https://doi.org/10.7840/kics.2022.47.11.1908

안전한 전자의무기록 관리 및 보존을 위한 법·제도 개정 제안

이 인 혜•, 진 정 하°

Proposal of Law Amendment for Secure Management and Preservation of EMR

In Hye Lee•, Jungha Jin°

요 약

ICT 기술의 발달에 따라 전자의무기록을 중심으로 한 기술적 및 법규적 적용 환경이 급격하게 변화하는 가운데, 현행 의료법 제23조와 그 하위 법령인 의료법 시행규칙과 그에 따른 기준들은 2016년 최종 개정된 이후 현재까지 적용되고 있는 현실이다. 그러나 2020년부터 전자의무기록시스템 인증제가 본격적으로 시행됨에 따라 의료산업계에서 전자의무기록시스템에 대한 구체적인 법안 적용과 해석에 대한 문제가 제기되고 있다. 이에 따라 본 논문에서는 기존에 '시설과 장비'로 국한된 규정의 범위를 '의료정보와 관련된 모든 보안 요구사항'을 포함하도록 확장하고, 의료기관 내부 보관과 외부보관을 구분하여 규정하고 있는 기준을 개인정보보호법이나 ISMS-P 등 타 법규에 부합하도록 통합하여 개정할 것을 제안한다. 상기와 같은 방안으로 보안성을 확보하기 위하여 향후 위험분석을 통해 의료정보 및 정보시스템을 위험도에 따라 분류할 필요성이 존재한다. 위험분석 기반으로 분류된 의료정보 및 정보시스템의 등급에 따라 정보보안 정책을 적용한다면 법규의 효율성과 효과성을 확보하면서 의료 IT 분야 전반에 일관성 있는 심층 보안을 제공할 수 있을 것으로 기대한다.

키워드 : 전자의무기록, 안전한 전자의무기록 관리 및 보존, 전자의무기록시스템 보안
Key Words : EMR, EMR systems, cybersecurity of EMR systems

ABSTRACT

With the development of ICT technology, the technological and legal application environment centered on Electronic Medical Record(EMR) is rapidly changing, but the current Article 23 of the Medical Act and its subordinate statutes such as the Enforcement Regulations of the Medical Act that have been revised in 2016 are still maintained. As the EMR system certification begins in earnest in 2020, the gap between these regulations and reality is raising questions about the specific application and interpretation of the regulations. Therefore, in this paper, it is proposed to expand the scope of regulations that were previously limited to 'facilities and equipment' to 'all security requirements related to medical information'. In addition, it is

※ 본 연구는 정부(과학기술정보통신부, 산업통상자원부, 보건복지부, 식품의약품안전처)의 재원으로 범부처전주기의료기기연구개발사업단의 지원을 받아 수행된 연구임(1711138615, KMDF_PR_20200901_0272)
• First Author : KOREA University School of Cybersecurity Institute of Cyber Security & Privacy, ihlee5937@gmail.com, 정회원
° Corresponding Author : KOREA University School of Cybersecurity Institute of Cyber Security & Privacy, nemoda75@korea.ac.kr, 종신회원
논문번호 : 202208-183-0-SE, Received August 15, 2022; Revised September 23, 2022; Accepted September 27, 2022

recommended to integrate and revise the regulations that separately stipulate the internal and external preservation of EMR in accordance with other regulations such as the Personal Information Protection Act and ISMS-P. The next step is to classify medical information and information systems based on the risk analysis to ensure consistent security of EMR under the Medical regulations. By establishing security countermeasures for medical information and information systems according to the levels of security, it is expected to provide consistent and in-depth security in the medical IT domain.

Ⅰ. 서 론

정보통신기술을 활용한 효율성 확보를 위하여 병원 환경에서 사용되던 의무기록들이 전자문서 형태로 보관 및 저장되어 관리되고 있다. 이러한 ICT 기술의 발달에 따라 전자의무기록을 중심으로 한 기술적 및 법규적 적용 환경이 급격하게 변화하는 현실에서 현행 의료법 제23조와 그 하위 규정인 의료법 시행규칙과 그에 따른 기준들은 2016년 최종 개정된 이후 현재까지 적용되고 있다. 특히, 2020년부터 시범 운영된 후 2022년 현재 본격적으로 시행되고 있는 '전자의무기록시스템 인증제'의 보안성 인증기준은 해당 법령을 근거로 규정되어 있다. 하지만 이러한 기존의 규정이나 기준이 현재의 정보보호 현황이나 의료계 현실과 맞지 않는 부분들이 다수 존재하여 전자의무기록시스템 인증기준에 대한 구체적인 법안 적용과 해석에서 다양한 이슈가 제기되고 있다.[1] 이에 따라 본 논문에서는 기존의 규정 및 기준에서 '시설과 장비'로 국한된 규정의 범위를 '의료정보와 관련된 모든 보안 요구사항'으로 확장하는 방안을 제시하고자 한다.

또한, 의료기관 내부와 외부에 보관하는 의무기록을 구분하여 적용함으로써 발생하는 기존 법령과 개인정보보호법이나 ISMS-P 등 타 규정과의 문제점을 고려하고, 의료정보 및 정보시스템에 대한 의료법 상 모든 정보보안 관련 규정에 일관성 있게 적용하는 방식의 대응 방안을 제안하고자 한다.

본 논문은 1장의 서론에 이어, 2장의 전자의무기록에 대한 정의 및 국외 사례를 포함하는 법규적 환경에 대한 분석을 수행하고, 3장의 법규 적용 범위에 대한 개정 방안, 4장의 안전한 전자의무기록 관리·보존을 위한 내부 및 외부 보관 기준 개정 방안, 그리고 5장의 결론으로 구성하였다.

Ⅱ. 국내 환경 분석 및 국외 동향

2.1 전자의무기록의 정의

전자의무기록은 의료법 제22조의 '진료기록부 등'에 전자서명법에 따른 전자서명을 기재한 전자문서이다[2]. 즉, 의료법에서 규정한 전자의무기록의 구성 요건은 진료기록부 등, 전자문서, 전자서명이라고 할 수 있다. 진료기록부 등은 환자와 관련된 의료인이 의료행위 전반에 걸쳐 환자 진료시마다 의료법 시행규칙 제14조에 규정된 사항뿐만 아니라 환자에 대한 주된 증상, 진단 및 치료에 대한 내용 등을 포함한 광범위한 기록이다. 진료기록부 등에 포함되는 기록은 진료기록부, 조산기록부, 간호기록부, 그 밖의 진료에 관한 기록이며, 이와 같은 기록에 추가 기재하거나 수정하여 추가 기재한 기록, 추가 기재 또는 수정하기 전의 원본을 모두 포함한다[3-5].

전자문서란 정보처리시스템에 의하여 전자적 형태로 작성되어 송신 또는 수신되거나 저장된 정보이다[6]. 전자문서로 기록된 의무기록은 단순히 종이 문서의 형태인 의무기록을 대체함으로써 얻을 수 있는 비용절감과 효율성의 실익을 넘어 진료의 질을 향상시키고[7] 의료 빅데이터 활용과 정밀의료, 의료 마이데이터 도입과 같은 첨단 의료 정보산업으로의 확산을 가능하게 한다.

의료법은 기존의 종이 형태의 진료기록부 등의 유효성을 확보하기 위한 수단으로 의료인의 서명을 의무화했던 것과 같은 맥락으로 전자의무기록의 유효성을 증명하기 위해 전자서명을 이용하도록 규정하고 있다[2,4]. 그러나, 비교적 위조와 변조가 용이한 전자문서에서의 전자서명은 단순히 유효성 확보를 위한 수단 뿐만 아니라 전자의무기록의 원본성과 무결성, 책임추적성과 같은 추가적인 법률적 쟁점을 해소하기 위한 효과적인 도구라고 볼 수 있다[3,7,8].

2.2 전자의무기록의 법규적 환경

전산정보처리시스템인 전자의무기록시스템을 통하여 생성·보관·전송·활용·관리되는[9] 전자의무기록은 디지털 산업이 제공하는 편익의 반대급부로 수반되는 개인정보 침해와 사이버보안 위험성에 노출되어 있다[10]. 종이형태의 진료기록부 등이 보안성 확보를 위해 의료진의 허위 진단서 작성, 도난, 폐업이나 재난에

의한 기록의 망실과 같은 물리적 침해만을 고려했다면, 전자의무기록 사용 현장에서는 원격지로부터 네트워크를 통해 의료정보 시스템에 침입하여 정보를 조작하거나 탈취하고 랜섬웨어를 통해 금품을 갈취하거나 침입한 시스템을 타고 제3의 유관기관 정보시스템에 침입하는 등 광범위하고 다양한 피해를 고민해야 한다[11].

전자의무기록의 태생적 보안 취약점을 고려하여 2002년 3월 30일 의료법은 전자의무기록에 대한 규정을 신설하면서 전자의무기록의 효율성과 안전성, 신뢰성 확보를 위한 시설과 장비(2002), 전자의무기록의 표준화와 전자의무기록 시스템 인증(2016), 진료정보 침해사고에 대한 예방과 대응 방안(2019) 등을 규정하였다[9,12,13]. 특히 2003년 10월 1일 신설되어 개정된 의료법 시행규칙 제16조(2016. 2), 이의 하위 법령으로 규정된 전자의무기록 관리·보존에 필요한 시설과 장비에 관한 기준 및 의료기관 외의 장소에 전자의무기록 보관시 필요한 추가적인 조치(2016. 8)들은 디지털 전환기의 의료정보산업 육성에 따른 사이버침해 증가에 대비하고 국민의 주요 의료정보 및 개인정보를 보호하기 위한 선제적 방안으로 마련되었다[14-16].

또한 전자의무기록 및 전자의무기록 시스템을 둘러싼 법규적 환경 변화는 급격하게 이루어지고 있다. 2015년 12월 1일 개정된 정보통신망 이용촉진 및 정보보호 등에 관한 법률에서 ISMS 인증 대상을 명시하여 상급종합병원이 의무 도입 기관이 됨으로써 전자의무기록시스템을 비롯한 병원정보시스템의 보안성 확보 문제는 시급한 해결과제가 되었다[17]. 이와 함께 정부의 각 부처별로 분산되어 처리되어 왔던 개인정보보호 관련 업무가 2020년 8월 중앙행정기관으로 승격된 개인정보보호위원회로 이관되어 일원화되었고 유럽연합의 GDPR 기조에 따라 국내 개인정보보호법이 점차 강화되고 있다.

한편, 2020년부터 전자의무기록시스템 인증제가 본격 시행됨에 따라 의료법 상 규정하고 있는 보안성 확보 방안에 대한 실질적인 해석과 적용이 의료정보 산업 부문의 중요한 화두가 되었다. 특히 전자의무기록시스템 인증기준[18] 중 전자의무기록의 외부보관에 대한 인증기준인 S014는 전자의무기록 관리·보존에 필요한 시설과 장비에 관한 기준 및 의료기관 외의 장소에 전자의무기록 보관시 필요한 추가적인 조치, 클라우드 컴퓨팅서비스 정보보호에 관한 기준[19] 등 광범위한 내용을 포괄하고 있는 항목으로 그 실효성과 적절성에 대한 논란이 제기되고 있다.

2.3 국외 동향

미국의 경우 2009에 제정된 HITECH Act를 통해 전자의무기록시스템의 전국적인 확산에 결정적인 계기가 되었으며, 이 법을 근거로 EHR(Electronic Health Record)을 병원 또는 의료인에게 인센티브와 페널티를 동시에 제공하며 사용하도록 독려하여 사용자들의 의미있는 참여를 유도하였고, 미국 보건부 산하 국립건강정보기술조정위원장실(ONC, Office of the National Coordinator for Health Information Technology)이 건강 관련 IT 기술과 관련한 자율적 인증프로그램을 도입할 것을 요구하고 있다[20]. 인증기능을 포함하는 EHR 기술의 장점으로는 대부분의 인증요건이 데이터의 상호운용성 및 기밀성과 보안성을 보장하는 절차를 가능하게 하는 데에 초점이 맞추어져 있다는 점이다. ONC의 건강 관련 IT 기술 인증프로그램에 따라 인증을 받은 모든 EHR 기술은 개인의 건강정보에 관한 특정 프라이버시 보호 및 보안 요건을 충족하도록 법률 규정을 마련하고 있다[21]. 미국의 ONC 에서는 ONC 건강정보 기술 인증프로그램에서 보다 광의의 health IT란 개념을 도입하여 EHR 및 건강 IT의 종류를 포함하고 있다[22]. 또한, 미국은 의료와 관련된 개인정보보호를 위하여 1996년 연방의회에서 제정된 '의료보험의 이전과 그에 수반하는 책임에 관한 법률(HIPAA, Health Insurance Portability and Accountability Act)'을 제정하였으며, 이러한 HIPAA 프라이버시 규칙(HIPAA Privacy Rule)에서는 종이기반 형태를 포함하는 전자적 형태에 모두 적용되고 있어서 환자의 미래 기대치까지를 포함하는 식별 가능한 건강정보 등에 대한 보호를 의무화 시키고 있다[23]. 특히, HIPAA에서 제시하고 있는 다양한 개인정보보호 및 보안 요구사항에 대한 변경 사항을 HITECH 법에 부합시키고 있는 추세이다.

영국의 보건 및 사회복지법(Health and Social Care Act)은 국가보건의료서비스법(National Health Service Act 1946)에 의해 1948년에 설립된 영국 국가보건의료서비스(NHS) 전체에 영향을 미치는 법으로서 특히 일반의(GP, General Practitioner)에 대한 권한을 부여하는 법률이다. 이 법률에 근거하여 영국 보건의료정보 담당기구인 NHS Digital은 2016년 보건의료정보 관련하여 설립된 전담기구로서 주로 보건의료정보 인프라 구축, 보건의료데이터 수집 및 활용, 정보보안과 관련된 일을 수행한다. 특히 보건의료정보 인프라인 NHS Spine은 GP 진료소의 시스템을 통해 전자의무기록이 자동으로 생성하여 업로드 시키고, 이를 통해 시스템의 엑세스 권한을 부여 받은 다른 지역

보건의료인의 접근이 가능하다. 보건의료정보 보안센터(Data Security Centre)를 운영하여 보건의료기관에 대한 데이터 및 사이버 보안에 대응하도록 보안정책 및 지침에 대한 교육을 제공하고 있다.

상기와 같이 미국과 영국의 동향을 살펴보면 개인정보보호 및 특수범주의 정보를 목적으로 데이터 보안을 유지하기 위해 사이버 공간에서의 관리적 조치, 물리적 조치, 기술적 조치에 대한 보안을 규정하고 있음을 확인할 수 있다. 정보에 대하여 전송 및 보존에서의 기밀성과 무결성, 가용성을 보호하기 위한 관리적, 물리적, 기술 안전적 수행을 제공하고 있다. 어느 국가에서든지 기본원칙을 제시하는 개인정보보호 법률이 있고, 특수범주의 정보로서 의료정보에 관한 보호 법률을 별도로 제정하여 의료정보 보호를 더욱 강화하고 있음을 확인할 수 있다.

Ⅲ. 법규 적용 범위에 대한 개정 방안

전자의무기록의 안전한 관리 및 보존을 위한 규정의 범위를 '시설과 장비'로 한정함으로써 발생하는 법규적 이슈로 인한 문제가 다수임에 따라서 이를 살펴보고 개정 방안을 다음과 같이 제시하고자 한다.

3.1 의료법 제23조 제2항의 시설과 장비

동 조항에 따르면 전자의무기록을 관리· 보존하는 전자의무기록시스템의 기능을 '안전하게' 수행하는 '시설과 장비'를 갖추도록 규정하고 있고, 이와 연계된 하위 규정인 의료법 시행규칙 제16조와 전자의무기록의 관리·보존에 필요한 시설과 장비에 관한 기준 등에서 '시설과 장비'의 관점으로 법률적 정보보호 요구사항을 규정하고 있다. 다음의 표 1은 개인정보보호법 시행령과 의료법 시행규칙에서 다루고 있는 내용을 비교하여 나타내고 있다.

정보통신기술이 혁신적으로 발전하고 다양한 형태의 서비스가 개발되고 있는 현재의 산업동향을 고려하여 물리적인 의미를 함축하는 '시설과 장비'라는 용어로 인해 기술적 적용의 한계가 존재할 가능성이 크다. 또한, 개인정보의 안전성 확보 조치 기준[24], 개인정보의 안전성 확보 조치 기준에 관한 특례[25] 등 관련 타법의 규정에서 통상적으로 '시설과 장비'를 적시하는 것 보다는 요구사항 중심으로 포괄적으로 규정하여 각 조항의 궁극적인 목적 달성을 위한 다양한 형태의 수단을 융통성 있게 허용하고 있는 점에 착안하여 다음의 표 2와 같이 의료법 시행규칙 제16조에 대하여 개정하는 방안을 제시하고자 한다.

표 1 의료 시설과 장비에 대한 타법과의 비교
Table 1. Comparison with the Personal Information Protection Act

Enforcement Rules of the Medical Service Act	Enforcement Decree of the Personal Information Protection Act
1. Equipment that can generate and store EMRs and verify electronic signatures	1. To formulate and implement an internal management plan for the safe processing of personal information;
2. Equipment necessary for the history management of EMRs, such as checking whether the EMRs have been changed after electronic signatures have been issued	2. To control access to personal information and restrict the authority to access personal information;
3. Backup storage equipment for EMRs	3. To adopt encryption technology to safely store and transmit personal information and other equivalent measures;
4. Network security facilities and equipment(It shall be limited to cases where equipment referred to in subparagraphs 1 through 3 is connected to wired and wireless Internet)	4. To retain login records to respond to incidents of infringement with respect to personal information and to take measures to prevent the forgery and falsification thereof;
5. Facilities and Equipment for EMRs System Security(It refers to a system in which servers, software, and databases related to the management and preservation of EMRs are electronically organized. be the same in this section below)	5. To install and upgrade security programs to protect personal information;
6. Physical access prevention facilities and equipment that fall under any of the following items to EMRs preservation sites: A. Controlled facilities such as access control areas B. Locking device	6. To take physical measures, such as a storage or locking system, to keep personal information securely
7. Where EMR storage equipment under subparagraph 1 or backup storage equipment under subparagraph 3 is installed in a place other than a medical institution (including a place where subsidiary business is conducted pursuant to Article 49 of the Medical Service Act), the following facilities and equipment: A. Facilities and equipment to check the operation and condition of the EMRs system in real time B. Spare equipment that can replace the equipment under subparagraphs 1 and 2 in the event of a failure of the EMRs system C. surveillance equipment such as CCTV(closed-circuit television) D. Disaster prevention facilities	

표 2. 시설과 장비에 대한 의료법 시행규칙 개정 방안
Table 2. Proposed amendment of the Enforcement Rules of the Medical Service Act on Facilities and Equipment

Current	Proposed Amendment
Article 16 (Facilities, Equipment, etc. Required for the Management and Preservation of EMR) (1) Medical personnel or founders of medical institutions shall be equipped with facilities and equipment necessary to safely manage and preserve EMR, as prescribed by Ordinance of the Ministry of Health and Welfare.	Article 16 (Facilities, Equipment, etc. Required for the Management and Preservation of EMR) (1) ---------- shall endeavor to safely manage and preserve EMR, ----------

3.2 의료법 제23조의2 시설과 장비

전자의무기록의 표준화 등을 규정한 동 조항의 제1항은 보건복지부장관이 전자의무기록 시스템, 시설, 장비 및 기록 서식 등에 관한 표준을 정하여 고시하도록 규정하고 있고 동 규정에 의하여 고시하도록 위임된 행정규칙은 전자의무기록의 관리·보존에 필요한 시설과 장비에 관한 기준과 연결되어 있다. 제2항과 제3항은 '전자의무기록시스템 인증기준'에 대한 내용을 포함하고 있어서, 동 조항의 맥락을 전체적으로 살펴보면 제1항에서 위임된 고시가 전자의무기록의 관리·보존에 필요한 시설과 장비에 관한 기준으로 규정된 것은 '전산정보시스템, 시설, 장비 및 기록 서식 등'에 대하여 전체적으로 포함하도록 한 본 규정의 취지 중 일부만을 포함하고 있다고 판단된다. 특히, 제2항에서 '제1항에 따른 표준, 전자의무기록 시스템 간 호환성, 정보보안 등'에 대한 인증기준을 언급하고 있음에 따라 동 조항은 전자의무기록시스템 인증제의 인증기준을 규정하기 위한 목적으로 해석되고 동 항은 '전자의무기록 시스템의 기능성·상호운용성·보안성' 인증기준 모두를 포함한 행정규칙과 연결하는 것이 적절하지만 현행법에서는 적절한 행정규칙이 규정되어 있지 않는 문제가 존재한다. 그리고 동 조항의 제2항에서 규정한 '보건복지부장관이 정한 표준'과 '대통령령으로 정하는 인증기준'에 대한 법규적 체계를 검토할 필요가 있는데 이는 동 조항의 제1항의 규정이 모호하고 적절하지 않아 발생한 부정합으로 판단된다.

상기 표 3에서는 일부 조문에 대하여 개정한 방안을 제시하고 있으며, 추가적으로 제시하는 개정안에 부합하도록 의료법 시행령 제10조의7 제1항[25]에서 명시하고 있는 전자의무기록시스템의 인증 기준에 대하여 전자의무기록시스템의 기능성 및 상호운용성, 그리고 보안성에 대한 인증 기준을 중점적으로 다루도록 개정하여 법과 시행령을 일치시켜야 할 것으로 판단된다.

표 3. 의료법 중 표준 고시 개정안
Table 3. Proposed amendment of Notification in Medical Service ACT

Current	Proposed Amendment
Article 23-2 (Standardization of EMR System) (1) For the purpose of the efficient and unified management and use of EMRs, the Minister of Health and Welfare may determine and publicly notify the standards concerning a computerized information processing system (hereafter referred to as "EMR system" in this Article), facilities, equipment, forms of records, etc. necessary to prepare, manage and preserve records, and recommend manufacturers and suppliers of the EMR system, medical personnel or founders of medical institutions to comply with such standards. (2) The Minister of Health and Welfare may certify an EMR system, if it meets the criteria for certification prescribed by Presidential Decree, such as the standards referred to in paragraph (1), compatibility among EMR systems and security of data.	Article 23-2 (Standardization of EMR System) (1) ---------- ---------- shall be related to computerized information processing system may set and announce standards for functionality, interoperability, and security, etc. (hereafter referred to as "EMR system" in this Article) necessary to prepare, manage and preserve records, and recommend manufacturers and suppliers of the EMR system, medical personnel or founders of medical institutions to comply with such standards. (2) ---------- ---------- grant certification prescribed by Presidential Decree if the EMR system conforms to the standards under paragraph (1).

3.3 의료법 시행규칙 제16조 시설과 장비

의료법 시행규칙 제16조는 앞선 1절에서 시설과 장비에 대하여 개인정보보호법과의 비교에서 잠시 살펴보았다. 동 조항의 제목은 '전자의무기록의 관리·보존에 필요한 시설과 장비 등'이다. 따라서, 앞선 2절에서 기능성 및 상호운용성, 그리고 보안성을 기반으로 인증을 부여하는 내용으로 관련 조항을 수정함에 있어서 본 조항 또한 '전자의무기록 관리·보존의 안전성 확보 조치'로 개정하여 전자의무 기록의 보안성을 목적으로 하는 규정임을 명확히 하고, 그에 부합하도록 조항의 내용을 개정할 필요가 있다고 판단된다. 이와 같은 제목의 변경은 개인정보보호법 상 개인정보보호의 안전성 확보조치 기준[24]과 궁극적인 목적과 형식의 일관성을 확보할 수 있다는 장점도 있다.

또한 '시설과 장비'라는 용어의 한계를 극복하고 '전자의무기록의 보안성 확보'라는 목적을 명확히 하고 정비한다면, 의료법 시행령 제10조의5[27]의 위임규칙으로서 연계하는 등 동 법규의 적용성을 확장할 수 있다.

한편, 동 조항에서 의미하는 '시설과 장비'의 범주

적 특성을 검토해 보면, 전자의무기록시스템 인증기준의 다른 기준을 준용하고 있어 관련자들에게 혼란을 야기하고 있다. 즉, 동 조 제1항에서는 '전자의무기록의 생성·저장과 전자서명을 검증할 수 있는 장비'와 '전자서명이 있은 후 전자의무기록의 변경 여부 확인 등 전자의무기록의 이력관리를 위하여 필요한 장비'를 제1호와 제2호에 각각 규정하고 있다.

그러나 제1호와 제2호의 장비 혹은 기능은 '전자의무기록시스템'이 기본적으로 갖추어야 할 기능적 요소이다. 전자의무기록 시스템 인증기준의 관점에서는 '기능성 인증기준'에 적합한 항목인 것이다. 진료기록부등의 전자적 형태인 전자의무기록시스템은 본질적으로 전자의무기록을 생성 및 저장할 수 있어야 하며, 생성된 전자의무기록에 대하여 전자서명을 해야 하고, 추가적인 기재나 수정 시 전자서명을 함으로써 전자의무기록 변경 증적을 남기고 무결성을 입증하는 기능을 제공해야하기 때문이다. 이에 반해, 제3호부터 7호까지의 장비 혹은 기능은 '안전하게' 전자의무기록을 관리· 보존하는 것과 관련된 장비 혹은 기능으로 전자의무기록시스템의 인증기준 중 보안성 요구사항을 포함하고 있다. 즉, 동 조항에서 전자의무기록시스템의 인증 기준과 관련된 항목을 범주의 일관성 없이 혼용함으로써 본 조항의 목적을 명확히 제시하지 못하고 혼란을 발생시키고 있다.

- 제1호와 제2호: 기능성 인증기준의 요구사항 해당
- 제3호: 보안성 인증기준에 포함되는 항목
- 제5호: 보안성 인증기준 적시
- 상호운용성 인증기준은 포함되지 않음

이에 따라, 제1호와 제2호는 삭제함으로써 동 조항

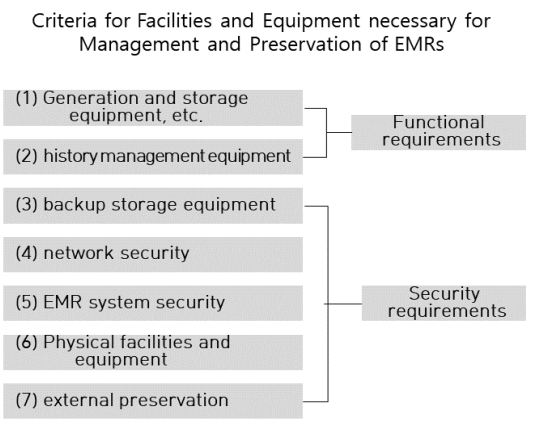

그림 1. 의료법 시행규칙 제16조 요구사항의 범주
Fig 1. Classification of Enforcement Rules of the Medical Act, Article 16

의 목적성을 명확히 하고 제1호의 '전자서명을 검증할 수 있는 장비'는 전자서명에 대한 요구사항을 별도의 항목 또는 적절한 범주의 하위에 규정함으로써 전자서명의 신뢰성을 확보할 수 있도록 하는 것이 적절하다고 판단된다. 이와 같은 맥락으로 의료법 시행규칙 제16조 제1항의 제1호 및 제2호는 삭제를 통해 개정하는 것이 바람직하다고 판단된다.

3.4 전자의무기록의 관리·보존에 필요한 시설과 장비에 관한 기준의 시설과 장비

상기 제시된 개정사항에 부합하도록 본 기준의 제목을 '전자의무기록 관리·보존의 보안성 확보 조치 기준'으로 변경하는 것을 제안한다. 또한 '시설과 장비'를 적시한 기준 항목들을 보안성 요구사항으로 정비함으로써 해당 기준의 목적을 명확히 하고 향후 개발될 수도 있는 어떠한 종류 및 형태의 혁신적 기술 수단도 수용할 수 있도록 가능성을 열어두는 것이 바람직하다고 판단된다. 따라서 다음과 같이 기준 고시의 제목에 대한 개정안을 제시한다.

표 4. 기준 고시 제목 개정안
Table 4. Proposed amendment of the title of the Public Notice

Current	Proposed Amendment
Criteria for facilities and equipment necessary for the management and preservation of EMR	Criteria for measures to ensure security of the management and preservation of EMR

Ⅳ. 안전한 전자의무기록 관리·보존을 위한 내부 및 외부 보관 기준 개정 방안

안전한 전자의무기록의 관리·보존을 위한 내부 및 외부 보관 기준이 구분되어 있는 현 규정을 타 법규의 현황과 비교하여 내·외부 구분의 타당성을 검토하고 개선안을 마련할 필요가 있을 것으로 판단된다. 특히 클라우드 환경의 급격한 발전 및 의료 산업계에 적용되어 사용됨에 따라 전자의무기록의 외부보관에서의 안전한 보관에 대한 법적 근거 마련이 다소 미흡한 현실이다.

4.1 의료기관 외의 장소에 전자의무기록 보관시 필요한 추가적인 조치

전자의무기록 관리·보존에 필요한 시설과 장비에 관한 기준 제7조에 '의료기관 외의 장소 관리·보존시 추가적 조치'를 규정하고 포함되는 별표의 '의료기관 외의 장소에 전자의무기록 보관시 필요한 추가적인

조치'에서 세부적으로 규정함으로써 물리적으로 전자의무기록을 의료기관 내부에 보관하는 경우와 외부에 보관하는 경우를 구분하고 있다는 것을 나타낸다. 추가적인 조치 기준이 제시되었던 당시는 국내에서 ISMS도 본격적으로 시행되기 이전으로 기관들의 보안에 대한 인식 및 수준이 현재에 비해 매우 낮은 상황이었다. 따라서 법규로서의 요구사항도 구체적인 적시와 최소한의 가이드라인을 제시하고자 하는 노력을 엿볼 수 있다. 특히, 동 기준의 제정 당시 진료기록부 등 의료정보를 의료기관 외부에 보관하지 못하도록 한 규제를 완화하려는 명확한 목적이 존재하는 바, 타 법이나 타 인증기준에서 일반적으로 적용되고 있는 기준이 동 규정에서 '외부 보관'이라는 표식을 달고 규정되고 있어 상호간의 부합되지 않는 부분이 존재하는 문제가 발생된다. 또한 기관의 내·외부와 관계없이 준수되어야 하는 기준이 의료부문에서는 외부보관 기준으로 적시됨으로써 일명 '내부보관'의 면죄부가 될 위험성도 존재한다.

4.2 전자의무기록 외부 보관에 대한 개선 방안

앞서 설명한 전자의무기록 관리·보존에 필요한 시설과 장비에 관한 기준 고시 제정 당시인 2016년과 현재를 비교해보았을 때 정부에서는 ISMS-P나 CSAP, 개인정보 영향평가 등 공공과 민간부문에 대한 다양한 제도적 장치를 도입하여 보안수준 향상을 위하여 노력해왔고 그 결과 의료보안 수준은 현재 괄목할 만한 성장을 이루고 있다. 이러한 부분이 현재 시점에서의 동 기준에서의 추가적인 조치 요구사항의 존속 이유를 찾기 어려운 점이 존재한다. 다음의 표 5에서는 전자의무기록의 외부보관에서의 추가적인 조치 요구사항과 ISMS-P와 CSAP의 요구사항을 비교하여 나타내고 있다.

표 5. 외부보관 요구사항과 ISMS-P, CSAP 요구사항
Table 5. Requirements comparison of the external preservation of EMR, ISMS and CSAP

The external preservation		ISMS-P	CSAP
Backup storage for EMR	Nondisruptive backup of the system	2.9.3	6.2.2
	Backup data recovery		
	Prevent forgery and tampering of backup data		
	Physical separation of backup facilities		
Facilities and equipment for	Configuring a Redundant Network	2.9.2	6.2.2
network security	Network Protection System	2.10.1, 2.11.3	11.1.3
Facilities and Equipment for EMR System Security	Use of certified information security products	N/A	N/A
	Data and software encryption and integrity	2.7.1, 2.9.4	7.2.2, 12.1.3, 12.1.4, 12.3.1, 13.1.3
	System Configuration for Strengthening Access Control	2.6, 2.8, 2.9.5, 2.9.7, 2.10.6, 2.11.3	7.2.2, 10.2, 13
	Establishment and monitoring of data management plan	2.11.5	12.1, 6.1.2
Facilities and equipment to prevent physical access to EMR storage	Defining the restricted area	2.4.1, 2.4.5	8.1.1, 8.1.3
	Access control and monitoring to the status information	2.4.2	8.1.2
	Restrirction tothe physical location	3.3.4	12.1.5
Facilities and equipment for real-time inspection of the EMR system	Real-time check of EMR system	2.9.2	N/A
	Monitoring of the network systems	2.9.2	11.1.2
Spare equipment	Auxiliary system operation	6.2.2	2.9.3
Surveillance equipment such as CCTV(closed-circuit television)	CCTV installation and operation	3.1.6	N/A
	Operation of the external intrusion detection equipment	2.4.3	8.1.4
	Confirmation of access status information	2.4.1	8.1.2
Disaster prevention facilities	Fire-warning facilities	2.4.4	8.2.2
	Fire extinguishing system		
	Prevention facilities of the flood		
	Supply facilities		8.2.4
	HVAC(heating, ventilating, and air conditioning)		8.2.2

상기 표와 같이 기존의 고시에서 추가적인 조치를 제시하는 내용이 ISMS-P나 CSAP에서 다루는 항목과 일치하고 있어서 전자의무기록 보관의 내·외부 기준을 철회하고 전자의무기록 관리·보관의 환경, 상황과 형태, 기관의 특성에 따라 위험평가를 기반으로 적절한 보안통제를 융통성 있게 구현하는 것이 바람직해 보인다. 따라서 다음과 같은 개정 방안을 제시한다.

표 6. 고시 제목 개정안
Table 6. Proposed amendment of the Public Notice for the external preservation of EMR

Current	Proposed Amendment
[attached Table] Additional measures necessary for preserving EMR outside a medical institution	[attached Table] (Delete)

V. 결 론

전자의무기록의 안전한 관리 및 보존을 위한 규정들은 앞선 3장과 4장에서 살펴본 개정 방안의 적용을 통하여 일부 개선이 가능할 것으로 보인다.

의료 IT에서 사용되는 전자의무기록에는 인적 정보, 처방정보, 검사정보, 금융정보, 각종 동의서와 관리정보 등 다양한 데이터와 정보를 포함하고 있고 해당 정보는 전자의무기록시스템 뿐만 아니라 의료기관 내외부 수많은 시스템과 연계되어 수집·활용·전송되고 있다. 각 시스템별 또는 목적별로 별도의 규정을 마련하여 전자의무기록 정보를 관리하는 것과 같은 보안정책은 전체적인 의료 IT 영역에서 보안을 일관되게 적용하기 어렵게 하고, 보안의 홀(hole)을 만들거나 취약점을 증가시킬 수 있는 문제점을 야기하게 된다. 따라서 '시설과 장비' 중심으로 규정된 기존 기준의 범위를 확장하여 전반적인 의료정보 및 정보시스템 보안성 확보 기준으로서 관리적·기술적· 물리적 요구사항을 수립하여야 할 것으로 보인다. 이는 '진료기록전송지원시스템이 보유한 정보의 안전성 확보를 위한 관리계획의 수립·시행' 규정과의 통합을 고려했을 때도 적절한 방식이라고 판단된다. 일관성 있고 통합적인 보안정책을 적용하기 위해서 보다 근본적인 해결책을 마련해야 할 필요성이 보이며 이를 위해서 현재 의료 IT에서 사용되는 전자의무기록과 관련하여 미국, 영국 등의 국외 동향을 살펴보면, 국가적 차원의 데이터 분류 및 등급화 메커니즘이 존재하며, 상위 수준의 원칙이 각 산업과 분야, 시스템에까지 일관되게 적용되고 있음을 확인할 수 있었다. 국내 정부에서도 일차적으로는 이와 같은 통일되고 일관성 있는 데이터 및 시스템의 분류와 등급화 원칙이 수립되어야 하며, 규정된 등급에 따라 적절하게 적용될 수 있는 가이드라인이 마련되어야 할 것으로 보인다.

이러한 의료 IT 분야 전반에서 적용할 수 있는 의료정보의 분류와 등급화 메커니즘을 마련한 후 이를 기반으로 목적과 대상에 따른 정책을 수립하는 것이 합리적인 접근법이라고 판단된다. 이와 같은 프로세스의 수립을 통해 전자의무기록 관리·보존의 보안성 확보 조치 기준을 앞서 설명하는 내용과 같이 개정하게 된다면, 법규의 상충과 혼란을 예방할 수 있고, 새로운 서비스와 기술이 발전에도 융통성 있게 대처할 수 있다고 판단된다. 즉, 보안성을 강화해야 하는 정보 및 정보시스템을 명확하게 식별함으로써 규제의 범위와 한계가 명확해짐으로 인하여 창의적이고 혁신적인 서비스 및 제품 개발을 위한 규제 강화와 완화를 융통성 있게 적용할 수 있다. 이는 법규의 안정성과 법 적용의 신뢰성을 확보할 수 있는 매우 근본적이고 효과적인 방안이다.

본 논문에서 살펴본 바와 같이 의료 IT에서 사용되는 전자의무기록시스템은 끊임없는 사이버보안 위협과 도전에 직면하고 있다. 이를 개선하기 위해 단기적이고 현실적인 대안은 앞서 기술했던 바와 같이 전자의무기록의 법규적 보안성 요구사항을 '전자의무기록 관리·보존의 보안성 확보 조치 기준'으로 통합하고, 그에 부합하도록 의료법, 의료법 시행령, 의료법 시행규칙 및 위임법규 등을 개정하는 방안이다. 현재의 법령에서는 전자의무기록 보안성 확보를 위한 방안이 전자의무기록 관리·보존에 필요한 시설과 장비에 관한 기준과 의료법 시행령 제10조의5 진료전송지원시스템 보유 정보의 안전성 확보 조치 등 필요에 따라 별도의 규정으로 적용되고 있다. 이와 같이 본질적으로 전자의무기록을 그 보호 대상으로 하는 규정들을 통합하여 전자의무기록을 보호하기 위한 하나의 일관성 있는 규정으로 통합하여 관리하여 법령의 신뢰성을 확보하고 중복 규제의 불편함을 해소할 필요가 있다.

또한 의료기관과 전자의무기록과 관련하여 적용될 수 있는 개인정보의 안전성 확보 조치 기준, 개인정보의 안전성 확보 조치 기준 특례 조항, ISMS-P, CSAP 등 타법 기반 규제나 제도의 요구 사항을 통합적으로 검토하여 개선방안을 마련함으로써 적용 대상자들의 부담을 경감시킬 필요가 있다고 판단된다.

References

[1] MoHW, "Public Notice On the Operation of the EMR System Certification System", *Public Notice of MoHW 2021-2,* Jan. 2021.

[2] MoHW, "Article 23 Electronic Medical Records", *Medical Service Act 17787,* Dec. 2020

[3] M. S. Hwang, "The legal problems on the crime of issuance of falsified medical

certificates and the false writing of medical examination Record," *J. Law*, vol. 28, no. 1, pp. 5-33, Mar. 2011.

[4] MoHW, "Article 22 Medical Records, etc.", *Medical Service Act 17787,* Dec. 2020.

[5] MoHW, "Article 14 Items to be Entered in Medical Records, etc.", *Enforcement Rule of the Medical Service Act 910,* Sept. 2022

[6] MSIT, "Article 2 Definition", *Digital Signature Act 18475,* Oct. 2021

[7] I. Y. Lee, "An analysis of the major issues on electronic medical records," *J. Law*, vol. 28 No. 1, pp. 75-98, Mar. 2011.

[8] J. S. Park and Y. W. Shin, "Development of guideline on electronic signatures for electronic medical record," *The J. Korea Contents Assoc.*, vol. 5, no. 6, pp. 120-128, Dec. 2005.

[9] MoHW, "Article 21-2 Electronic Medical Records, etc.", *Medical Service Act 6759,* Dec. 2002

[10] S. M. Lee, "The medical treatment informatization and medical treatment information protection," *J. Law*, vol. 25, no. 1, pp. 36-56, Mar. 2008.

[11] BoanNews, "A series of hacking attacks targeting large hospitals. How are HDOs responding?," Aug. 2022. (www.boannews.com/media/view.asp?idx=108971&kind=1)

[12] MoHW, "Article 23-2 Notification of Medical Information Incident", *Medical Service Act 14438,* Dec. 2016

[13] MoHW, "Article 23-4 Prevention and Response to Medical Information Incident, etc.", *Medical Service Act 16555, Aug.* 2019

[14] MoHW, "Article 18-2 Facilities, Equipment, etc. Necessary for the Management and Preservation of EMRs", *Enforcement Rules of the Medical Service Act, Decree of MoHW 261, Oct.* 2003

[15] MoHW, "Criteria for Facilities and Equipment Necessary for Management and Preservation of EMRs", *Public notice of MoHW 2016-140,* Aug. 2016.

[16] MoHW, "Criteria for Additional Measures Necessary for Preserving EMRs outside of HDOs", *Public notice of MoHW 2016-140,* Aug. 2016.

[17] Korea Communication Commission, "Article 47 ISMS Certification" *Act on Promotion of Information and Communications Network Utilization and Information Security, etc.* 13520, Dec. 2015.

[18] MoHW, "Criteria of EMR System Certification" v.1.1, Oct. 2021. (https://emrcert.mohw.go.kr/evaluateWeb/evaluateInfoList.es?mid=a10102020000)

[19] MSIT, "Criteria for Cloud Computing Service Information Protection" *Public Notice of MSIT 2017-7*, Aug. 2017.

[20] U.S. Congress, "Health Information Technology for Economic and Clinical Health Act", *PUBLIC LAW 111－5－FEB. 17*, 2009.

[21] Code of Federal Regulations, 45 CFR 170.314(d)(1) ~ (8) ; 45 CFR 170. 315(d)(1) ~ (11).

[22] ONC, "Health Information Technology (Health IT) Certification Criteria" 2015 Edition, *ONC Health IT Certification Program Modifications*, Published Oct. 16, 2015 (80 FR 62602 at 62602).

[23] U.S. Congress, "Health Insurance Portability and Accountability Act", PUBLIC LAW 104－191－AUG. 21, 1996.

[24] PIPC, "Article 30 Measures to Ensure the Security of Personal Information", *Enforcement Decree of the Personal Information Protection Act 32813*, July 2022.

[25] PIPC, "Article 48-2 Special Provisions on Measures to Ensure Security of Personal Information", *Enforcement Decree of the Personal Information Protection Act 32813*, July 2022.

[26] MoHW, "Paragraph 1, Article 10-7 Certification of EMR System", *Enforcement Decree of the Medical Service Act* 32842, Aug. 2022.

[27] MoHW, "Article 10-5 Measures to Ensure the Security of Information in the EMR

Transmission Support System", *Enforcement Decree of the Medical Service Act* 32842, Aug. 2022.

이 인 혜 (In Hye Lee)

1992년 : 한양대학교 철학과 (학사)
2018년 : 건국대학교 정보보안 전공 공학석사
2021년~현재 : 성균관대학교 삼성융합의과학원 의료기기 산업학과 박사과정
2019년~현재 : 고려대학교 정보보호연구원 연구원
<관심분야> 의료보안 표준, 의료데이터 보안, 의료기기 보안, 의료기기 규제 과학, ICT 융합보안
[ORCID:0000-0002-1579-7185]

진 정 하 (Jungha Jin)

2002년 : 국립 금오공과대학교 전자통신공학과(학사)
2006년 : 건국대학교 정보보안 전공 공학석사
2020년 : 건국대학교 정보보안 전공 공학박사
2020년~현재 : 고려대학교 정보보호연구원 연구교수
<관심분야> Health IT, ICT 융합보안, 사이버 보안
[ORCID:0000-0001-5303-7673]