

서울시 의료기관들의 개인정보처리방침에 있어 개인정보보호법 준수 현황 분석: 홈페이지 게재 내용을 중심으로

탁 지원¹ | 김 서 현¹ | 민 기 단¹ | 장 수 영¹ | 오 준 형^{1*}

¹ 서울여자대학교

* 교신저자: 오준형
(ohjun02@gmail.com)

| 초 록 |

본 연구는 서울 소재 의료기관의 개인정보 처리방침 공개 현황을 분석하고 병원 규모에 따른 차이를 평가하였다. 「개인정보 보호법」에 따라 의료기관은 개인정보 처리방침을 수립하고 공개해야 하지만, 실제 준수 현황에 대한 체계적 연구는 부족하다. 서울 내 10,004개 의료기관(3차 14곳, 2차 44곳, 1차 9,946곳) 중 홈페이지를 운영하는 의료기관을 대상으로 개인정보 처리방침 게시 여부와 내용의 적정성을 평가하였다. 분석 결과, 2차 및 3차 의료기관은 모두 홈페이지를 운영하며 법적 요구사항을 대부분 충족했으나, 홈페이지를 운영하는 1차 의료기관의 경우 처리방침 공개와 표준화된 용어 사용이 미흡한 것으로 나타났다. 이는 병원 규모에 따른 법적 준수 수준의 현격한 차이를 보여주며, 특히 1차 의료기관의 개인정보 보호 강화를 위한 맞춤형 정책적 지원과 기술적 도입이 필요함을 시사한다. 본 연구는 의료기관의 개인정보 보호 체계화에 기여할 수 있는 기초 자료로 활용될 수 있을 것이다.

주요 용어: 개인정보 처리방침, 개인정보 처리방침 현황, 의료기관, 개인정보 보호법

알기 쉬운 요약

이 연구는 왜 했을까? 개인정보 보호법에 따라 의료기관에서 개인정보 처리방침을 수립하고 공개해야 함에도 불구하고, 특히 1차 의료기관에서 이러한 방침의 수립과 공개가 미흡하거나 인터넷상에서 확인이 어려운 문제를 해결하고자 수행되었다. 이를 위해 서울 소재 의료기관 중 홈페이지를 운영하는 기관들을 대상으로 개인정보 처리방침의 현황을 체계적으로 분석하고, 의료기관 규모별 법적 준수 수준의 차이를 파악하고자 한다.

새롭게 밝혀진 내용은? 홈페이지를 운영하는 의료기관들을 분석한 결과, 2차와 3차 병원에서는 개인정보 처리방침의 수립 및 공개가 거의 모든 기관에서 이루어지고 있었으나, 1차 병원의 경우 이 비율이 현저히 낮은 것으로 나타났다. 이는 병원 규모에 따라 개인정보 보호법의 준수 수준에 큰 차이가 있으며, 특히 1차 의료기관의 개인정보 처리방침 수립 및 공개가 미흡함을 밝혀냈다.

앞으로 무엇을 해야 하나? 본 연구는 의료기관이 개인정보 보호법에 따라 개인정보 처리방침을 정확히 수립하고 투명하게 공개할 필요성을 제시한다. 특히 1차 의료기관의 개인정보 보호 수준을 제고하기 위해서는 표준화된 개인정보 처리방침 자동 생성기 개발과 같은 정책적 지원이 필요하며, 이를 통해 의료기관들이 법적 의무를 이행하고 환자 신뢰를 증진할 수 있도록 유도해야 할 것이다.

이 논문은 정부(교육부)의 지원을 받아 수행된 연구(2024년 부처 협업형 인재양성사업[정보보안 분야], No. 2024개인정보보호-002)이며, 서울여자대학교 학술연구비의 지원을 받았음(2025-0001).

■ 투 고 일: 2024. 10. 18.
■ 수 정 일: 2024. 12. 10.
■ 게재확정일: 2024. 12. 23.

I. 서론

2008년 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행규칙」의 개정으로 의료기관도 개인정보 보호 필수기관에 포함되었고(홍주연, 김환희, 2019), 이어 2011년에는 「개인정보 보호법」이 제정됨에 따라 민감한 개인정보를 많이 다루는 의료기관의 개인정보보호 관리는 사회적 이슈로 부각되기 시작하였다(황지환, 2017). 이러한 법적 변화와 더불어 의료계에선 의료 정보의 디지털화와 병원 업무의 전산화가 빠르게 자리 잡으면서(오진석, 2020), 이는 환자에게 향상된 의료 서비스를 제공하는 데 기여하였으나, 동시에 네트워크를 통한 의료 정보 유출 위험성도 증가하였다(Anderson, 2000, 홍주연, 김환희, 2019에서 재인용). 개인의료정보는 국민의 건강을 보호하고 증진하기 위해 의료인과 의료기관이 행하는 의료 행위와 관련된 정보로 정의되며(백운철, 2005, 이한주, 2012에서 재인용), 이는 민감한 특성을 지니고 있다(Jang, 2007, 최선영 외, 2016에서 재인용). 국민 건강과 밀접하게 연관된 민감정보는 단순히 유출만으로도 개인의 사생활 침해(이한주, 2012)뿐만 아니라 정보 주체에 따라 정치적, 사회적, 경제적 문제를 야기할 수 있다(오진석, 2020). 특히, 한 번 유출된 정보는 복구가 어렵기 때문에 사전 예방 조치가 무엇보다 중요하며(강지원, 2018, 신민지 외, 2019에서 재인용), 이를 위한 가장 기본적인 필수적인 조치 중 하나는 의료기관이 개인정보 처리방침을 수립하고 이를 투명하게 공개하는 것이다(정영철, 2014).

그러나, 국내 의료기관에서의 보안 중요성에 대한 인식은 여전히 부족하며, 구체적인 보호 방안 또한 미흡한 상황이다(신민지 외, 2019). 이에 대한의사협회는 의료기관의 개인정보 보호를 돕기 위해 자율점검 시스템을 운영하고 있으나(박선재, 2023), 해당 시스템이 체크리스트에 O/X만 표기하는 형식적인 점검에 그쳐 실효성에 의문이 제기된다. 이러한 우려를 반영하듯, 최근 몇 년간 의료기관의 개인정보 유출 사건이 빈번히 발생하고 있다(신민지 외, 2019). 2024년 7월 개인정보보호위원회가 17개의 종합병원이 환자의 민감 정보를 유출한 사건을 조사한 결과, 16개 병원이 개인정보 처리 시스템에서 안전 조치를 소홀히 한 것으로 밝혀졌으며, 이에 따라 6,480만 원의 과태료가 부과되었다(개인정보보호위원회, 2024). 이 사건은 의료기관의 개인정보 관리가 얼마나 취약한지를 잘 보여주는 사례로, 유출된 정보는 총 18만 5,271명의 환자와 관련된 민감 정보였다(개인정보보호위원회, 2024). 이처럼 의료기관을 대상으로 한 보안 위협은 지속해서 발생하고 있으나, 의료기관의 특성을 고려한 의료현실에 적합한 실질적 보안체계가 필요하다(신민지 외, 2019).

2023년 조사에 따르면, 개인정보 침해에 대한 우려는 54.6%에 달했다(한국정보보호산업협회, 2023). 개인정보에 대한 침해 우려가 절반 이상을 차지하는 상황에서, 정보 주체는 자신의 개인정보가 어떻게 사용되고 있는지 확인하기 위해 개인정보 처리방침을 활용할 수 있다. 그러나 의료기관에서는 개인정보 처리방침을 수립하여 출력하거나, 홈페이지 운영 시 이를 게시해야 하지만(황지환, 2017), 이러한 방침이 없거나, 있다 하더라도 구체적으로 작성되지 않은 경우가 많다(한국인터넷진흥원, 2021).

개인정보 처리방침은 의료기관이 개인정보 보호에 대한 경각심을 높일 뿐 아니라(정찬모, 2013), 정보 주체가 자신의 정보가 어떻게 처리되고 있는지 투명하게 알 수 있는 중요한 도구이다(정영철, 2014). 「개인정보 보호법」에 따라 모든 기관은 개인정보 처리방침을 수립하고 이를 공개해야 하며, 이는 해당 기관의 개인정보 보호 수준을 평가하는 중요한 지표다(정영철, 2014). 그러나, 의료기관의 개인정보 처리방침 준수 현황에 대한 체계적인 연구는 부족한 상황이다. 의료기관 간 법적 준수 수준을 비교하고, 이를 통해 각 기관의 개인정보 보호 수준을 객관적으로 평가하는 것은 의료기관의 정보 보호 체계를 개선하는 데 중요한 기초 자료를 제공할 수 있다.

따라서, 본 연구는 서울 내 1차, 2차, 3차 병원의 개인정보 처리방침 수립 및 공개 현황을 분석하여, 각 병원의 개인정보 보호 준수 수준을 평가하고자 한다. 구체적으로는 각 의료기관의 개인정보 처리방침 수립 및 공개 여부와 그 내용을 항목별로 면밀히 분석하여 의료기관 유형별로 현황을 비교하고, 이를 통해 각 병원의 법적 준수

상태를 명확히 파악하고자 한다. 이를 위해 서울에 있는 총 10,004개의 병원을 대상으로 분석을 수행하였으며, 이 중 3차 병원은 14개, 2차 병원은 44개, 1차 병원은 9,946개로 구성되어 있다. 병원의 홈페이지에 게시된 개인정보 처리방침을 분석 대상으로 하였으며, 홈페이지가 없는 경우와 홈페이지에 개인정보 처리방침이 게시되지 않은 경우, 해당 기관이 이를 수립하지 않은 것으로 판단하였다.

본 연구는 기존 연구에서 다루지 않았던 다양한 유형의 의료기관에서의 개인정보 처리방침 준수 실태를 분석함으로써, 의료기관 간의 법적 준수 수준을 비교하고, 이를 통해 개인정보 보호의 실질적 이행 수준을 평가하고자 한다. 이러한 연구 결과는 의료기관의 개인정보 보호 수준을 평가하는 체계적인 연구를 통해 의료기관 간 법적 준수 수준을 비교할 수 있는 객관적인 데이터를 제공함으로써, 개인정보 보호와 의료 정보 관리 분야의 연구에 중요한 기초 자료로 활용될 수 있다. 또한, 연구 결과를 바탕으로 각 의료기관이 개인정보 보호 체계를 자발적으로 개선하도록 유도하고, 「개인정보 보호법」 준수를 강화하는 데 기여할 수 있다. 궁극적으로는 의료기관의 개인정보 보호 수준을 향상해 국민의 신뢰를 높이고, 더욱 안전한 의료환경을 조성하는 데 기여하고자 한다.

II. 선행연구

현재, 개인정보 분야에 관한 관심이 높아지면서 개인정보보호를 주제로 한 연구가 꾸준히 이루어지고 있다. 개인정보 처리방침은 개인정보 보호법(2023) 제30조에 따라 수립하고 공개해야 하는 필수적인 사항이므로, 개인정보 처리방침을 주제로 한 연구는 주로 그 내용을 분석, 검증, 효과, 비교하는 방식으로 개인정보 처리방침의 내용을 활용하는 연구가 주를 이루고 있다.

심혜연 외(2024)는 개인정보가 오남용되는 문제상황에서 개인정보 오남용을 예방하기 위해 개인정보 처리방침을 확인하는 것이라고 주장하였다. 이를 확인하는 여러 방법에서 생성형 인공지능을 활용하는 방법으로 개인정보 처리방침의 안전성을 검증하는 연구를 진행하였다. 연구 결과, GPT를 활용한 안전성 검증 방법은 기존의 블랙리스트 기반 안전성 검증 기법에 비해 유의미하게 높은 정확도를 보였으나 최소 정확도는 높지 않은 것으로 나타났다.

조용현, 차영균(2020)은 개인정보 처리방침의 내용이 복잡하여 읽지 않는 기존의 문제점을 해결할 수 있도록 딥러닝을 활용해 국내 주요기업과 개인정보 관리체계 인증기업의 개인정보 처리방침의 내용을 요약 및 분석하는 연구를 진행하였다. 단순화된 개인정보 처리방침은 소비자와 기업 관계에서 정보의 비대칭성을 해결하는데 기여하는 역할을 할 것이라고 주장하였으며 연구 결과 임베딩을 통한 분석이 가능한 것을 입증하였다. 또한 주요 기업의 개인정보 처리방침 데이터셋을 구축하였다는 시사점을 가진다.

이재근 외(2013)는 1,000개의 개인정보 처리방침과 연관 데이터를 메타데이터 형식 및 엔코딩 스킴을 통해 수집하여 통계적으로 분석하는 연구를 진행하였다. 직접 데이터와 연관 데이터로 처리방침의 데이터를 구분하였으며 개인정보 처리방침의 각 항목의 기술 현황을 조사하였다. 이 연구는 메타데이터 형식 및 엔코딩 스킴을 통한 개인정보 처리방침 조사 방법이 대규모의 처리방침 정보를 수집, 저장하기 용이하다는 결과를 나타내었다.

정윤교(2023)는 모바일 앱의 사용자가 개인정보 처리방침을 신뢰할 수 있는지 확인하기 위해 안드로이드 정적 분석을 바탕으로 개인정보 처리방침의 내용과 모바일 앱을 분석하여 비교하는 시스템을 설계하고 이를 활용하는 연구를 진행하였다.

백인주 외(2019)는 GDPR의 투명성 원칙에 초점을 두어 개인정보 처리방침이 투명성의 원칙 준수 여부를 판별하는 연구를 진행하였으며, GDPR 투명성 원칙의 의미와 확보 방안을 제시하였다.

이은숙 외(2016)은 다수의 사용자가 개인정보 처리방침이 게재되었음에도 불구하고 확인하지 않는 문제가 있

는 상황에서, 개인정보를 민감하게 생각하는 집단과 그렇지 않은 집단으로 개인정보 처리방침을 확인한 이후의 행동을 비교하는 실험을 통해 개인정보 처리방침을 확인하는 것이 사용자 행동에 어떤 영향을 끼치는지 확인하는 연구를 진행하였다. 연구 결과, 개인정보 처리방침을 확인하는 것이 보호 행동에 영향을 주는 것으로 확인할 수 있었다.

이처럼 기존의 연구들은 개인정보 처리방침의 역할과 내용을 분석하는 연구들이 주를 이루었으며, 개인정보 처리방침을 평가하는 연구 대부분은 여러 분야의 개인정보 처리방침을 분석하거나 적은 데이터의 개인정보 처리방침을 조사하였기에 연구 결과를 일반화하기 어려웠다는 한계를 갖고 있었다. 반면, 본 연구는 조사 범위를 의료 분야로 한정하고, 서울시에 위치한 홈페이지가 있는 병원의 개인정보 처리방침을 분석함으로써 연구 결과의 일반화를 가능하게 하였다. 이러한 점에서 본 연구는 기존 연구와 차별화되며, 의료기관 간 개인정보 처리방침의 준수 현황을 평가할 수 있는 체계적인 데이터를 제공한다는 의의를 가진다.

III. 연구 방법

1. 조사설계

개인정보 처리방침은 개인정보 처리의 기준과 보호 조치로서, 개인정보 보호법(2023) 제30조에 따라 수립 및 공개가 의무화되어 있다. 또한, 동법 시행령(2024) 제31조에서는 개인정보 처리방침의 내용과 공개 방법을 규정하고 있으며, 표준 개인정보 보호지침(2024) 제18조부터 제21조까지는 개인정보 처리방침의 공개, 변경, 작성 기준, 필수 기재사항 및 임의 기재사항을 제시하고 있다.

본 연구는 분석 시점인 2024년 8월을 기준으로, 건강보험심사평가원 (2024)에 등록·공개된 의료기관 중 서울에 위치한 상급종합병원, 종합병원, 병원, 의원 등 총 10,004개 의료기관의 홈페이지에서 개인정보 처리방침 현황을 파악하기 위해 수행되었다. 조사 대상은 3차 병원 14개, 2차 병원 44개, 1차 병원 9,946개로 분류된다.

먼저 상용 검색 포털을 통해 각 의료기관의 홈페이지 존재 여부를 확인하였으며, 홈페이지가 존재할 경우 개인정보 처리방침의 게시 여부를 검토하였다. 개인정보 처리방침이 게시된 경우, ‘개인정보 처리방침’이라는 명칭을 사용하고 있는지를 평가한다. 또한, 필수적 기재사항인 ‘개인정보 처리 목적’, ‘처리하는 개인정보 항목’, ‘개인정보 처리 및 보유 기간’, ‘개인정보 파기 사항’, ‘개인정보 안전성 확보조치’, ‘개인정보 처리방침 변경’, ‘개인정보 보호 책임자’, ‘정보주체 권리·의무 및 행사 방법’, ‘정보주체 권익침해 구제 방법’과 1)해당 시 기재사항인 ‘개인정보 제3자 제공 사항’, ‘개인정보 위탁 사항’, ‘가명정보 처리 사항’, ‘개인정보 자동 수집 장치 운영 및 거부 사항’, ‘고정형 영상 정보처리기기 운영 및 관리 사항’ 14개의 항목이 포함되었는지와 각 항목이 충분히 기술되어 있는지에 대한 평가 기준을 세우고 이를 바탕으로 평가를 진행하였다(개인정보 보호법, 2023; 표준 개인정보 보호지침, 2024; 개인정보 보호법 시행령, 2024)(표 1-2, 1-3 참고).

조사 항목은 개인정보 보호법(2023), 개인정보 보호법 시행령(2024), 표준 개인정보 보호지침(2024)을 기준으로 선정하였다(표 1-1 참고).

1) ‘해당 시 기재사항’은 의료기관별 운영 현황에 따라 추가 기재가 필요한 항목을 본 연구에서 구분하여 지칭한 것으로, 각 의료기관의 개인정보 처리 방식에 따라 선택적으로 작성되는 항목을 의미함.

표 1-1. 개인정보 처리방침 구성내용 법적 근거

구분	내용	법적 근거
개인정보 처리방침 수립	개인정보 처리방침을 수립하여야 함	개인정보 보호법 제30조 제1항
개인정보 처리방침 게시	개인정보 처리방침을 게시하여야 함	개인정보 보호법 제30조 제2항
개인정보 처리방침 공개 방법	수립한 개인정보 처리방침은 인터넷 홈페이지에 게재하여야 함	개인정보 보호법 시행령 제31조
개인정보 처리방침 명칭	'개인정보 처리방침'이라는 명칭을 사용함	표준 개인정보 보호지침 제20조
개인정보 처리방침 작성 기준	개인정보 처리항목에 정보주체의 동의를 받는 항목과 동의를 받지 않는 항목을 구분하여 표시함	표준 개인정보 보호지침 제12조 제5항
필수적 기재사항	-개인정보 처리 목적 -처리하는 개인정보 항목 -개인정보 처리 및 보유 기간 -개인정보 파기 사항 -개인정보 안전성 확보조치 -개인정보 처리방침 변경 -개인정보 보호책임자 -정보주체 권리·의무 및 행사 방법 -정보주체 권익침해 구제 방법	표준 개인정보 보호지침 제19조
해당 시 기재사항	-개인정보 제3자 제공 사항 -개인정보 위탁 사항 -가명정보 처리 사항 -개인정보 자동 수집 장치 운영 및 거부 사항 -고정형 영상 정보처리기기 운영 및 관리 사항	표준 개인정보 보호지침 제19조 개인정보 보호법 제25조 제7항

표준 개인정보 보호지침(2024) 제20조(개인정보 처리방침의 공개) 제1항에 따르면 개인정보처리자가 개인정보 보호법(2023) 제30조 제2항에 따라 개인정보 처리방침을 수립하는 경우에는 인터넷 홈페이지를 통해 지속적으로 게재하여야 하며, 이 경우 '개인정보 처리방침'이라는 명칭을 사용하여야 한다고 명시되어 있다.

표 1-2. 의료기관 개인정보 처리방침 홈페이지 게재

구분	조사 항목
홈페이지 게재 여부	상용 검색 포털을 통해 각 의료기관의 홈페이지 존재 여부를 확인할 수 있는가?
처리방침 게재 여부	홈페이지 내에서 개인정보 처리방침을 확인할 수 있는가?
'개인정보 처리방침' 명칭 사용	개인정보 처리방침 게재 시 '개인정보 처리방침' 명칭을 사용하였는가?

표 1-3. 의료기관 홈페이지 개인정보 처리방침 조사 항목

구분	조사 항목
개인정보 처리 목적	병원 등록번호, 성명(한글), 주민등록번호, 주소, 연락처(전화번호, 휴대전화 번호), 병력 및 가족력 등등과 같이 개인정보 처리 목적에 진료 관련 내용이 포함되어 있는가?
처리하는 개인정보 항목	처리하고 있는 개인정보 각 항목에 진료 관련 내용이 포함되어 있는가? 동의와 비용의 및 법적 근거를 기재하였는가?
개인정보 처리 및 보유 기간	정보주체로부터 동의 받은 '보유·이용 기간' 혹은 법령에 의한 '보유·이용기간'이 기재되어 있는가?
개인정보 파기 사항	개인정보 파기 절차 및 방법이 명시되어 있는가?
개인정보 제3자 제공 사항	제3자 제공을 하는 경우 제3자 제공에 관한 내용이 명시되어 있는가?
개인정보 위탁 사항	위탁하는 경우 위탁에 관한 내용이 명시되어 있는가?
개인정보 안전성 확보조치	안전성 확보조치 사항이 명시되어 있는가?

구분	조사 항목
개인정보 자동 수집 장치 운영 및 거부 사항	개인정보 자동 수집 장치 운영 및 거부 사항이 명시되어 있는가?
가명정보 처리 사항	가명정보 처리에 관한 사항이 명시되어 있는가?
정보주체 권리·의무 및 행사 방법	정보주체의 권리, 의무사항이 명시되어 있는가?
개인정보 보호책임자	개인정보 보호책임자 사항이 명시되어 있는가?
정보주체 권익침해 구제 방법	권익침해에 대한 구제 방법이 명시되어 있는가?
고정형 영상 정보처리기기 운영 및 관리 사항	고정형 영상 정보 처리기기 운영 및 관리 사항이 명시되어 있는가?
개인정보 처리방침 변경 사항	개인정보 처리방침의 시행 일자가 기재되어 있는가?

본 연구에서는 개인정보 처리방침의 기재 현황을 평가하기 위해 항목별로 구체적인 기준을 설정하여 준수 여부를 평가하였다. 평가에서 사용된 항목들은 모두 개인정보 보호법(2023) 제30조 제1항과 표준 개인정보 보호 지침(2024) 19조(개인정보 처리방침의 기재사항)에서 규정하는 각 호의 사항에 해당하며, 개인정보 처리방침의 적정성과 법적 준수 여부를 검토하기 위해 설정되었다. 해당 조항들은 개인정보처리자가 개인정보 처리방침을 수립하고 공개할 때 포함해야 하는 사항들을 명시하고 있으며, 공공기관의 경우 개인정보 보호법(2023) 제32조에 따라 등록 대상이 되는 개인정보 파일에 대한 처리방침을 정하도록 규정하고 있다.

본 연구에서 사용된 각 평가 항목의 기준은 다음과 같다. 먼저, 개인정보 처리방침이라는 명칭을 사용하고 있는 경우와 ‘개인정보 취급 약관’, ‘개인정보 취급방침’, ‘개인정보 보호 정책’ 등 다른 명칭을 사용하는 경우를 구분하여 평가하였다. 표준 개인정보 보호지침(2024) 제20조(개인정보 처리방침의 공개) 제1항에 따르면, 개인정보 처리자가 개인정보 보호법(2023) 제30조 제2항에 따라 개인정보 처리방침을 수립하는 경우, 인터넷 홈페이지를 통해 지속적으로 게재하여야 하며, 이 경우 ‘개인정보 처리방침’이라는 명칭을 사용해야 한다고 규정하고 있다.

‘개인정보 처리 목적’ 항목의 경우, 병원 등록번호, 성명, 주민등록번호, 주소, 연락처, 병력 및 가족력 등의 진료 관련 정보가 포함되어 있는지를 평가하였다. 이는 개인정보 보호법(2023) 제30조 제1항 제1호에서 요구하는 개인정보의 처리 목적에 대한 명시 여부를 확인하기 위한 것으로, 진료 관련 목적이 모두 명시된 경우에는 ‘준수로 평가하였다. 진료와 관련된 내용이 누락되었거나 홈페이지 관련 내용만 언급된 경우에는 ‘미흡’으로, 해당 항목 자체가 처리방침 내에 명시되지 않은 경우에는 ‘미기재’로 평가하였다.

‘처리하는 개인정보 항목’에서는 진료 관련 항목이 모두 명시된 경우에만 ‘준수로 평가하였다. 진료와 관련된 내용이 누락되었거나, 홈페이지 관련 내용만 언급된 경우에는 ‘미흡’으로, 해당 항목 자체가 개인정보 처리방침 내에 명시되지 않은 경우에는 ‘미기재’로 평가하였다. 개인정보 보호법(2023) 개정에 따라 법 제15조 제1항 제2호부터 제7호 중 어느 하나에도 해당하면 정보주체의 동의를 받지 않아도 개인정보를 수집할 수 있게 되었고, 이에 따른 표준 개인정보 보호지침(2024) 제12조 제5항에 의해 정보주체의 동의 없이 처리하는 개인정보에 대해서는 그 항목과 처리의 법적 근거를 동의받아 수집하는 개인정보와 구분하여 기재하여야 한다. 개인정보 처리의 법적 근거는 개인정보 보호법(2023) 제15조 제1항 각 호의 사항 또는 개별 법령에 근거하는 경우 해당 법령을 기재하여야 한다. 특히 진료 사항의 경우, 의료법(2023) 제22조와 의료법 시행규칙(2024) 제14조에 따라 진료를 목적으로 개인정보를 환자의 동의 없이 수집 이용할 수 있다. 이를 근거하여 병원은 환자에게 정보주체 동의 없이 개인정보를 수집할 수 있다는 내용을 반드시 포함되어야 한다. 따라서 동의 여부 구분 및 법적 근거가 기재되어 있는지를 확인하기 위한 별도의 항목을 추가하여 평가하였다.

‘개인정보 처리 및 보유 기간’ 항목은 개인정보 보호법(2023) 제30조 제1항 제2호에 따라 정보주체로부터 동의를 받은 ‘보유·이용 기간 또는 법령에 의한 ‘보유·이용 기간’이 명시되어 있는지를 평가하였다. 진료 관련 정보의 의료법(2023) 제15조와 같은 법적 근거와 함께 명시된 경우에는 ‘준수로 평가하였으며, 진료 관련 기간과 근거가 명시되지 않거나 부분적으로만 기재된 경우 ‘미흡’, 해당 항목 자체가 없는 경우에는 ‘미기재’로 평가하였다.

‘개인정보 제3자 제공 사항’과 ‘개인정보 위탁 사항’의 경우, 각각 개인정보 보호법(2023) 제30조 제1항 제3호와 제4호에 근거하여 제3자 제공 및 위탁에 관한 세부 사항이 명시되어 있는지를 평가하였다. 해당 항목에 해당하는 경우 내용이 명시된 경우 ‘준수’, ‘00’이나 공백으로 제공사나 위탁사에 관련된 내용이 명확하게 기재되지 않은 경우 ‘미흡’, 관련 정보가 전혀 없는 경우 ‘미기재’로 평가하였다.

‘고정형 영상 정보 처리기기’ 운영자는 개인정보 보호법(2023) 제25조 제7항 본문과 대통령령으로 정하는 바에 따라 고정형 영상 정보 처리기기 운영·관리 방침을 마련해야 한다. 다만, 같은 조항 단서에 의하면 개인정보 보호법(2023) 제30조에 따른 개인정보 처리방침을 정할 때 고정형 영상정보처리기기 운영·관리에 관한 사항을 포함한 경우에는 고정형 영상정보처리기기 운영·관리 방침을 마련하지 아니할 수 있다. 고정형 영상정보처리기기 운영 및 관리 사항을 처리방침 내에 기재하였는지의 여부를 파악하고 아래 기준에 따라 ‘준수’, ‘미흡’, ‘미기재’로 평가하였다.

CCTV 설치 대수, 촬영 범위, 관리 책임자 등 개인정보 보호법 시행령(2024) 제25조 제1항 따른 운영 관리에 필요한 정보가 명시되어 있는지를 확인하고 명시된 경우에는 ‘준수’, 일부 항목이 ‘00’ 또는 공백으로 기재된 경우에는 ‘미흡’, 관련 내용이 전혀 없는 경우에는 ‘미기재’로 평가하였다.

‘개인정보 처리방침 변경’ 항목은 표준 개인정보 보호지침(2024) 제20조(개인정보 처리방침의 공개) 근거하여 개인정보 처리방침의 시행 일자가 명시되어 있는지를 평가하였다. 해당 내용이 기재된 경우에는 ‘준수’, 기재되지 않은 경우에는 ‘미기재’로 평가하였다. 표준 개인정보 보호지침(2024) 제21조(개인정보 처리방침의 변경) 제1항에 따르면 개인정보처리자가 개인정보 처리방침을 변경하는 경우에는 변경 및 시행의 시기, 변경된 내용을 지속적으로 공개하여야 하며, 변경된 내용은 정보주체가 쉽게 확인할 수 있도록 변경 전·후를 비교하여 공개하여야 한다. 그러나 해당 병원의 개인정보 처리방침이 최초 게재된 이후 수정 여부는 확인할 수 없기 때문에, 단순히 변경된 내용과 시기에 관한 사항이 없다고 규제를 위반하였다 단정 짓기는 어렵다. 이에 따라 본 연구에서는 처리방침의 변경에 관련된 평가는 제외하고 시행일의 기재 여부를 기준으로 평가하였다.

‘개인정보 파기 사항’, ‘개인정보 안전성 확보조치’, ‘개인정보 자동 수집 장치 운영 및 거부 사항’, ‘정보주체 권익침해 구제 방법’ 항목에서는 각 항목이 개인정보 처리방침 내에 명시되어 있는지를 평가하였으며, 명시된 경우 ‘준수’, 그렇지 않은 경우 ‘미기재’로 평가하였다.

‘가명정보 처리 사항’은 항목이 처리방침 내에 명시되어 있는지를 평가하였으며, 명시된 경우에만 ‘기재’로 평가하였다. 2차 및 3차 병원에서는 통계 작성, 과학적 연구, 공익적 기록 보존 등을 위해 가명정보를 처리하는 경우가 있어 해당 병원들에서만 ‘가명정보 처리 사항’을 평가하였다. 반면, 1차 병원에서는 이러한 처리 필요성이 상대적으로 낮다고 판단하여 ‘가명정보 처리 사항’은 조사 항목에서 제외하였다.

이와 같은 평가 기준을 바탕으로 각 항목의 기재 여부와 항목의 내용이 준수한지를 평가하였으며, 이를 통해 본 연구 내에서 개인정보 처리방침의 기재 현황과 병원 규모에 따른 처리방침의 수준을 구체적으로 파악할 수 있는 근거를 마련하게 되었다. 평가 기간은 2024년 8월 1일부터 8월 7일까지 1차 평가를 진행하였으며, 2024년 9월 2일부터 9월 6일까지 추가 검토를 통해 평가 항목과 평가 결과를 재확인하여 정확성을 높였다. 개인정보 보호법(2023) 제30조 제1항 각 호에서 요구하는 사항들이 실제 처리방침에 적절히 반영되었는지를 평가하고자 하였다.

IV. 연구 결과

1. 병원 규모별 홈페이지 및 처리방침 보유 현황

<표 2>는 서울시에 위치한 1차 병원 9,946개, 2차 병원 44개, 3차 병원 14개를 대상으로 개인정보 보호법(2023)에서 확인할 수 있는 개인정보 처리방침의 게재 방식인 인터넷 홈페이지 유무, 개인정보 처리방침 유무, '개인정보 처리방침' 명칭 사용 여부를 조사한 결과이다.

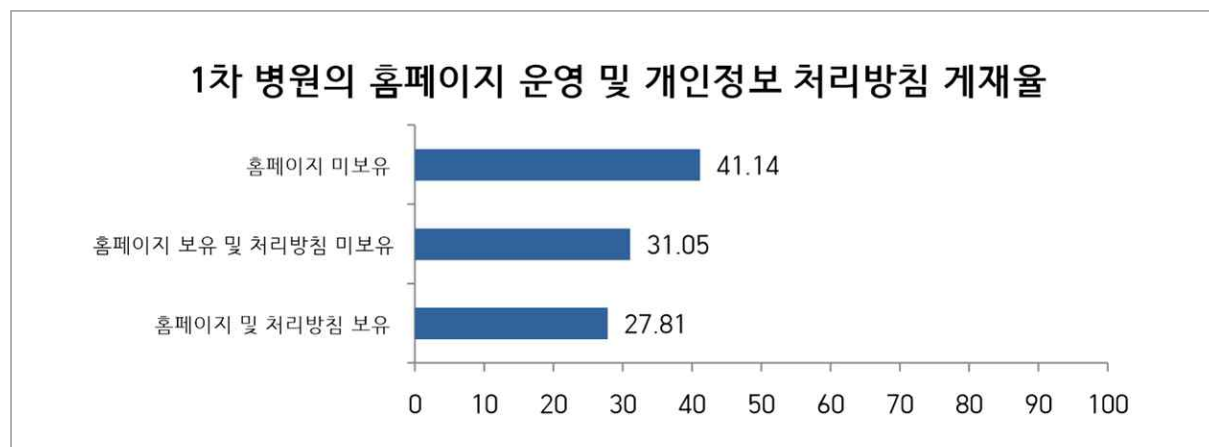
1차 병원의 경우, 전체 9,946개 중 58.86%에 해당하는 5,854개 병원이 홈페이지를 운영하고 있었으며, 그중 2,766개의 병원이 개인정보 처리방침을 게재하고 있었다. 그러나 개인정보 처리방침을 게재한 2,766개 병원 중에서 '개인정보 처리방침'이라는 표준 명칭을 사용한 병원은 1,176개에 불과했다. 이는 홈페이지를 운영하는 1차 병원의 20.09%만이 표준 개인정보 보호지침(2024)에 따른 정확한 명칭을 사용하여 개인정보 처리방침을 제공하고 있음을 의미한다. 2차 병원의 경우, 44개 병원 모두 홈페이지를 운영하면서 개인정보 처리방침을 게재하고 있었으나 표준 개인정보 보호지침(2024) 제20조 제1항에 따라 '개인정보 처리방침' 명칭을 사용한 병원은 37개로 정확한 명칭 사용 비율은 84.09%로 나타났다. 2차 병원뿐만 아니라 1차 병원에서도 홈 화면과 개인정보 처리방침의 제목에 '개인정보 처리방침'이 아닌 '개인정보 취급방침'이라는 잘못된 표현을 사용하는 경우를 다수 확인했다. 이는 표준 개인정보 보호지침(2024) 제20조 제1항에서 '개인정보 처리방침'이라는 표준화된 명칭을 사용하도록 명시한 규정을 위반하는 것이다. 3차 병원의 경우 14개의 모든 병원이 홈페이지를 운영하고 개인정보 처리방침을 게재하고 있었다. 또한 3차 병원의 경우, 14개 병원 모두 '개인정보 처리방침'이라는 표준 명칭을 올바르게 표기하고 있음을 확인하였다(표 2 참고).

표 2. 홈페이지 및 처리방침 보유 현황

구분	3차 병원	2차 병원	1차 병원
홈페이지 게재 여부	14/14 (100%)	44/44 (100%)	5854/9946 (58.86%)
처리방침 게재 여부	14/14 (100%)	44/44 (100%)	2766/5854 (47.25%)
'개인정보 처리방침' 명칭 사용 여부	14/14 (100%)	37/44 (84.09%)	1176/2766 (42.52%)

9,946개의 1차 병원 전체에서 홈페이지를 운영하며 개인정보 처리방침을 게재한 경우는 2차 병원(100%)과 3차 병원(100%)에 비해 27.81%로 낮은 비율의 양상을 보였다. 이를 통해 개인정보처리자는 개인정보 보호법(2023)을 근거하여 개인정보 처리방침을 수립하고 공개해야 하지만 이를 지키지 않고 있음을 확인할 수 있다(그림 1 참고). 다만, 1차 병원의 상당수가 홈페이지를 운영하지 않고 있어, 온라인에서 개인정보 처리방침을 확인하기 어려운 경우가 많았다.

그림 1. 그림으로 나타낸 1차 병원의 홈페이지 운영 및 개인정보 처리방침 게재율



2. 병원 규모별 항목 기재 현황

인터넷 홈페이지에 공개된 개인정보 처리방침을 통해 확인할 수 있는 필수 항목과 해당 시 기재해야 하는 항목의 비율을 조사하여 <표 3>으로 나타냈다. 필수 기재 항목에는 '개인정보 처리 목적', '처리하는 개인정보 항목', '동의/비동의 구분 및 법적 근거 기재', '개인정보 처리 및 보유 기간', '개인정보 파기 사항', '개인정보 안전성 확보조치', '정보주체 권리·의무 및 행사 방법', '개인정보 보호책임자', '정보주체의 권익침해 구제 방법', '개인정보 처리방침 변경'이 포함된다. 해당 시 기재항목에는 '개인정보 제3자 제공 사항', '개인정보 위탁 사항', '가명정보 처리 사항', '개인정보 자동 수집 장치 운영 및 거부 사항', '고정형 영상 정보처리기기 운영 및 관리 사항'이 있다(개인정보 보호법, 2023; 표준 개인정보 보호지침, 2024; 개인정보 보호법 시행령, 2024).

표 3. 개인정보 처리방침 항목 기재 현황

구분		3차 병원	2차 병원	1차 병원
필수 기재 항목 유무	개인정보 처리 목적	14/14 (100%)	43/44 (97.73%)	2,704/2,766 (97.76%)
	처리하는 개인정보 항목	14/14 (100%))	43/44 (97.73%)	2,685/2,766 (97.07%)
	동의/비동의 구분 및 법적 근거 기재	6/14 (42.86%)	13/44 (29.25%)	574/2,766 (20.75%)
	개인정보 처리 및 보유 기간	14/14 (100%)	44/44 (100%)	2,670/2,766 (96.53%)
	개인정보 파기 사항	14/14 (100%)	42/44 (95.45%)	2,401/2,766 (86.80%)
	개인정보 안전성 확보조치	14/14 (100%)	42/44 (95.45%)	1,957/2,766 (70.75%)
	정보주체 권리·의무 및 행사 방법	14/14 (100%)	43/44 (97.73%)	2,351/2,766 (85.00%)
	개인정보 보호책임자	14/14 (100%)	43/44 (97.73%)	2,432/2,766 (87.92%)
	정보주체 권익침해 구제 방법	14/14 (100%)	41/44 (93.18%)	2,028/2,766 (73.32%)
	개인정보 처리방침 변경	14/14 (100%)	42/44 (95.45%)	2,103/2,766 (76.03%)

구분		3차 병원	2차 병원	1차 병원
해당 시 기재 항목 유무	개인정보 제3자 제공 사항	14/14 (100%)	39/44 (88.64%)	2,014/2,766 (72.81%)
	개인정보 위탁 사항	14/14 (100%)	42/44 (95.45%)	1,888/2,766 (68.26%)
	가명정보 처리 사항	10/14 (71.43%)	4/44 (9.09%)	해당 없음.
	개인정보 자동 수집 장치 운영 및 거부 사항	14/14 (100%)	31/44 (70.45%)	2,325/2,756 (84.06%)
	고정형 영상 정보처리기기 운영 및 관리 사항	13/14 (92.86%)	32/44 (72.73%)	328/2,766 (11.86%)

3차 병원 모두 필수 기재 항목 중 '동의/비동의 구분' 및 '법적 근거 기재' 항목을 제외한 나머지 항목에서 100%의 기재율을 보였다. 그러나 '동의/비동의 구분 및 법적 근거 기재' 항목의 경우, 42.86%의 기재율로 비교적 낮게 나타났다. 이는 '처리하는 개인정보 항목에 진료 관련 사항이 올바르게 기재되었더라도, 의료법(2023)과 개인정보보호법(2023)에 따라 진료 관련 개인정보는 동의 없이 수집이 가능하다는 사실을 명시하지 않은 사례가 절반 가까이 됨을 시사한다.

개인정보처리자는 정보주체의 동의 없이 처리할 수 있는 개인정보의 항목과 그 처리의 법적 근거를 정보주체의 동의를 받아 처리하는 개인정보와 명확히 구분하여 개인정보 보호법(2023) 제30조 제2항에 따라 공개하거나, 서면, 전자우편, 팩스, 전화, 문자 전송 등으로 정보주체에게 고지해야 한다. 표준 개인정보 보호지침(2024) 제12조 제5항에서도 이 내용을 명시하고 있다. 2023년 3월, 「개인정보 보호법」 개정으로 개인정보의 수집 이용 제도가 개편되고, 개인정보 보호법(2023) 제22조 제3항에 따라, 정보주체의 동의 없이 처리되는 개인정보의 항목과 처리의 법적 근거를 동의받아 수집하는 개인정보와 별도의 항목으로 명확히 구분하여 기재해야 한다. 3차 병원에서도 해당 항목의 기재율이 낮은 것은 이러한 최근 개정된 법과 지침에서 신설·변경된 사항이 아직 처리방침에 반영되지 않았기 때문으로 판단된다. 이전 지침에서는 정보주체의 동의 없이 처리되는 개인정보의 항목과 법적 근거를 알리기 위해 노력해야 한다는 점을 강조하였으나, 개정된 지침에서는 동의받아 처리하는 개인정보와 구분하여 개인정보 처리방침에 명확하게 공개하거나, 서면 등의 방법으로 이를 반드시 고지해야 한다고 규정하고 있다. 개인정보 보호위원회에서 발간한 '개인정보 처리방침 작성지침 개정본'에서 또한 해당 부분을 강조하고 있다.

해당 시 기재 항목에서도 '가명정보 처리 사항(71.43%)', '고정형 영상 정보처리기기 운영 및 관리 사항(92.86%)'을 제외한 항목들이 100% 작성되었다. 이를 통해 3차 병원의 경우 대부분 개인정보 처리방침을 올바르게 작성하고 있던 것으로 확인된다.

44개의 2차 병원 중 '동의/비동의 구분 및 법적 근거 기재' 항목을 제외한 필수 항목이 93% 이상의 기재율을 나타냈다. 대부분의 필수 항목은 충실히 기재하였으나, '동의/비동의 구분 및 법적 근거 기재' 항목의 기재율은 29.55%로 낮게 나타났다. 해당 시 기재 항목에서는 '가명정보 처리 사항(9.09%)' 및 '개인정보 자동 수집 장치 운영 및 거부 사항(70.45%)'이 3차 병원에 비해 낮은 기재율을 보인다.

1차 병원(2766개)은 해당 시 기재 항목뿐만 아니라 필수 기재 항목의 기재율도 2차 병원과 3차 병원에 비해 전체적으로 낮은 편이다. '고정형 영상 정보처리기기 운영 및 관리 사항'은 11.86%로 가장 낮은 기재율을 보인다. 다만, '고정형 영상 정보처리기기 운영 및 관리 사항'은 개인정보 보호법(2023) 제25조 제7항에 따라 '고정형 영상 정보처리기기 운영관리 방침'을 개인정보 처리방침에 포함하여 작성하는 경우에만 분석되었기 때문에, 개인정보 처리방침에 기재하지 않았다고 해서 병원이 고정형 영상정보처리기기 운영관리 방침을 제정하고 공개하지 않았다고 단정하기 어렵다.

‘동의/비동의 구분 및 법적 근거 기재’ 항목은 병원 규모와 관계없이 다른 항목에 비해 낮은 기재율을 보였다. ‘동의/비동의 구분 및 법적 근거 기재’ 항목을 제외한 필수 기재 항목에서는 3차 병원의 100%, 2차 병원의 93% 이상, 1차 병원에서는 70% 이상을 기재하고 있다. 해당 시 기재 항목에서 가명정보 처리에 관한 사항을 제외했을 경우, 3차 병원의 100%, 2차 병원의 70% 이상, 1차 병원의 11% 이상이 작성되었음을 알 수 있다(표 3 참고).

3. 홈페이지 규모별 항목 미흡률

표 4. 개인정보 처리방침 기재 항목 미흡률

구분		3차 병원	2차 병원	1차 병원
필수 기재 항목 유무	개인정보 처리 목적	0/14 (0%)	4/44 (9.30%)	1,513/2,704 (55.95%)
	처리하는 개인정보 항목	0/14 (0%)	3/44 (6.98%)	1,526/2,685 (56.83%)
	개인정보 처리 및 보유 기간	0/14 (0%)	5/44 (11.36%)	1,612/2,670 (60.37%)
	개인정보 보호책임자	0/14 (0%)	0/44 (0%)	584/2,432 (24.01%)
	개인정보 제3자 제공 사항	0/14 (0%)	0/44 (0%)	143/2,014 (7.10%)
해당 시 기재 항목 유무	고정형 영상 정보처리기기 운영 및 관리 사항	0/13 (0%)	0/32 (0%)	39/328 (11.89%)
	개인정보 위탁 사항	0/14 (0%)	0/42 (0%)	273/1,888 (14.46%)

개인정보 처리방침을 조사할 때, 내용이 기준을 충족하지 못하거나 해당 항목에 대한 내용을 ‘000’으로 기재했을 경우 ‘미흡’으로 평가하였다. 필수 기재 항목 중 ‘개인정보 처리 목적’, ‘처리하는 개인정보 항목’, ‘개인정보 처리 및 보유 기간’, ‘개인정보보호 책임자’ 항목과 해당 시 기재 항목 중 ‘개인정보 제3자 제공 사항’, ‘개인정보 위탁 사항’, ‘고정형 영상 정보처리기기 운영 및 관리 사항’ 항목이 이에 해당한다. 각 항목의 구체적인 기준은 아래에 제시한다.

‘개인정보 처리 목적’ 항목을 작성할 때는, 개인정보처리자가 진료를 목적으로 정보주체의 개인정보를 수집한다는 점을 명확히 명시해야 한다. 그러나 1차 병원에서는 이를 제대로 기재하지 않은 경우가 절반을 넘는 것으로 나타났다. 구체적으로, 1차 병원의 ‘개인정보 처리 목적’ 항목 미흡률은 55.95%로, ‘개인정보 처리 목적’을 기재한 1차 병원 중 절반 이상(1513개)이 이 항목을 누락하거나 부정확하게 기재한 것을 확인할 수 있다. 2차 병원의 경우 미흡률은 9.30%로 비교적 낮은 편이며, 3차 병원은 이 항목을 모두 준수하여 미흡률이 0%를 보인다. 실제 병원의 개인정보 처리방침에서 확인한 “본원은 다음의 목적을 위하여 개인정보를 처리하고 있으며, 다음의 목적 이외의 용도로는 이용하지 않습니다.”, “-고객 가입 의사 확인, 고객에 대한 서비스 제공에 따른 본인 식별 인증, 회원자격 유지, 관리, 물품 또는 서비스 공급에 따른 금액 결제, 물품 또는 서비스의 공급, 배송 등”처럼 진료 목적으로 수집한다는 내용이 없었을 경우 ‘미흡’으로 평가하였다.

‘처리하는 개인정보의 항목’도 ‘개인정보 처리 목적’과 마찬가지로, 병원이 진료와 관련된 개인정보를 수집하고 처리함을 명확히 기재해야 한다. 그러나 1차 병원에서는 이 항목을 제대로 기재하지 않은 경우가 많았는데, ‘처리하는 개인정보의 항목’ 미흡률은 56.83%로, 절반 이상의 병원이 진료와 관련된 개인정보 항목을 작성하지 않은 것으로 나타났다. 2차 병원에서는 ‘처리하는 개인정보의 항목’의 미흡률이 6.98%를 보여 1차 병원에 비해 상대적

으로 양호했으며, 3차 병원은 모든 항목을 충실히 기재하여 미흡률이 0%를 보여 법을 준수하여 작성했음을 확인할 수 있다. 또한 “회사는 상담 등을 위해 아래와 같은 개인정보를 수집하고 있습니다.”, “온라인 문의 -수집 항목: 이름, 연락처, 이메일, 문의 내용 등”처럼 진료를 목적으로 어떤 개인정보를 수집한다는 내용이 없을 경우 ‘미흡’으로 평가하였다.

‘개인정보의 처리 및 보유 기간’ 항목에서는 개인정보 보호법(2023) 또는 의료법(2023)을 근거로 하여 수집한 진료 정보들을 의료법(2023)에 따라 보존한다는 내용을 명시해야 한다. 1차 병원은 이 항목을 제대로 기재하지 않은 경우가 많았으며 구체적으로, 1차 병원의 ‘개인정보의 처리 및 보유 기간’ 미흡률은 60.37%로, 절반 이상의 병원이 진료와 관련된 개인정보의 처리 및 보유 기간을 누락하거나 부정확하게 기재한 것으로 나타났다. 반면 2차 병원의 미흡률은 11.36%로 비교적 낮은 편이며, 3차 병원은 모든 항목을 충실히 기재하여 미흡률이 0%를 보인다.

‘개인정보 보호책임자’ 항목에서는 개인정보 보호법(2023) 제30조 제1항 제6호에 따라 개인정보 보호책임자의 성명 또는 개인정보 보호 업무 및 관련 고충 사항을 처리하는 부서의 명칭과 연락처(전화번호, 이메일 등)를 기재해야 한다. 그러나 일부 병원에서는 개인정보 보호책임자나 담당 부서의 연락처를 기재하지 않은 경우가 많았다. 특히, 1차 병원의 경우 24.01%의 병원이 책임자의 성명, 전화번호 또는 이메일 주소를 누락하여 정보주체가 개인정보 관련 문의를 할 수 있는 방법을 제대로 제공하지 않았다. 또한, ‘미흡’으로 평가된 일부 병원에서는 책임자의 성명을 명시하지 않고 직책만을 기재하거나 ‘홍길동’이나 ‘000’ 등으로 작성해 둔 경우도 확인되었다. 이는 정보주체가 책임자에게 직접적으로 접근하기 어렵게 만들어 「개인정보 보호법」의 요구사항을 충족하지 못하는 사례 중 하나로 분석된다.

해당 시 기재 항목은 실제로 해당하는 경우에만 작성하는 항목들로, ‘개인정보 제3자 제공 사항’, ‘개인정보 위탁 사항’, ‘고정형 영상 정보처리기기 운영 및 관리 사항’이 이에 해당한다. 이 항목들은 공통으로 제공 기관, 위탁 기관, 영상 정보 처리기기의 설치 대수나 위치 등을 명확히 기재하지 않고, ‘000’이나 ‘홍길동’ 같은 허위된 정보로 기재한 사례가 발견되었다. 이러한 기재 방식은 정보주체가 개인정보 제공 및 관리 상황을 정확히 파악할 수 없게 하며, 병원의 개인정보 보호 투명성을 저해할 수 있다. 그러나 실제로도 법적 예외를 제외하고 이러한 제공 및 위탁이 이루어지지 않는지, 혹은 처리방침에 명시하지 않은 상태에서 제공이나 위탁이 이루어지고 있는지는 확인할 수 없다. 따라서 본 연구에서는 병원이 처리방침을 정확하게 기재했음을 전제로 분석을 진행하였다.

1차 병원은 특히 개인정보 보호 책임자 정보와 같은 중요한 항목에서 미흡률이 2차, 3차 병원에 비해 높게 나타났다. 종합적으로, 본 연구 결과는 병원의 규모에 따라 홈페이지 운영률, 개인정보 처리방침 게재율, 표준 명칭 사용률, 그리고 필수 기재사항 및 해당 시 기재사항의 준수율에서 뚜렷한 차이가 있음을 보여주었다. 특히 3차 병원과 2차 병원이 대부분의 항목에서 높은 준수율을 보인 반면, 1차 병원은 전반적으로 낮은 준수율을 나타내어 의료기관 규모별 개인정보보호 수준의 격차가 존재함을 확인할 수 있었다.

V. 논의

1. 개인정보 처리방침 미기재, 미흡의 시사점

본 논문의 연구를 위해 서울시에 위치한 1차 병원 9,946개, 2차 병원 44개, 3차 병원 14개의 개인정보 처리방침을 확인하고 기재 항목 여부와 내용을 분류하면서 병원 관계자의 개인정보 처리방침에 대한 중요성 인식 부재를

더불어서 인지할 수 있는 또 다른 문제점은 홈페이지 위탁 업체가 제공하는 개인정보 처리방침을 해당 병원에 맞추어 수정하지 않은 채로 그대로 게재한다는 것이다. 조사를 통해 병원은 홈페이지, 블로그, 카페 등 여러 방식으로 홈페이지를 운영하고 있었음을 파악할 수 있었다. 개인정보 처리방침의 ‘개인정보 위탁 사항’ 항목을 분석한 결과, 홈페이지 위탁업체가 일치할 경우 개인정보 처리방침의 양식과 기재 항목의 내용이 동일하다는 문제점이 확인되었다. 이러한 특성으로 인해 본 연구의 방법론을 적용해 평가하게 되면, 홈페이지 위탁업체의 개인정보 처리방침에 대한 관심도에 따라 위탁한 해당 병원의 평가가 달라질 수 있으며, 여러 병원이 동일한 업체에 홈페이지 운영을 위탁할 경우 동일한 평가를 받게 된다. 이로 인해, 개인정보처리자가 개인정보 처리방침에 대한 인식이 부족하더라도 홈페이지 위탁업체가 개인정보 처리방침의 내용을 준수하게 작성했다면 본 연구 내에서는 ‘준수’로 표기하게 되어 올바른 개인정보 처리방침으로 평가하게 된다.

실제로 N사에서 제공하는 홈페이지 제작 기능으로 홈페이지를 운영하는 1차 병원의 개인정보 처리방침은 필수 기재 항목부터 해당 시 기재 항목까지 모두 기재된 개인정보 처리방침의 수보다 그렇지 않은 개인정보 처리방침의 수가 훨씬 많았다. 특히 ‘개인정보 제3자 제공 사항’과 ‘개인정보 위탁 사항’ 항목에서 “업체명: ○○택배사”, “위탁업무: 주문상품 배송”을 확인할 수 있는데 이 항목에서 병원이 실제로 작성한 것으로 보이지 않았으며 제공받은 개인정보 처리방침을 해당 병원에 맞추어 수정하여 기재한 것이 아니라 그대로 이용한 것으로 추측할 수 있다(표 5-1 참고).

또한, 홈페이지를 M사에 위탁한 다수의 병원 홈페이지에서는 공통적으로 필수 기재 항목인 ‘개인정보 처리방침 변경’에 관한 사항에서 처리방침 시행일의 날짜가 같다는 문제점을 확인할 수 있었다. 이를 통해 개인정보 처리방침의 내용이 정확하게 작성된 것이 아니라는 문제점을 알 수 있었다. 실제로 개인정보 처리방침이 같은 날짜에 수립되거나 변경되었을 가능성도 있지만, 해당 업체의 서비스를 이용한 병원에서만 동일한 날짜가 확인되었다는 점을 고려해야 한다(표 5-2 참고).

그러나 M사에 위탁하였음에도 처리방침의 모든 항목을 정확하게 작성한 병원도 있었다. 이는 개인정보 처리방침의 작성 및 공개 수준이 병원의 관리 체계와 개인정보 보호책임자의 인식 수준에 따라 달라질 수 있음을 보여준다.

본 연구는 개인정보 처리방침을 미흡하게 작성하거나 공개하지 않은 병원들이, 「개인정보 보호법」 및 관련 법률을 준수하여 개인정보 처리방침을 작성한 병원을 참고하여 해당 병원에 맞추어 작성할 수 있었음에도 불구하고, 개인정보 보호법(2023) 제3조에서 명시한 개인정보처리자의 책임 이행과 신뢰성 확보를 위한 충분한 노력을 기울이지 않았음을 시사한다.

표 5-1. N사에 위탁한 개인정보 처리방침의 ‘개인정보 제3자 제공 사항’ 및 ‘개인정보 위탁 사항’ 항목의 내용

3. 개인정보의 제3자 제공 및 처리 위탁
법령에 의거하여 제3자 제공 및 처리 위탁 동의가 필요한 경우에는 이용자에게 명시적으로 통의를 받습니다.
공개로 동의를 대신할 수 있는 처리 위탁은 아래와 같습니다.
-업체명: ○○택배사
-위탁업무: 주문상품 배송

표 5-2. N사에 위탁한 개인정보 처리방침의 ‘개인정보 처리방침 변경’ 항목의 내용

-공고일자: 2017년 12월 22일
-시행일자: 2017년 12월 29일

개인정보 보호법 시행령(2024) 제63조(과태료의 부과 기준) [별표 2]에 따라, 개인정보 처리방침을 수립하지 않거나 공개하지 않은 병원은 1회 위반 기준 200만 원의 과태료가 부과될 수 있다. 본 연구에서 확인한 바에 따르면, 3,088개의 1차 병원이 홈페이지에 개인정보 처리방침을 공개하지 않은 것으로 나타났으며, 이러한 병원들은 법적으로 200만 원의 과태료 부과 대상이 될 수 있다. 그러나 홈페이지를 통한 개인정보 처리방침의 유무를 조사나, 홈페이지를 미운영하는 병원의 경우 오프라인에서 기재 여부를 확인하는 절차가 이뤄지지 않았기 때문에, 개인정보 처리방침을 게시하지 않은 병원에 실제로 과태료가 부과되고 있다고 단정하기는 어렵다. 이는 개인정보 처리방침의 게재뿐만 아니라, 법적으로 규정된 사항들이 실제로 준수되지 않는 경우가 많을 수 있음을 시사한다.

개인정보 처리방침을 게재하지 않은 병원들의 경우, 의료진이 개인정보에 대한 법률을 충분히 인지하지 못했거나, 혹은 인지하고 있음에도 개인정보 처리방침의 작성 및 게재의 중요성을 간과했을 가능성이 있다. 본 연구의 조사 과정에서 개인정보 처리방침을 게시하지 않았으나, 의료법(2023)에 명시된 환자의 권리와 의무에 대해 홈페이지에 별도로 게재한 사례를 확인할 수 있었다. 이는 해당 병원이 개인정보와 환자 권리에 대해 일부 주의를 기울였으나, 개인정보 보호법(2023) 제30조에서 요구하는 개인정보 처리방침의 작성 및 공개 의무에 대한 이해가 미흡했음을 보여준다.

또한 본 연구는 서울에 위치한 1차, 2차, 3차 병원 총 10,004개의 홈페이지 운영 여부와 홈페이지에 기재된 개인정보 처리방침의 항목의 기재 유무 및 내용을 평가하였기에 표본의 개수가 부족하여 연구 결과를 일반화하기 어렵다는 한계를 지닌 기존 연구들과 달리, 본 연구는 병원의 개인정보 처리방침 보유 현황과 기재 항목 내용의 준수 정도에 대해 더 포괄적인 결론을 도출할 수 있었다. 이러한 연구 결과는 향후 개인정보 처리방침의 현황을 분석하려는 연구자들에게 유용한 참고 자료가 될 것으로 기대된다.

2. 병원 규모별 개인정보보호 수준 격차와 시사점

본 연구 결과는 병원의 규모에 따른 개인정보 보호 수준의 격차를 명확히 보여주었다. 특히, 상급종합병원과 종합병원의 경우 전문적인 개인정보 보호책임자와 담당 부서를 보유하고 있어 처리방침 게재와 작성 방식을 적절히 준수하고 있는 반면, 1차 병원과 같은 소규모 병원들이 재정적·기술적 한계로 인해 법적 요구 사항을 제대로 충족하지 못하고 있다는 사실이 드러났다. 이는 소규모 의료기관에서 개인정보 보호를 위한 체계적인 지원이 필요함을 시사한다. 1차 병원의 개인정보 처리방침 공개율이 낮고, 표준 용어 사용 비율이 현저히 떨어지는 점은 병원 자체의 인식 부족뿐만 아니라, 해당 병원이 처리방침 수립에 필요한 전문 지식과 자원이 부족하다는 것을 의미한다. 특히 개인정보 보호 책임자 정보, 개인정보 위탁 사항, 고정형 영상 정보처리기기 운영 및 관리 사항과 같은 항목에서 1차 병원의 미흡률이 높게 나타난 것은 이러한 현실을 반영한다. 다만, 개인정보 보호법 시행령(2024) 제31조 제3항에 따르면 병원 내부에 개인정보 처리방침을 게시하는 것도 법적 요건을 충족할 수 있는 방법이므로, 단순히 홈페이지 미보유나 미게재를 법적 요구사항 미준수로 단정 짓기는 어렵다. 그러나 처리방침을 병원 내부에만 게시할 경우 환자나 보호자의 정보 접근성이 제한될 수 있어, 온라인 공개를 통한 접근성 향상이 필요하다.

병원의 정보보호 수준을 향상하기 위해 개인정보 보호 관련 지침과 규제에 대한 명확한 안내가 필요하다. 병원들이 복잡한 법적 요구 사항을 이해하고 준수할 수 있도록 구체적인 지침과 지원을 제공하는 것이 중요하다. 특히, 정부나 관련 기관은 1차 병원을 대상으로 한 맞춤형 교육 프로그램이나 처리방침 자동 생성 도구를 개발해 제공함으로써, 법적 요구 사항을 더욱 쉽게 이해하고 적용할 수 있도록 해야 한다. 이는 병원 규모에 따른 격차를 줄이고, 보다 일관된 개인정보 보호 정책의 적용을 가능하게 할 것이다.

또한, 「개인정보 보호법」의 요구 사항을 준수하는 데 있어 병원의 규모뿐만 아니라, 병원의 운영 방식과 정책적

인 요소도 중요한 역할을 할 수 있다. 예를 들어, 대형 병원은 체계적인 IT 인프라와 전담 인력을 통해 개인정보 보호에 필요한 기술적·관리적 보호 조치를 충분히 시행할 수 있지만, 소규모 병원은 비용 및 인력의 제약으로 인해 그러한 시스템을 갖추는 데 어려움을 겪을 수 있다. 이와 같은 격차는 단순히 병원의 규모만이 아니라, 병원 운영의 재정적 구조와 정부의 지원 정책의 부족에서 기인할 수 있으며, 이를 해소하기 위한 체계적 지원이 필요하다.

3. 연구의 한계 및 후속 연구 제언

본 연구의 한계는 다음과 같다. 첫째, 서울 지역 병원만을 대상으로 하였기 때문에 전국적인 상황을 반영하지 못했다는 점이다. 서울 이외의 지역 병원, 특히 지방에 위치한 병원들은 서울에 비해 더 큰 재정적·기술적 한계를 가질 가능성이 있으며, 이에 대한 연구가 부족하다는 점을 고려해야 한다. 이를 보완하기 위해, 향후 연구에서는 다양한 지역을 포함한 확대된 분석을 통해 병원 규모와 지역별로 차별화된 개인정보 보호 수준을 평가해야 한다. 둘째, 병원 홈페이지에 게시된 개인정보 처리방침만을 분석하였으므로, 실제 운영 중인 보안 조치의 실효성을 평가하는 데 한계가 있다. 병원이 온라인으로 공개한 정보가 실제 운영 환경과 일치하지 않을 가능성이 있기 때문에, 병원 내부의 보안 조치가 실제로 어떻게 이행되고 있는지를 확인하는 현장 조사가 필요하다. 마지막으로, 홈페이지를 운영하지 않고 오프라인으로 처리방침을 게재한 경우는 조사하지 못했다는 점이다. 이는 병원이 오프라인에서 처리방침을 제공하는 방식이 환자와 보호자에게 얼마나 접근성이 있는지에 대한 평가가 필요함을 시사한다. 향후 연구에서는 이러한 오프라인 조사를 통해 병원들이 실제로 법적 요구 사항을 준수하고 있는지를 평가해야 하며, 처리방침이 오프라인으로만 제공될 경우 환자나 보호자에게 충분한 정보 접근성을 제공하고 있는지 분석할 필요가 있다.

또한, 본 연구는 웹사이트 분석을 통한 정량적 연구방법을 채택하였다. 이는 대규모 의료기관의 현황을 객관적으로 파악할 수 있다는 장점이 있으나, 의료기관이 개인정보 처리방침을 제대로 게시하지 못하는 실질적인 원인과 어려움을 파악하기에는 한계가 있다. 따라서 향후 연구에서는 정성적 연구를 통해 병원의 개인정보 보호 조치의 운영 실태와 의료진 및 환자의 처리방침 인식을 심층적으로 조사할 필요가 있다. 특히 1차 의료기관의 낮은 준수율의 근본적 원인을 이해하기 위해서는 병원 관리자 인터뷰나 설문조사 등을 통해 정보보호 체계와 실제 관리 수준에 대한 면밀한 분석이 요구된다. 이러한 정성적 연구를 통해 소규모 병원의 현실적 어려움을 파악하고 그에 맞는 맞춤형 지원책을 마련할 수 있을 것이다. 이는 소규모 병원의 「개인정보 보호법」 준수를 용이하게 하고, 궁극적으로 환자의 신뢰를 강화하며 보다 안전한 의료 환경을 조성하는 데 기여할 수 있을 것이다.

VI. 결론

본 연구는 개인정보 처리방침의 법적 준수와 명칭 사용 현황을 병원 규모별로 분석하였다. 이를 통해 1차 병원(의원), 2차 병원(병원, 종합병원), 3차 병원(상급종합병원)의 개인정보 처리방침 보유 및 명칭 사용 실태를 체계적으로 평가하였다. 개인정보 보호법(2023) 제30조 제1항에 따라, 개인정보처리자는 개인정보 처리방침을 수립하고 공개할 의무가 있으며, 본 연구는 이러한 법적 요구가 실제로 어떻게 이행되고 있는지를 평가하였다.

연구 결과, 3차 병원(상급종합병원)의 경우 모든 병원이 홈페이지와 개인정보 처리방침을 보유하고 있으며, 모든 3차 병원이 '개인정보 처리방침'이라는 올바른 명칭을 사용하고 있다. 2차 병원(병원, 종합병원)의 경우, 모든 병원이 개인정보 처리방침을 보유하고 있었으나, 명칭의 정확한 사용 비율은 84.09%로 일부 병원에서는

부정확한 명칭을 사용하고 있음을 확인했다. 1차 병원(의원)의 경우, 58.86%만이 홈페이지를 운영하고 있었으며, 이 중 47.25%만이 개인정보 처리방침을 보유하고 있었다. 특히, 홈페이지에 개인정보 처리방침을 보유한 병원 중에서 명칭의 정확한 사용 비율은 42.52%로 저조했다. 즉, 홈페이지를 운영하는 1차 의료기관을 기준으로 했을 때, 20.09%만이 정확한 명칭의 개인정보 처리방침을 제공하고 있었다. 이러한 결과는 특히, 1차 병원의 개인정보 처리방침 작성 및 공개가 미흡하다는 점을 시사하며, 개인정보 보호법(2023) 제30조의 규정을 명확히 이해하고 준수할 필요가 있음을 강조한다.

개인정보 처리방침의 필수 기재 항목과 관련해서도, 3차 병원은 대부분의 항목을 충실히 기재하고 있었으나, 2차 병원과 1차 병원에서는 일부 항목의 기재율이 낮게 나타났다. 특히, 1차 병원은 ‘동의/비동의 구분 및 법적 근거 기재’ 항목의 기재율이 매우 낮았다. 이는 2024년에 개정된 개인정보 보호법(2023)에서 강조된 사항을 제대로 이행하지 않음으로써 1차 병원들이 개인정보 처리방침의 작성과 공개에서 법적 요건을 충분히 이해하지 못하고 있음을 반영한다. 그뿐만 아니라 이는 개인정보 처리방침의 적정성 및 준수 여부에 대한 관심과 규제의 강화가 필요한 시점임을 의미한다. 특히, 1차 병원의 경우 타 기관에서 제공한 개인정보 처리방침을 수정하지 않고 그대로 가져오는 경우가 다수 존재하며, 이를 개선하기 위한 교육과 정책적 지원이 필요하다.

본 연구는 개인정보 처리방침의 명칭 사용 및 기재 현황을 체계적으로 분석하여 병원 규모에 따른 차이를 명확히 규명하였으며, 이를 통해 개인정보 보호의 중요성과 법적 준수의 필요성을 다시 한번 강조하였다. 향후 연구에서는 병원 내부에서 개인정보 처리방침을 어떻게 운영하고 관리하는지, 실제로 개인정보 보호 조치가 얼마나 효과적으로 이행되고 있는지에 대한 추가 조사가 필요하다. 이러한 연구는 병원의 개인정보 보호 수준을 높이고, 환자와 보호자가 개인정보 처리방침에 쉽게 접근할 수 있도록 하는 데 기여할 것이다.

결론적으로, 본 연구는 병원들이 개인정보 보호법(2023)을 준수하여 개인정보 처리방침을 정확히 작성하고 공개함으로써 개인정보 보호의 신뢰성을 제고하는 데 중요한 기초 자료로 활용될 수 있을 것이다. 향후 정책적 개선과 병원의 적극적인 참여를 통해 개인정보 보호 수준이 한층 더 강화될 것으로 기대된다.

향후 연구에서는 1차 병원 의사들이 쉽게 사용할 수 있는 개인정보 처리방침 자동 생성기를 개발하는 것을 목표로 하고자 한다. 이러한 생성기는 개인정보 보호법(2023)의 규정에 맞춘 표준화된 개인정보 처리방침을 자동으로 작성해 줌으로써, 법적 요구사항을 잘 모르는 병원들도 손쉽게 적절한 개인정보 처리방침을 마련할 수 있도록 도울 것이다. 이는 1차 병원의 개인정보 보호 수준을 높이고, 과태료 부과를 줄이는 데 실질적인 도움을 줄 수 있을 것으로 기대된다.

탁지원(주저자)은 서울여자대학교에서 제1전공 정보보호학과, 제2전공 개인정보보호학과 학사과정 중이다. 주요 관심 분야는 개인정보보호, 인공지능이며, 현재 관련 연구를 진행 중이다.

(E-mail: jiwontark@naver.com)

김서현(공동저자)은 서울여자대학교 정보보호학과를 전공하고 있으며, 부전공으로 개인정보보호학과를 이수 중이다. 주요 연구 관심 분야는 데이터 보안, 인공지능, 프라이버시 보호 기술 등이다.

(E-mail: emily7868@swu.ac.kr)

민기단(공동저자)은 서울여자대학교 제1전공 정보보호학과, 제2전공 개인정보보호학과 학사과정 중이다. 주요 관심 연구 분야는 사이버 보안, 데이터 보호, 개인정보보호이다.

(E-mail: airmass@swu.ac.kr)

장수영(공동저자)은 서울여자대학교에서 정보보호학과 학사과정 중이다. 주요 관심 분야는 개인정보보호, 시스템보안, 웹보안 등이다.

(E-mail: suyeongjj@gmail.com)

오준형(교신저자)은 고려대학교 정보보호대학원에서 박사학위를 받았으며, 서울여자대학교 정보보호학부에서 교수로 재직 중이다. 주요 관심 분야는 개인정보보호이며, 인공지능 기반의 개인정보보호 자동화 및 개인정보보호 위험 관리 등을 연구하고 있다.

(E-mail: ohjun02@gmail.com)

참고문헌

- 강지원. (2018). 병원 간호사의 의료정보보안 측정도구 개발 [박사학위논문, 고려대학교]. <https://dcollection.korea.ac.kr/srch/src/hDetail/000000080107>
- 개인정보 보호법, 법률 제19234호 (2023).
- 개인정보 보호법 시행령, 대통령령 제34309호 (2024).
- 개인정보보호위원회. (2024. 7.). 개인정보위, 환자정보 유출 17개 종합병원 제재. 대한민국 정책브리핑. <https://korea.kr/briefing/pressReleaseView.do?newsId=156582640>
- 건강보험심사평가원. (2024). 병원·약국 종류별 찾기 [데이터 세트]. 건강보험심사평가원 홈페이지. <https://www.hira.or.kr/ra/healthMap/getHealthMap.do?pgmid=HIRAA030002010000&WT.gnb=%EB%B3%91%EC%9B%90+%C2%B7+%EC%95%BD%EA%B5%AD%EC%B0%BE%EA%B8%B0>
- 박선재. (2023, 9. 14.). 의원급 의료기관 개인정보 자율점검 이렇게만 하세요! 의협신문. <https://www.doctorsnews.co.kr/news/articleView.html?idxno=151404>
- 백운철. (2005). 우리나라에서 의료정보와 개인정보보호 헌법학연구, 11(1), 418. <https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART001159815>
- 백인주, 오준형, 이경호. (2019). 안드로이드 환경에서 개인정보 처리방침의 투명성 확보방안에 관한 연구: GDPR을 기반으로 정보보호학회논문지, 29(6), 1477-1489. <https://doi.org/10.13089/JKIISC.2019.29.6.1477>
- 신민지, 이창무, 조성필. (2019). 중소형 의료기관의 개인정보 보안 실태 및 개선방안. 융합보안논문지, 19(4), 123-132. <https://scienceon.kisti.re.kr/srch/selectPORSrchArticle.do?cn=JAKO201925863869241&SITE=CLICK>
- 심혜연. 권민서, 윤다영, 서지영, 이일구. (2024). GPT를 활용한 개인정보 처리방침 안전성 검증 기법. 정보보호학회논문지, 34(2), 207-216. <https://doi.org/10.13089/JKIISC.2024.34.2.207>
- 오진석. (2020). 의료기관의 개인정보처리 문제점과 개선방안 [석사학위논문, 아주대학교 정보통신대학원]. dCollection@ajou. <http://dcoll.ajou.ac.kr:9080/dcollection/common/orgView/000000029573>
- 의료법, 법률 제19818호 (2023).
- 이은숙, 이준기, 차경진. (2016). 개인정보 취급방침의 인지가 개인정보보호 행동에 미치는 영향: 카카오톡 이용자를 중심으로 The Journal of Society for e-Business Studies, 21(2), 135-150. <http://dx.doi.org/10.7838/jsebs.2016.21.2.135>
- 이재근, 강상욱, 염홍열. (2013). 개인정보 처리방침의 데이터를 활용한 개인정보보호 현황 분석. 한국정보보호학회 논문지, 23(4), 767-780. <https://doi.org/10.13089/JKIISC.2013.23.4.767>
- 이한주. (2012). 의료영역에서의 개인정보보호의 문제점과 해결방안. 한국의료법학회지, 20(2), 267-293. <https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART001723461>
- 정영철. (2014). 우리나라 상급종합병원의 개인정보 처리방침 운영실태. 보건복지포럼, (212), 49. <https://kiss.kstudy.com/Detail/Ar?key=3540733>
- 정윤교. (2023). 안드로이드 정적 분석을 활용한 개인정보 처리방침의 신뢰성 분석. 한국정보처리학회, 12(1), 17-24. <https://kiss.kstudy.com/Detail/Ar?key=3957815>
- 정찬모. (2013). 개인정보취급방침 심사와 개인정보보호 감사제도 도입방안. 법학논총, 20(1), 3-29. https://www.kci.go.kr/kciportal/landing/article.kci?arti_id=ART001764631
- 조용현, 차영균. (2020). 딥러닝을 활용한 개인정보 처리방침 분석 기법 연구. 정보보호학회논문지, 30(2), 305-312. <https://doi.org/10.13089/JKIISC.2020.30.2.305>
- 최선영, 임도연, 고일선, 문인오. (2016). 보건계열 대학생의 환자 의료 정보 보호에 대한 인식과 수행. 한국간호교육학회지, 22(1), 83-95. <http://dx.doi.org/10.5977/jkasne.2016.22.1.83>
- 표준 개인정보 보호지침, 개인정보보호위원회고시 제2024-1호 (2024).

- 한국인터넷진흥원. (2021. 6. 28.) 2021 개인정보보호실태조사. <https://www.kisa.or.kr/20505/form?postSeq=2&page=1#findoDocumentPreview>
- 한국정보보호산업협회. (2024. 2.) 2023 정보보호실태조사. https://www.kisia.or.kr/research/reference_board/31/
- 홍주연, 김환희. (2019). 개인정보 보호에 대한 의료기관 종사자들의 인식수준에 관한 연구. *한국엔터테인먼트산업학회논문지*, 13(8), 647-659. <https://doi.org/10.21184/jkeia.2019.12.13.8.647>
- 황지환. (2017). 의료기관의 개인정보 보호의 현황과 향후 개선방안. *의료정책포럼*, 14(4), 56-61. <https://www.riss.kr/link?id=A103043774>
- Anderson, J-G. (2000). Security of the distributed electronic patient record: a case-based approach to identifying policy issues. *International Journal of Medical Information*, 60(2), 111-118. [https://doi.org/10.1016/S1386-5056\(00\)00110-6](https://doi.org/10.1016/S1386-5056(00)00110-6).
- Jang, S. C. (2007). Problem in the civil law and the protection of medical information. *Legal Research*, 28, 159-180. <https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE00923950>

Analysis of Personal Information Protection Act Compliance in Privacy Policies of Seoul Medical Institutions: Focusing on Website Disclosures

Tark, Ji Won¹ | Kim, Seo Hyeon¹ | Min, Gi Dan¹ | Jang, Su Yeong¹ | Oh, Jun Hyoung^{1*}

¹ Seoul Women's University

* Corresponding author:
Oh, Jun Hyoung
(ohjun02@gmail.com)

| Abstract |

This study analyzed the current state of privacy policies in medical institutions in Seoul, evaluating differences based on their size. The Personal Information Protection Act requires medical institutions to disclose and state their privacy policies; however, systematic research on actual compliance remains insufficient. Of the 10,004 medical institutions in Seoul (14 tertiary, 44 secondary, and 9,946 primary), we focused on those with websites, examining whether their privacy policies were posted and kept up to date. The analysis found that all secondary and tertiary institutions were running their websites and generally met most legal requirements. However, primary institutions with websites only posted their privacy policies without further updates. This pattern was consistent across institutions, highlighting the need for stronger personal information protection and enhanced measures, particularly for primary medical institutions. This study provides foundational data for improving personal information protection in medical institutions.

Keywords: Privacy Policy, Privacy Policy Implementation Status, Medical Institutions, Personal Information Protection Act