있다. 따라서 이 데이터는 저위험군에 속하더라도 기본적인 암호화나 사용자 인증과 같은 보호 조치가 필요하다. 분류할 저위험 의료데이터는 개별 정보로는 심각한 프라이버시 침해나 법적 피해로 이어질 가능성이 낮지만, 외부 정보와의 결합, 장기적인 추적, 또는 의료기관 외 활용 등 다양한 상황에 놓일 시 위험 수준이 상승할 수 있다. 모바일 디바이스, IoT 기반 체외진단기기 등에서 수집되는 데이터는 무선통신 환경에 노출되기 쉬우므로 최소한의 보호가 필요하다.

표 31 의료데이터 저위험 분류

구분	의료데이터 유형	보안 필요성
일반 혈액 진단	백혈구 및 적혈구 수, 헤모글로빈 농도 등	단독 사용 시 위험도 낮음

지혈진단	혈액응고 수치	일반적 수치는 위험도 낮으나 수술 관련 정보 포함 시 위험도 높음
비질환성 생체정보	키, 몸무게 등	데이터의 민감도, 위험도 낮음

자가혈당측정은 단일 혈당 수치만을 기준을 보면 개인정보보호법이나 GDPR, HIPAA 등 국내외 개인정보 보호 규정상 명시적 민감정보에는 해당하지 않아 저위험 데이터로 분류될 수 있다. 그러나 해당 데이터는 병원 외부 환경에서 사용되는 모바일 앱, 블루투스 연동 기기 등을 통해 수집·전송되며, 장기적으로 축정될 경우 당뇨병과 같은 만성 질환의 진단 및 경과 관찰에 활용될 가능성이 있다. 특히 보험사나 고용주 등이 이 데이터를 통해 개인의 질병 이력이나 건강 위험도를 추정해 차별적 결정이 내릴 경우 사회적·경제적 피해로 이러질 수 있다. 따라서 자가혈당측정 데이터는 데이터 자체는 저위험이지만, 사용 환경과 활용 가능성을 고려할 때 중위험 등급으로 분류하는 것이 더 타당하다고 생각된다.

단일로만 봤을 때 위험도나 민감도가 상대적으로 낮아보일 수 있으나 만성 질환 진단이나 경과 관찰, 개인의 건강 상태를 나타내 의료적으로 중요한 지표의 경우, 사용 구조 고려 시 중위험으로 분류했다. 중위험 분류의 예로 혈당 검사의 경우 당뇨병 진단 및 관리에 핵심적인 지표로 보험사에서 질병 이력이나 만성질환 위험도 평가의 핵심 자료로 활용되어 보험료 책정, 보장 범위 결정에 영향을 미칠 수 있으며 임신 검사 결과의 경우 출산 보장 항목의 적용 여부나 산모 및 태아 보험, 기존 보험 상품에 대한 보장 범위 결정에 영향을 미칠 수 있다. 혈당검사, 임신검사 결과가 보험사에 무단 노출될 경우, 보험 가입 거절, 보험료 할증, 특정 질환 보장 제외 등 차별적 불이익이 발생할 수 있으며 이는 보험업법 제 97 조(보험계약의 체결 또는 모집에 관한 금지행위)에서 금지하는 부당한 차별에 해당할 수 있다.[65] 이는 검사 결과 정보의 유출이나 무단 활용이 보험 차별이나 불이익으로 이어질 수 있다는 점을 우려하는 점을 보인다. 혈당검사의 경우 단일 수치로만 볼 때 민감도가 상대적으로 낮아 보일 수 있지만,

해당 결과가 당뇨병과 같은 만성 질환의 진단 및 경과 관찰에 활용된다는 점에서 의료적으로 중요할 수 있는 지표이다. 중위험으로 분류된 의료데이터는 민감도는 다소 낮지만, 사회적 해석이 되거나 제 3 자 활용 시 잠재적 피해가 우려되는 경우이다. 사용하는 장소나 방법, 디바이스 이용으로 네트워크 상 보안이 필요한 경우, 다른 정보와 조합 시 위험성 증가 등의 경우로 기술적으로 보호하거나 접근통제가 필요하다.

표 32 의료데이터 중위험 분류

구분	의료데이터 유형	보안 필요성
자가혈당측정	혈당 수치	데이터의 민감도는 낮으나 데이터 누적 시 질병 추정 가능, 외부에서 디바이스 사용으로 확인하는 결과로 데이터 전송 과정 시 위험성 존재, 보험 차별 가능성 존재
면역화학 및 임상화학 검사	임신 진단 검사, 갑상선 호르몬 검사, 성호르몬 검사, 약물 농도 모니터링 검사	직접적인 민감정보는 아니지만 지속적인 기록이나 타 정보와 결합 시 의료적으로 민감한 정보 전환 가능
지혈진단	혈액 응고 검사	

고위험 보안으로는 유전정보나 감염병 관련 진단 결과를 나타내는 의료데이터다. 법적 보호 수준이 가장 높고, 유출 시 개인의 생명권, 사회적 차별, 사생활 침해의 위험성, 법적 불이익 등 실질적인 피해가 발생할 가능성이 높은 데이터를 포함한다. 다양한 의료데이터 중 유전정보는 국내 개인정보보호법상 민감정보로 분류되며, GDPR 제 9 조 민감정보 범주에서 처리 자체가 제한될 정도로 높은 수준의 보호가 요구된다. 특히 개인정보보호법 제 23 조에서

민감정보의 처리에 대해 명확한 제한을 두고 있다. 제 23 조 제 2 항에서 분실·도난·유출·위조·변조 또는 훼손 방지를 위한 안전성 확보 조치가 법적으로 요구된다.[20] 따라서 유전자 정보, 감염병 여부, 성병이나 정신질환 확인을 위한 정보는 고위험 의료데이터로 분류되며 정보주체의 권리 보장과 개인정보의 안전한 관리를 위해 기술적 및 관리적 보호조치가 가장 필요하다.

표 33 의료데이터 고위험 분류

구분	의료데이터 유형	보안 필요성
분자진단	유전자 검사	GDPR 및 개인정보보호법에 따라 민감정보로 정의됨. 고유 식별자 역할로 유전병 가능성 및 가족 구성원의 건강정보까지 유추 가능
면역화학진단	HIV 감염 검사, B 형/C 형 간염 바이러스 검사, 성병 검사, 자가면역질환 검사	감염병 정보는 사회적 차별 가능성, 사생활 침해에 있어 민감정보로 보호해야 함
치료약물농도 모니터링	정신질환 관련 치료약물 모니터링	정신질환 관련 정보가 포함되어 고용·보험 차별 가능성, 고위험 민감정보로서 보안 필요

IV. 고찰

의료 분야의 정보 유출 사고는 환자의 기본적인 개인정보뿐만 아니라 진료정보, 보험과 관련된 사회보장 정보, 금융 정보 등 환자의 다양한 민감 정보를 포함한다. 본 연구에서는 체외진단 의료장비에서 생성되는 다양한 의료데이터를 위험도 및 민감도 기준으로 분류하고, 그에 따른 보안 대응의 필요성을 제시한다. GDPR, HIPAA, 개인정보 보호법 등 국내외 주요 개인정보 보호 규제에서 규정한 민감정보 범주와 데이터 유출 시 데이터 자체의 민감도와 데이터 유출 시 예상되는 피해 수준(사회적·금융적 피해)을 기반으로 의료데이터를 분류했다. 의료기기는 위해도에 따라 각 국가별 의료기기 등급이 분류된다. 국내의 경우 식품의약품안전처에서 사용목적, 침습성, 생명유지여부 등을 기준으로 1~4 등급으로 분류된다. 기존의 의료기기 등급별 분류 체계처럼 의료데이터도 민감도와 위험도에 따라 차등 보호가 필요하다는 것을 제시한다.

모든 의료기기와 의료데이터의 보안은 중요하지만 상대적인 민감도, 위험도에 따라 분류하고 보안 방식을 제안해본다. 체외진단 의료기기로부터 생성되는 의료데이터를 민감도(정보 노출 시 개인 및 사회적 영향, 사생활 침해 가능성 기준)와 위험도 수준에 따라 저위험, 중위험, 고위험으로 분류했다. 저위험으로 분류된 의료데이터는 상대적으로 민감도가 낮지만, 개인정보 보호법의 적용을 받는 정보이므로 일정 수준의 보안이 필요하다. 따라서 이중 인증을 적용시키는 것을 제안한다. 중위험 데이터에는 특정 개인의 건강 상태를 직·간접적으로 파악할 수 있는 정보이다. 데이터 유출 시 차별 가능성이나 사생활 침해 가능성이 존재하므로 다중 인증이나 RBAC 을 도입해 데이터 접근 제한이 필요하다고 생각된다. 특히 고위험으로 분류되는 의료데이터는 유전 정보, 감염성 결과 등 노출 시 심각한 인권 침해 유발될 수 있다. 고위험으로 분류한 의료데이터는 유전 정보, 감염성 결과 등 노출 시 심각한 인권 침해 유발될 수 있다. 역할 기반 접근 제어(RBAC)로 사용자의 역할에 따라 의료정보 접근을 제한해 승인된 인원만 접근할 수 있도록 해 노출의 가능성을 최소화하고 암호화를 통해 데이터 유출의 가능성을 줄인다.

따라서 의료데이터 보호를 위해서는 역할 기반 접근 제어(RBAC)를 필수적으로 적용하되, 데이터 자체에는 보호를 위해 AES 암호화 방식을 병행 적용하는 것이 효과적일 것이다. 이와 같은 다중 보안 체계는 내부·외부 위협 모두에 대응하며, 데이터 유출 시에도 실질적 피해를 최소화할 수 있다

표 34 민감도, 위험도에 따른 의료데이터 등급 분류

등급	검사 유형	위험성	보안 필요 이유
고위험	유전자 검사	보험 가입 제한, 가족력 유추 가능	특정 유전 질환, 암 관련 유전자 변이, 약물 반응 예측 등 개인의 건강, 질병, 가족력, 미래 건강 상태까지 예측 가능함, 국내 개인정보보호법 및 GDPR 에서 민감정보로 명시
	감염병 검사 (HIV, B 형·C 형 간염, HTLV 등)	사회적 낙인, 고용 차별	사회적 낙인, 차별, 보험·취업 등에서 불이익 가능성이 큼
	이식 전 감염병/면역상태 검사	치료 결정에 영향	이식 적합성, 감염 위험 등 민감한 건강정보 포함됨, 환자의 생명권과 직결될 수 있는 정보
중위험	혈액형 검사 결과(ABO, RhD 등)	거의 없음	응급상황 외에는 비교적 덜 민감하지만, 특정 상황(이식, 수혈 등)에서는 중요
	혈당, 콜레스테롤, 빈혈 등 만성질환 관련 검사 결과	만성질환 유추, 보험료 인상 가능	당뇨, 고지혈증, 빈혈 등 만성질환 여부
	종양(암) 표지자 검사	암 진단 가능성 추정	암 진단, 재발·전이 여부 등 중대한 건강정보 포함
	임신 진단 결과	사생활 침해	개인의 사생활과 연관, 노출 시 사생활 침해 가능

	알레르기 패널 검사	특정 질환 추정 가능	특정 알레르기에 대한 반응 정보
저위험	일반 생화학 검사 (간기능, 신장기능 등)	단독 식별성 낮음	건강상태 확인 용도, 개별 정보의 파급력 낮음.
	혈압, 키, 체중 등 생체정보	위험도 낮음	비질환성 정보로 분류되며 일반적인 건강 지표에 해당. 외부와 연동 시 최소한의 보안 조치 필요

표 35 의료데이터 등급별 권장 보안 기술

위험도	적용 대상 의료데이터 종류	권장 보안 기술
저위험	– 비질환성 생체정보 – 일반 생화학 검사, 혈압	– 이중 인증
중위험	– 혈액형 검사 결과(ABO, RhD 등) – 혈당, 콜레스테롤, 빈혈 등 만성질환 관련 검사 결과 – 임신 진단 결과 – 알레르기 패널 검사 결과 – 개인용혈당측정기와 같이 휴대용 디바이스로 의료데이터 확인 – 종양(암) 표지자 결과	– 다중 인증 – 접근 제한 강화
고위험	– HIV·HBV·HCV·HTLV 등 감염병 검사 결과 – 유전자 검사 결과 – 이식 전 감염병/면역상태 검사	– 다중 인증 – SIEM 시스템 도입 – 네트워크 세분화 – RBAC, AES 암호화 조합

본 연구에서 등급별 의료데이터 특성과 위험도에 적합한 보안 기술을 적용하여 제안하였다. 그러나 이 보안 조치가 현실의 의료 환경에 일괄적으로 적용되기에는 기술적·운영상 제약이 존재한다. 저위험 의료데이터에 제안된 이중 인증은 현재 의료기관 내에서도 폭넓게 채택되고 있는 인증 방식으로 현실 적용 가능성이 높다. 반면, 중위험 이상의 데이터에 적용된 다중 인증이나 데이터 암호화는 시스템 구조의 변경이나 외부 솔루션 연동이 요구되며 의료기기의 내장 소프트웨어나 개인용 디바이스에 연계될 경우 기기 호환성, 성능 관련 확인이 필요할 것이다. 고위험 데이터에 제안된 SIEM 시스템, 네트워크 세분화, RBAC 와 암호화 AES 조합은 보안 수준은 높지만 구축과 유지에 어려움이 있을 것으로 생각된다.

이러한 보안 조치는 의료기관이나 기업, 그리고 사용 환경의 IT 인프라 수준, 예산을 고려해 단계적으로 또는 선별적으로 적용하는 방안을 제안한다. 예를 들어, 고위험 데이터에 대해서는 AES 암호화와 RBAC 은 필수적용 후 네트워크 분리, SIEM 은 단계적으로 도입한다. 중위험 데이터는 다중 인증은 필수로 적용하되 디바이스 특성이나 데이터 활용에 따라 데이터 암호화를 선택 적용한다. 저위험 데이터는 확인 시 최소 이중 인증을 통해 데이터를 확인하게 해 데이터 노출의 위험성을 최소화할 수 있도록 한다.

이와 같이 의료데이터의 민감도 및 위험도에 따른 차등화된 보안 정책과 기술 적용은 현실적 제약을 고려하면서도 개인정보 유출과 그로 인한 사회적 · 경제적 피해를 최소화하는 데 기여할 수 있을 것이다.

V. 결론

본 연구에서는 국내외 체외진단 의료기기 시장 및 현황과 사이버 보안 동향을 살펴보고, 실제 의료데이터 침해 사례와 관련 법·규제를 분석함으로써 의료데이터 보호의 필요성을 고찰했다. 의료 분야를 포함해 다른 산업분야에서 활용되는 보안 기술들을 의료데이터 보호에 어떻게 적용할 수 있는지 검토하고, 의료데이터의 민감도 및 위험도에 따라 분류하여 등급별 보안 방안을 제시했다.

체외진단 분야는 최근 기술의 발전과 시장의 성장으로 인해 진단뿐만 아니라 예방과 치료 단계에서도 다양한 의료데이터를 생성하고 있다. 이로 인해 의료데이터가 사이버 공격의 주요 표적이 되고 있으며, 침해 발생 시 금전적 손실과 개인의 프라이버시, 생명권에까지 영향을 미치는 심각한 피해가 발생할 수 있다. 특히 의료 정보는 타 산업에 비해 민감도가 높아, 암호화, 인증, 접근 제어, 네트워크 보안 등의 체계적인 보호 조치가 필수적이다.

본 연구에서는 체외진단기기에서 생성되는 의료데이터를 민감도 및 위험도 기준에 따라 저위험, 중위험, 고위험으로 등급화하고, 각 등급에 적합한 보안 기술(예: 이중/다중 인증, 암호화, RBAC, 네트워크 세분화, SIEM 등)을 제안하였다. 이 과정에서 의료기기의 등급 분류 체계를 참고하여, 데이터 보호에 있어서도 상대적 중요도에 따른 차등적 대응의 필요성을 강조하였다. 다만, 제안된 보안 기술들이 현실 의료 환경에 모두 일괄 적용되기 어려운 측면도 존재한다. 이에 따라 의료기관의 IT 인프라 수준, 예산, 사용 환경 등을 고려하여 핵심 보안 조치를 선별적으로 단계 적용하는 방법이 필요하다. 제시한 보안 방법과 같은 기술적 보호 조치뿐만 아니라 조직적 차원, 사용자의 대응도 중요하다. 정기적인 장비 보안 업데이트, 보안 인식 제고를 위한 교육, 내부 보안 정책 수립 등 사이버 보안에 대한 인식과 문화 정착이 병행되어야 한다.

본 연구는 체외진단 의료기기에서 생성되는 데이터의 보안 위협에 대응하기 위해 데이터 등급화 및 보안 기술 적용을 통해 대응 방안을 제시하였으며, 향후 체외진단

기술 성장과 함께 의료데이터 보호를 위한 맞춤형 규제나 보안에 기여해 피해 사례가 줄 수 있기를 기대한다.

참고 문헌

1. 한국바이오협회. 바이오경제연구센터. 2022. 글로벌 체외진단(IVD) 동향
2. Knowledge Sourcing Intelligence. 2024. 세계의 체외진단(IVD) 시장－예측 (2024－2029년)
3. Precedence Research. 2024. In Vitro Diagnostics Market Size to Hit USD 132.18 Billion by 2034
4. SUGENTECH, 한국IR협의회 기업리서치센터, 2024. “코로나19 수혜에서 벗어나 본업에 집중”
5. Allied Market Research. 2021. Global In-Vitro Diagnostics Market
6. 연구개발특구진흥재단. 2021. 유망시장 Issue Report 체외진단
7. 한국보건산업진흥원. 2024. 보건산업브리프 vol.414 『체외진단의료기기 산업 현황 및 전망
8. Emily Bonnie. (2025.01.03). Secureframe. 110+ of the Latest Data Breach Statistics [Updated 2025]. https://secureframe.com/blog/data-breach-statistics (검색일: 2025.04.15)
9. Kim Theodos. Scott Sitting. 2021. 『Health Information Privacy Laws in the Digital Age: HIPAA Doesn't Apply』. Perspect Health Information Management. 2020 Dec 7;18(Winter):1l. eCollection 2021 Winter
10. Steve Alder. (2024.12.30). “HHS Prposes Strengthened HIPAA Security Rule”. The HIPAA Journal. https://www.hipaajournal.com/hhs-strengthened-hipaa-security-rule/ (검색일: 2025.04.19)
11. Liam Johnson. (2025.01.09). “New HIPAA Regulations 2024-2025”. The HIPAA Guide. https://www.hipaaguide.net/new-hipaa-regulations/ (검색일:2025.04.19)
12. Errol Weiss. (2025.01.21). “Securing Health Data in 2025: The Rising Cybersecurity Challenges”. Health-ISAC . https://health-isac.org/securing-health-data-in-2025-the-rising-cybersecurity-challenges/ (검색일: 2025.04.02)
13. Allen R. Killworth . (2024.11.11). “HISAA: New Legislation Would Bring

Cybersecurity Requirements for HIPAA Covered Entities and Business Associates". Health Law Advisor
https://www.healthlawadvisor.com/hisaa-new-federal-legislation-introduced-that-would-create-significant-new-cybersecurity-requirements-for-hipaa-covered-entities-and-business-associates (검색일: 2025.04.15)

14. Steve Alder. (2024.07.14) "Consumer Health Information Privacy Protection Act Introduced in DC to Protect Non-HIPAA Health Data. HIPPA Journal.
https://www.hipaajournal.com/consumer-health-information-privacy-protection-act-district-columbia/ (검색일:2025.04.15)
15. 『PIPEDA fair informations principles』. 2024. Office of the Privacy Commissioner of Canada
16. 『Personal Health Information Protection Act. 2024』. Ontario e-Law
17. "Patient Privacy & Data Protection: Different laws around the world". (2021.01.31). BRAINLAB
https://www.brainlab.com/journal/patient-privacy-data-protection-different-laws-around-the-world/ (검색일: 2025.03.18)
18. THALES. "GDPR(일반 데이터 보호 규정)준수" .
https://cpl.thalesgroup.com/ko/compliance/gdpr-compliance (검색일: 2025-04-01)
19. 『2018 정보보호법(Data Protection Act 2018)』. 2018 (2024 개정. 세계법제정보센터
20. 『개인정보 보호법』 [시행 2025. 3. 13.] [법률 제19234호. 2023. 3. 14.. 일부개정]. 국가법령정보센터.
21. 세계법제정보센터. 『 개인정보보호에 관한 법률(個人情報の保護に関する法律)』(제16조-제59조). 2024
22. 『체외진단의료기기법』 제2조(정의) [시행 2025. 4. 1] [법률 제20900호. 2025. 4. 1., 일부개정]. 국가법령정보센터
23. 심의대상. 한국의료기기산업협회 의료기기광고심의위원회.
https://adv.kmdia.or.kr/ADV/_Document/Introduct/sub01_09.asp (검색일: 2025-03-15)

24. 이광제. 2024. “의료기기법의 의료기기 등급분류에 관한 법제 개선방안 연구”. 법제처
25. 『의료기기법 시행령』 [시행 2004.5.30.] [대통령령 제18401호. 2004.5.25., 제정]. [제정·개정이유]. 국가법령정보센터
26. 『보건의료기본법』 [시행 2024.8.7.] [법률 제20216호, 2024. 2.6. 일부개정] 제3조(정의). 국가법령정보센터
27. Art Gross. (2021.10.03). “PHI or PII? What’s the Difference?”. HIPAA Secure Now!. https://www.hipaasecurenow.com/phi-or-pii-whats-the-difference/ (검색일: 2025.05.07)
28. 송순종. 2024. 의료데이터의 안전한 활용을 위한 개인정보보호의 보안 기술에 관한 연구. 순천향대학교
29. Hannah T. Neprash. PhD; Claire C. McGlave. MPH; Dori A. Cross, PhD; Beth A. Virnig, PhD; Michael A. Puskarich, MD; Jared D. Huling, PhD; Alan Z. Rozenshtein, JD; Sayeh S. Nikpay, PhD. 2022. 『Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021』. JAMA Health Forum
30. Frontiers. Liat Wasserman, Yair Wasserman. 2022.『Hospital cybersecurity risks and gaps: Review (for the non-cyber professional)』. Front Digit Health
31. Steve Alder. 2025.“Healthcare Data Breach Statistics”. THE HIPPA JOURNAL. https://www.hipaajournal.com/healthcare-data-breach-statistics/ (검색일: 2025.04.07)
32. FederalRegister.gov website. 2024.“Health Breach Notification Rule”. https://www.federalregister.gov/documents/2024/05/30/2024-10855/health-breach-notification-rule (검색일: 2025.04.07)
33. 세계법제정보센터. (2025.03.21). “유럽연합, 『유럽건강데이터공간(EHDS) 규정』 채택”. https://world.moleg.go.kr/web/dta/lgslTrendReadPage.do?CTS_SEQ=54907&AST_SEQ=96&ETC=1 (검색일:2025.04.05)
34. ALLBRIGHT LAW OFFICES. “The Regulations on Network Data Security Management Released”. https://www.allbrightlaw.com/EN/10531/133d3b9110fe14da.aspx (검색일: 2025.04.02)

35. 『Personal Health Information Protection Act』. 2024. Ontario e-Law
36. 정준호, 김정숙, 2015,『u-헬스케어(Healthcare) 환경에 따른 의료 정보 보안 이슈』. 한국멀티미디어학회지 제19권 제3호
37. 최성호, 곽 진, 2015.『국외 의료기기 보안위협 사례 및 보안 동향 조사』. 정보보호학회지 제25권 제3호
38. 박의래, (2022.11.21).” 호주 건보사 해커, HIV 등 민감 정보 명단 잇따라 공개”. 연합뉴스. https://www.yna.co.kr/view/AKR20221121077700104?site=mapping_hyperlink (검색일: 2025.03.15)
39. 23andMe Blog. (2024.12.05) “Addressing Data Security Concerns – Action Plan”. https://blog.23andme.com/articles/addressing-data-security-concerns (검색일:2025.03.15)
40. European Data Protection Board(EU website). (2022.05.04). “Health data breach: Dedalus Biologie fined 1.5 million euros”. https://www.edpb.europa.eu/news/national-news/2022/health-data-breach-dedalus-biologie-fined-15-million-euros_en (검색일: 2025.03.15)
41. Steve Sabicer.2020. “Tandem Diabetes Care Announces Security Incident with Five Employee Email Accounts”. TANDEM Diabetes care
42. Steve Alder. (201910.14). “Philadelphia Department of Public Health Data Breach Exposed Data of Hepatitis Patients” .THE HIPPA JOURNAL https://www.hipaajournal.com/philadelphia-department-of-public-health-data-breach-exposed-hepatitis-patients-data/ (검색일:2025.03.15)
43. Alina BÎZGĂ. (2020.04.28). “Medical Information of 233,000 Individuals Exposed after Genetic Testing Lab Hack”. Bitdefender (검색일:2025.03.17)
44. Richard Console, Jr..(2025.01.02). “Northwest Asthma & Allergy Center Files Notice of November 2024 Data Breach”. JDSUPRA https://www.jdsupra.com/legalnews/northwest-asthma-allergy-center-files-6134535/(검색일:2025.03.15)
45. 23andMe.2023. Enhanced Customer Security at 23andMe with 2-Step Verification.

https://blog.23andme.com/articles/enhanced-customer-security-at-23andme-with-2-step-verification (검색일: 2025.03.15)

46. Bill Toulas. 2022. “Medical software firm fined €1.5M for leaking data of 490k patients”. BLEEPINGCOMPUTER. https://www.bleepingcomputer.com/news/security/medical-software-firm-fined-15m-for-leaking-data-of-490k-patients/ (검색일: 2025.03.15)
47. 『General Data Protection Regulation(GDPR)』. https://gdpr-info.eu/ (검색일:2025.03.17)
48. 유시온. (2024.10.17). “ [국감] EMR 사용인증 의료기관 12%”. 후생신보. https://www.whosaeng.com/155776 (검색일: 2025.05.04)
49. 권선정. (202401.10). 보도자료 “개인정보위-보건복지부 협력 통해 의료기관의 개인정보 보호 강화 나선다!”. 개인정보위원회. https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=9845 (검색일: 2025-05-28)
50. 이슬비. (2021.06.10). “전자의무기록(EMR) 병ㆍ의원 '랜섬웨어' 공격 빈발”. Dailymedi. https://dailymedi.com/news/news_view.php?wr_id=870453 (검색일: 2025.05.07)
51. Joachim Ott. (2025.02.25). “Technologies for maximum cybersecurity in medical technology”. COMPAMED. https://www.compamed-tradefair.com/en/it-in-tech/cybersecurity-medical-technologies (검색일: 2025.04.07)
52. 삼정KPMG 경제연구원. 2018. “스마트 헬스케어의 시대, 데이터 전쟁을 대비하라”. 제94호 삼정KPMG
53. Team DigitalDefynd. “Top 10 Healthcare Cybersecurity Case Studies [2025]”. DigitalDefynd. https://digitaldefynd.com/IQ/healthcare-cybersecurity-case-studies/ (검색일:2025.04.15)
54. V500 systems. (2018.06.20) . Article “The Case for Multi-Factor Authentication that stops almost 100% automated attacks” . https://www.v500.com/mfa-for-users/ (검색일: 2025.04.07)

55. SailPoint. (2024.12.27). Article “ What is multi-factor authentication (MFA)? ”. https://www.sailpoint.com/ko/identity-library/what-is-multi-factor-authentication?elqct=websiteelqchannel%3Dorganicdirect. (검색일: 2025.04.07)
56. 정보통신산업진흥원. 2024, 품목별 ICT 시장동향 생체인식.
57. Silverfort. Article “ Adaptive Authentication” . https://www.silverfort.com/glossary/adaptive-authentication/ (검색일: 2025.04.07)
58. SECUREAUTH. 2024. “Importance of Adaptive Authentication in Financial Services”. https://www.secureauth.com/resources/importance-of-adaptive-authentication-in-financial-services/ (검색일: 2025.04.07)
59. Edward Robin. (2023.09.03). “How Do Banks Encrypt Data? ”. NewSoftwares.net https://www.newsoftwares.net/blog/how-do-banks-encrypt-data/ (검색일:2025.03.28)
60. Marcelo Antonio de Carvalho Junior, Paulo Bandiera-Paiva. 2018. 『Health Information System Role-Based Access Control Current Security Trends and Challenges, J Healthc Eng. 2018 Feb 19:2018:6510249. doi: 10.1155/2018/6510249
61. 송제민, 김명식, 정경지, 신문선. 2014. 『RBAC에 기반한 개인 맞춤형 건강정보 제공 헬스케어 서비스 플랫폼』. Journal of the Korea Academia-Industrial cooperation Society Vol. 15, No. 3 pp. 1740-1748.
62. 임경숙, 김점구. 2016. 『의료정보시스템의 RBAC 프로토콜 연구』. 융합보안논문지 제 16 권 제 7 호 (2016. 12)
63. SECURIUM SOLUTIONS. SECURITY INCIDENT EVENT MANAGEMENT (SIEM SECURITY). https://securiumsolutions.com/security-incident-event-management-siem-security/ (검색일: 2025.04.15)
64. Kayode Sheriffdeen. 2024. 『The Role of Network Segmentation in Enhancing Data Privacy and Meeting Security Standards』. EasyChair Preprint
65. 법령. 보험업법. 시행 2025.1.31.『법률 제 20436 호, 2024.09.29., 타법개정』

ABSTRACT

Study on Classification and Protection Measures of In Vitro Diagnostics Medical Data for Cybersecurity Enhancement

Na Gyong Lee
Department of Medical Device Engineering and Management
The Graduate School, Yonsei University

(Directed by Seung Hwan Han, M.D., Ph.D.)

The rapid advancement of technologies such as artificial intelligence (AI), the Internet of Things (IoT), and telemedicine has accelerated the growth of the in vitro diagnostics (IVD) market and has significantly increased both the volume and complexity of medical data. However, these technological developments have also heightened cybersecurity risks, particularly in the healthcare sector, which has experienced one of the highest rates of data breaches among all industries in recent years. IVD medical devices generate highly sensitive information, including genetic data and infectious disease test results, which, if compromised, could seriously impact patient safety and public trust.

This study aims to classify medical data generated in the IVD field according to sensitivity and risk level, and to propose differentiated security measures tailored to each category. To achieve this, the current status of medical data cybersecurity was reviewed both domestically and internationally, and relevant regulatory standards such as the General Data Protection Regulation (GDPR), the

Health Insurance Portability and Accountability Act (HIPAA), and Korea's Personal Information Protection Act (PIPA) were analyzed. In addition, real-world cybersecurity incidents were investigated and best practices from other industries were examined.

Based on this analysis, IVD medical data were categorized into high-risk, medium-risk, and low-risk groups. For each category, appropriate security measures—such as encryption, multi-factor authentication, role-based access control, and network segmentation—were proposed. The findings of this study are expected to help minimize the risk of data breaches and tampering in the IVD sector and to contribute to the development of more robust security policies in healthcare institutions. Ultimately, it is hoped that the proposed framework will enhance patient safety and strengthen the reliability of healthcare services.

Key words: In Vitro Diagnostics, Medical Data, Cybersecurity