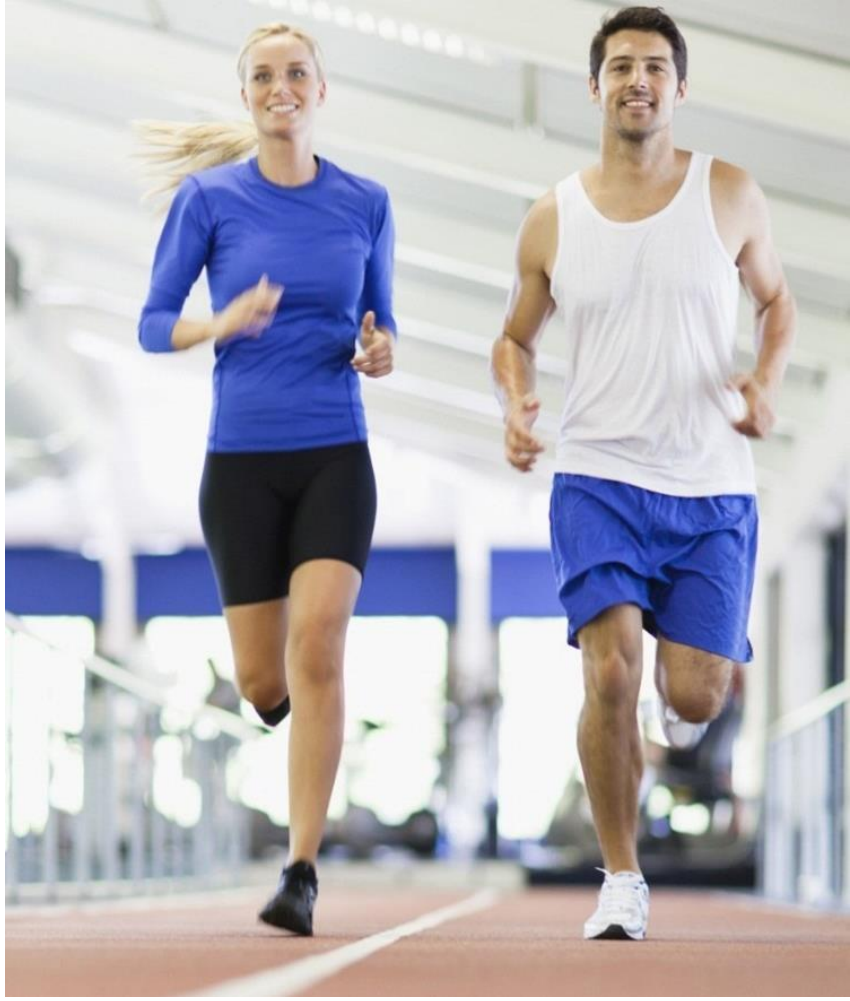




디지털 헬스케어 산업 활성화에 따른 개인정보보호 및 정보보호 관리체계 운영 방안

GC케어 최중우

1. 헬스케어 산업의 발달

헬스케어 산업은 디지털 기술 아래서 급진적으로 변화해 가고 있다. 세계적 대유행인 **코로나19를 통해 원격의료 및 빅데이터를 통한 개인의 맞춤형 건강관리**에 대해 전 세계가 시대 변화에 도전하고 있다.

헬스케어 산업의 확장은 **개인의 건강 관리를 위한 영역**과 **원격의료를 위한 의료 데이터 영역**에 대한 관심이 커지고 있다.

그에 따른 **개인의 의료정보 및 건강정보를** 다루고 있는 다수의 의료기관 및 헬스케어 기업에 대한 **정보보안 및 개인정보보호 중요성도 상승**하고 있다.

1. 헬스케어 산업의 발달

EMR(전자의무기록)은 종종 EHR(전자건강기록)이라고 불리는데, 주로 병원에서 쓰이는 **환자의 의료/건강 관리 전반에 대해 시스템화**한 것으로 환자의 인적 기록부터 진료, 처방 등 병력까지 모든 의료 정보가 기록되기 때문에 **대량의 헬스케어 데이터를 얻는 데 중요한 역할**을 하고 있으며 빅데이터 분석의 선결 조건이 대량의 데이터인 만큼, **헬스케어 산업에서 중요한 역할**로 자리매김하고 있다.

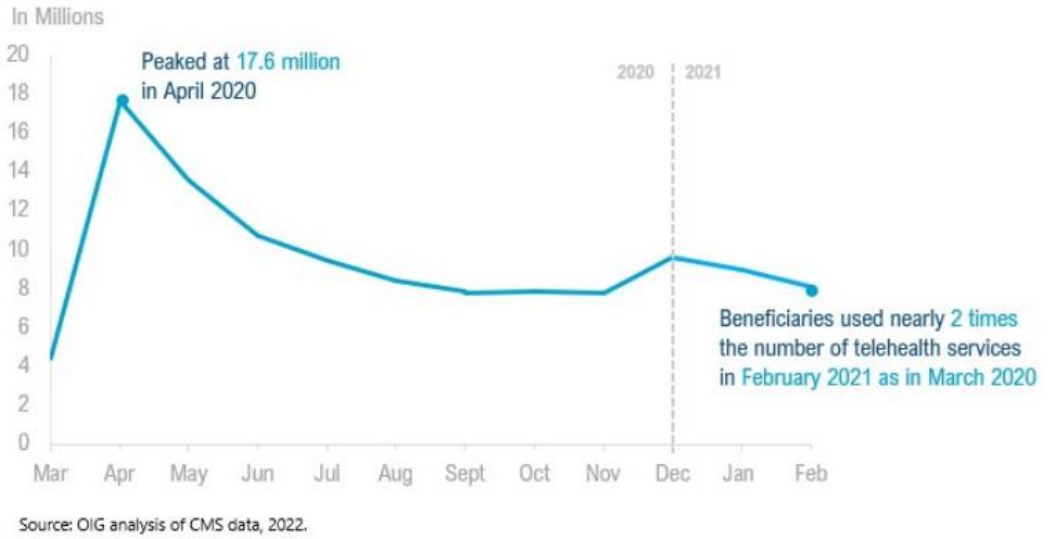
	EMR	EHR
내용	의료기록	의료기록 뿐아니라 환자의 전체적인 건강정보를 포함
의료기관 공유	타 의료기관과 공유되지 않음	타 의료기관에서 공유됨
환자 공유	본인에게 공유되지 않음	본인도 열람 가능

<표1. EMR/EHR 비교>

1. 헬스케어 산업의 발달

2017년 미국 내 전체 병원 중 96%는 EHR을 도입했다. 특히 **대형병원의 도입율은 99%를 기록**했으며 지방 소형 병원도 도입율이 93%에 육박할 정도로 매우 높다. 전자의무기록 도입이 보편화되면서 종이차트 사용으로 인한 불편함이 크게 감소했다. 2008년 9.4%에 불과했던 도입률이 7년만에 9배 상승한 것이다. 당연한 얘기지만 규모가 작고 시골에 위치할수록 EMR 보급률이 떨어진다고 한다. **한국의 경우 거의 모든 병/의원이 EMR을 사용**하고 있다고 하겠다.

2. 미국 헬스케어 산업



<그림1. 최근 미국 원격 의료 서비스 이용자수 동향,자료:미국 보건복지부>

○ 원격 의료 (홈케어)

미국 보건복지부에서 2022년 3월 15일 발표한 보고서에 따르면 **미국에서 코로나19 발생 첫 해(2020년 3월~2021년 2월)에 2800만 명이 넘는 메디케어 수혜자가 원격 의료 서비스를 이용**한 것으로 나타났으며, 이는 전년도**(2019년)보다 88배 폭증**한 것으로 전체 메디케어 수혜자의 약 43%에 해당하는 수치다.

미국 보건복지부에서는 코로나19 발생 첫 해 메디케어 수혜자에게 의료서비스를 제공하는데 원격의료가 매우 중요한 역할을 했으며, 원격의료가 의료서비스의 접근성을 높일 수 있는 잠재력을 보여줌으로 **향후 연방 기관인 CMS(Centers for Medicare and Medical Services)가 원격 의료 서비스의 영구적 허용 여부를 고려할 때 중요한 사항**으로 보고 있다.

2. 미국 헬스케어 산업

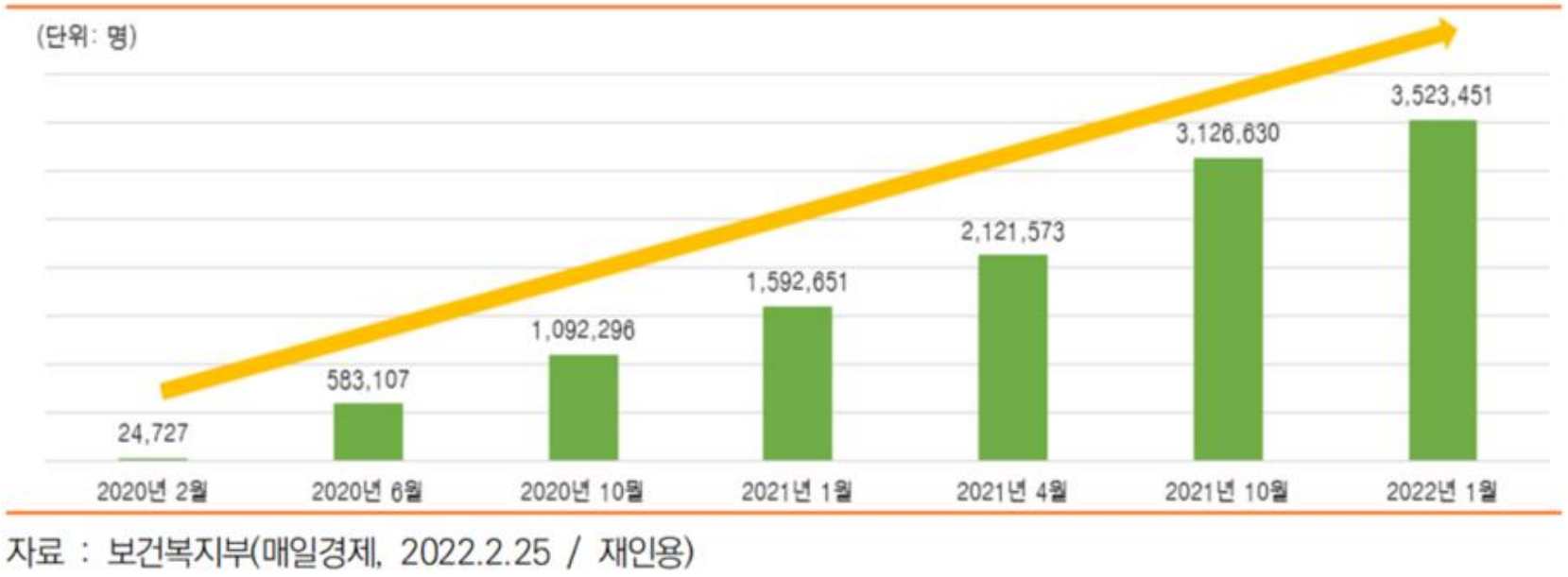
글로벌 컨설팅 회사인 **McKinsey**는 **많은 미국인들이 병원에 가지 않고 가정에서 치료 서비스를 받을 수 있는 홈케어를 선호하고 있다고 분석**하였으며, 미국 메디케어 행위별 수가제(Fee-for Service)* 및 메디케어 어드밴티지(MA) 수요자 중 최대 2650억 달러 규모 의료서비스가 **2025년까지 전통적인 병원 치료 형태에서 홈케어로 이동할 것으로 전망**했다.

* 의료인이 제공한 의료서비스에 대해 서비스 별로 가격을 정하여 사용량과 가격에 의해 진료비를 지불하는 제도

McKinsey는 홈케어 서비스 진행시 **1차 진료, 외래 환자 전문의 상담, 응급실 및 긴급 의료 서비스, 호스피스, 정신건강/행동건강 분야 외래환자 상담 서비스 등이 속하는 그룹**은 특히 코로나19 팬데믹 기간 동안 이용량이 급증했으며 홈케어 부문 주요서비스로 확장될 가능성이 큰 것으로 보고 가정 기반 투석과 같은 신흥 영역도 빠르게 성장하고 있다고 분석했다.

3. 국내 헬스케어 산업

- 코로나19 초기 경증환자는 생활치료센터에서 치료를 받았지만, **확진자의 급증으로 재택 '자가치료'로 정부 방침이 변경**되면서 비대면 진료가 증가하였다.
- **비대면 진료 서비스는 환자가 앱에 개인 정보와 증상을 입력해서 원하는 진료 과목을 선택하여 병원을 연결해서 전화, 화상 진료를 볼 수 있으며 처방전을 약국에 연결해 약을 배송받음**
- 코로나19 사태 속 내원이 불가능한 여건에서 **시간·공간에 구애받지 않고 진료와 처방**을 받음



자료 : 보건복지부(매일경제, 2022.2.25 / 재인용)

<표3. 비대면 진료 환자 수 추이>

4. 헬스케어 산업의 변화(게임)

- 디지털 치료제 분야 임상 증가

  Akili Interactive는 스마트폰 및 태블릿 장치에서 몰입형 비디오 게임 경험을 통해 8-12세 아동 주의력 결핍 행동장애(ADHD, 주의력 결핍 과잉행동장애)를 치료할 수 있는 최초 FDA 승인 디지털 치료제'EndeavorRx'를 선보였다.

  의학저널인 PLOS ONE에 게재된 사항에 따르면 'EndeavorRx'로 치료한 경우 뇌파 검사결과에서 주의력 기능과 관련된 뇌 활동이 증가한 것으로 나타났다.


AMERICA
GMA

4. 헬스케어 산업의 변화(메타버스)

ㅇ 의료계 신사업, 메타버스

메타버스와 의료서비스를 연결하는 기술로 **AR/VR을 통해 의료서비스 제공자와 환자가 치료, 교육, 보조 목적으로 환자 자신의 가상세계 속 아바타를 통해 가상공간에서 시뮬레이션**하여 결과를 미리 예측하고 최적화한 기술을 의료분야에 적용하는 것이다.

미국에서는 이미 **해당 분야 및 기술을 기반으로 하는 스타트업이 속속 등장하며 투자 자금을 지원받는 기조가 형성**되는 중이며 디지털 헬스 분야 시장 인사이트를 제공하는 Rock Health 분석에 따르면 2021년 기준 11건의 거래에서 AR/VR 기술을 통합하는 미국의 디지털 헬스분야 스타트업에 1억9800만 달러의 자금이 조달됐으며, 해당 금액은 2020년 대비 2배 이상 오른 것으로 나타났다.

5. 헬스케어 시스템 보안 위협

미국의 주요 병원에 **EHR, 전자 처방 및 의사 결정 지원 시스템, 지능형 난방, 환기 및 공조(HVAC), 주입 펌프, 의료 사물 인터넷(IoMT) 장치** 등 모두 사이버 범죄 위협을 받고 있다.

의료 기관에서는 환자의 개인정보보호를 통해 양질의 진료를 제공하고 HIPAA , GDPR 및 기타 규정을 준수하여 균형을 유지하고자 한다. 위협을 받는 유형으로 **피싱, MITM, 네트워크 취약성 공격, 랜섬웨어**를 들 수 있다.

- 피싱 : 피싱 이메일, 소셜 미디어 또는 문자 메시지의 링크 또는 첨부 파일은 종종 임상 네트워크를 통해 확산되는 악성코드로 컴퓨터 시스템을 감염한다.
- MITM(Man-in-the-Middle) 공격 : 사이버 범죄자는 대화나 데이터 전송에 자신을 투입하고 사용자 기밀 정보를 훔쳐가는 공격을 수행한다.
- 네트워크 취약성에 대한 공격 : ARP 및 HTTPS 스푸핑을 수행하는데 있어서 환자 정보에 대한 액세스 하기위해 의료 센터의 유선 및 무선 네트워크에 접근한다.
- 랜섬웨어 : 의료 데이터를 암호화하고 암호 해독을 위해 금전을 갈취할 뿐만 아니라 전체 임상시스템에 대한 액세스를 차단하여 외과 수술 및 생명 유지를 위한 장비 작업을 마비시킨다.

6. 의료분야 정보보안 및 개인정보보호

ISO/IEC 27001:2013 인증은 정보보호 관련 14개의 관리 영역과 114개의 세부 항목에 대한 엄격한 심사를 거친 기업만이 인증을 획득할 수 있는 정보보호 분야의 최고 권위를 자랑하는 인증이다.

ISO 27799 역시 의료정보 보호에 관한 국제 표준으로 가장 민감한 정보라 할 수 있는 개인 의료 데이터의 기밀성, 가용성을 보장하기 위한 기준을 규정하고 있다.

6. 의료분야 정보보안 및 개인정보보호

- ISO 27799 : 2016 규제

- **액세스 제어**

- **관리자 액세스와 민감 데이터 분리 :** 의료 기관은 **관리자와 데이터 소유자의 역할과 의무 분리, 메타데이터를 그대로 두고 파일을 암호화**, 이 방식으로 하이퍼바이저, 클라우드, 스토리지 및 서버 관리자를 비롯한 IT 관리자는 자신이 관리하는 시스템에있는 주요데이터에 대한 관리자 액세스 권한 없이 시스템 관리 작업을 수행

- **강력한 직무분리 : 강력한 직무 분리 기능**으로 한 명의 관리자가 데이터 보안 활동, 암호키관리 모두를 제어할 수 해야하며 관리자 액세스를 위해 **2팩터 인증**을 사용합니다.

- **세분화된 관리자 액세스 제어 : 최소 액세스 권한 관리기능으로 관리자의 데이터 오용과 APT공격으로부터 데이터를 보호**합니다. 세분화된 관리자 액세스 관리 정책은 사용자, 프로세스, 파일 유형, 시간 및 기타 매개 변수를 사용하여 적용됩니다. 적용 옵션은 평문 데이터에 대한 액세스 권한뿐만 아니라 사용자가 사용할 수있는 파일 시스템 명령도 제어할 수 있습니다.

6. 의료분야 정보보안 및 개인정보보호

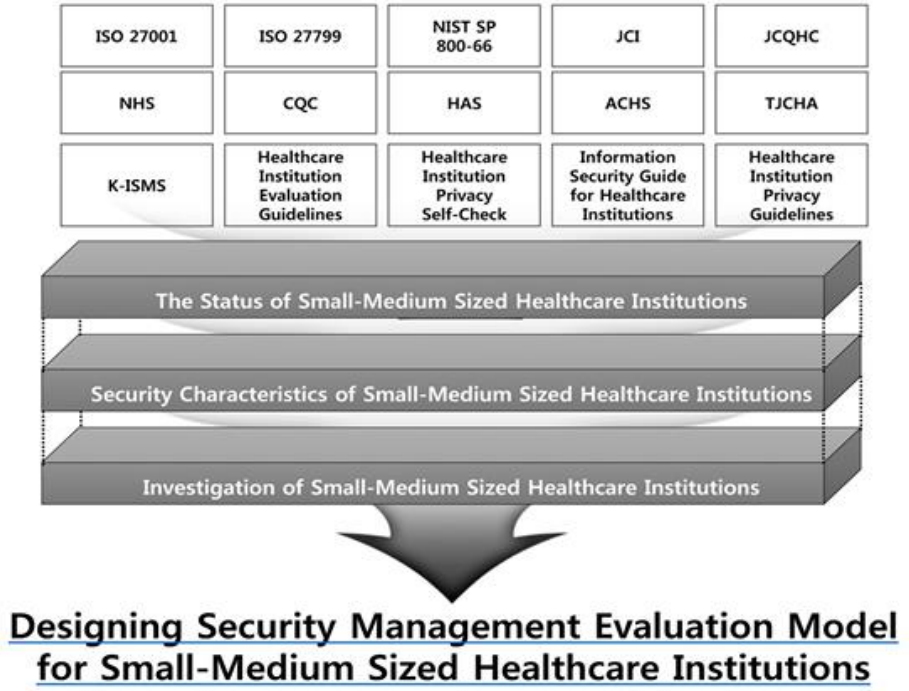
- **데이터 중심 보안**
  - 암호화를 통해 데이터가 탈취되어도 복호화 할 도구가 없을 경우 개인정보 데이터 유출 방지 가능

- **통합 키 관리**
  - 분산된 암호키를 통합 키 관리로 암호키 운영과 관리상의 문제가 간소화될 뿐 아니라 안전한 키 보안이 보장되며 승인된 암호화 서비스에만 키 제공

- **보안 인텔리전스 로그**
  - 비정상적인 데이터 액세스 활동을 모니터링하여 식별하고 사용자의 데이터 액세스에 대한 상세한 로그로 어떤 데이터에 액세스 했는지, 내부 정책에 따른 승인된 엑세스인지 모니터링 해야한다. 일례로 개인정보 관리자가 정상보다 많은 양의 데이터에 액세스하거나 파일의 무단 다운로드 하려하는 것을 모니터링하여 악의적인 내부자의 위협을 사전 감지한다.

6. 의료분야 정보보안 및 개인정보보호

해외 의료분야와 관련된 정보보안 및 개인정보보호와 관련된 관리체계로는 ISO27001(정보보호경영시스템), ISO 27799 (의료개인정보보호 경영시스템), NIST SP 800-66(「의료정보보호법(HIPAA)」 실행 가이드문서), JCI(국제의료기관평가위원회), JCQHC(일본의료기능 평가기구)를 들 수 있으며, **국내**에서는 ISMS-P, 개인정보보호자율점검표(대한병원협회), 의료기관을 위한 정보보호 안내서(병원편, 보건복지부), 개인정보보호가이드라인(의료기관편, 개인정보보호위원회) 기준을 참고하고 있다.



<그림2. 중소형 의료기관의 보안관리 평가 모델 설계>

7. 정보보안 및 개인정보보호 운영 방안

개인정보 파일명	수집항목	법률 근거
처방전	환자의 성명, 주민등록번호, 의료기관 명칭, 전화번호 및 팩스번호, 질병분류기호, 의료인의 성명·면허종류 및 번호, 처방 의약품의 명칭·분량·용법 및 용량, 처방전 발급 연월일 및 사용기간, 의약품 조제시 참고 사항, 「국민건강보험법 시행령」 별표 2에 따라 건강보험 가입자 또는 피부양자가 요양급여 비용의 일부를 부담하는 행위·약제 및 치료재료에 대하여 보건복지부장관이 정하여 고시하는 본인부담 구분기호, 「의료급여법 시행령」 별표 1 및 「의료급여법 시행규칙」 별표 1의2에 따라 수급자가 의료급여 비용의 전부 또는 일부를 부담하는 행위·약제 및 치료재료에 대하여 보건복지부장관이 정하여 고시하는 본인부담 구분기호	「의료법」 제18조, 같은 법 시행규칙 제12조
수술기록	① 환자의 성명, 수술명, 수술기록 등 ② 수술의사의 성명 등	「의료법」 제22조, 같은 법 시행규칙 제15조
검사소견서	성명, 주민등록번호, 의사면허번호, 소견인 성명, 질병 검사 소견 등	「의료법」 제22조, 같은 법 시행규칙 제15조
방사선사진 및 소견서	성명, 주민등록번호, 의사면허번호, 소견인 성명, 방사선 사진에 대한 검사 소견 등	「의료법」 제22조, 같은 법 시행규칙 제15조
진단서	① 환자의 성명, 주민등록번호, 주소, 병명 및 「통계법」 제22조제1항 전단에 따른 한국표준질병·사인 분류에 따른 질병분류기호, 발병 연월일 및 진단 연월일, 치료 내용 및 향후 치료에 대한 소견, 입원·퇴원 연월일, 의료기관의 명칭·주소, 진찰한 의사·치과의사 또는 한의사의 성명·면허자격·면허번호 ② 질병의 원인이 상해로 인한 것인 경우 – 상해의 원인 또는 추정되는 상해의 원인, 상해의 부위 및 정도, 입원의 필요 여부, 외과적 수술 여부, 합병증의 발생 가능 여부, 통상 활동의 가능 여부, 식사의 가능 여부, 상해에 대한 소견, 치료기간	「의료법」 제17조, 같은 법 시행규칙 제9조
사망진단서 (시체검안서)	① 사망자의 성명, 성별, 주민등록번호, 실제생년월일, 직업, 주소, 발병일시, 사망일시, 사망장소, 사망의 원인, 사망의 종류, 외인사항(사고종류, 사고발생일시, 사고발생장소) ② 의사·치과의사·한의사의 면허번호, 성명	「의료법」 제17조, 같은 법 시행규칙 제10조
출생증명서	① 출생아 부모의 성명, 생년월일, 직업, 산모의 주소, 출생장소, 출생일시, 임신기간, 다태(多胎), 출생아의 성별, 산모의 산아수, 출생아의 신체 상황(몸무게·신장), 출생아의 건강 상황 ② 의사·한의사·조산사의 면허번호 및 성명	「의료법」 제17조, 같은 법 시행규칙 제11조

개인정보 파일명	수집항목	법률 근거
진료 신청서	성명, 주민등록번호, 진료과목, 전화번호, 환자등록번호 (진료카드번호) 등	「의료법」 제22조
선택진료 신청서	성명, 주소, 전화번호, 주민등록번호, 진료 지원항목 등	「의료법」 제46조
진료기록부	주소, 성명, 연락처, 주민등록번호, 병력 및 가족력, 주된 증상, 진단 결과 또는 진단명, 진료 경과, 처치 등), 진료일시(日時)	「의료법」 제22조,
조산기록부	주소, 성명, 연락처, 주민등록번호, 임신 후의 경과와 그에 대한 소견, 건강진단의 유무(결핵·성병에 관한 및 분만 연월일시분, 분만의 경과 및 성별 및 생·사의 구별, 산아와 태아 산후의 의사의 건강진단 유무	
간호기록부	간호를 받는 사람의 성명, 체온·맥 사항, 투약에 관한 사항, 섭취 및 배설 간호에 관한 사항, 간호 일시	
환자명부	주소, 성명, 주민등록번호, 전화번호	

개인정보 파일명	수집항목	법률 근거
사산 또는 사태증명서	① 사산아 부모의 성명, 생년월일, 직업, 주소, 사산장소, 사산연월일, 임신기간, 다태, 사산의 종류, 자연사산의 원인, 인공임신중절을 위한 이유 ② 의료기관 주소, 명칭, 의사·한의사·조산사의 면허번호 및 성명	「의료법」 제17조, 같은 법 시행규칙 제11조
환자 진료기록의 열람 및 사본 교부	① 환자 본인 – 성명, 연락처, 주민등록번호(외국인등록번호), 주소 ② 신청인 – 성명, 연락처, 주민등록번호(외국인등록번호), 주소, 환자와의 관계 ③ 위임장 ㉠ 수임인의 성명, 연락처, 주민등록번호(외국인등록번호), 주소, 위임인과의 관계 ㉡ 위임인의 성명, 전화번호, 주민등록번호(외국인등록번호), 주소	「의료법」 제21조, 같은 법 시행규칙 제13조의3
요양급여의뢰서	① 건강보험증번호, 가입자·세대주·환자의 성명 및 주민등록번호, 주소, 전화번호, 상병명, 상병분류기호, 진료기간, 진료구분, 환자상태 및 진료소견 ② 요양기관의 기호·소재지, 대표자 성명, 담당 의사 성명	「국민건강보험법」 제41조, 국민건강보험 요양급여의 기준에 관한 규칙 제2조
자원봉사자 정보	① 이름, 주소, 연락처, 이메일, 학력사항, 자원봉사 활동내역 ② 주민등록번호(불가피한 경우, 보험 가입 시)	「자원봉사활동기본법」, 「자원봉사활동 기본법 시행령」 제16조
진료비 수납	신용카드번호, 진료비, 신용카드사 등	「전자금융거래법」

■ 환자 등 개인정보의 제3자 제공 금지

- 환자 등의 개인정보를 법률에 근거하는 등 정당한 사유 없이 제3자에게 제공할 수 없으며, 제공이 필요한 경우 당사자의 동의를 받아야 함
  - 특히, 진료기록은 「의료법」에서 정한 위임장 등 관련서류를 첨부한 경우에만 제공 가능
- 환자 등에게 의료기관이 제공하는 의료정보 및 의료기관의 행사 정보 등을 안내하기 위한 인쇄물, 이메일, 전화, 문자서비스 등을 제공할 목적으로 수집한 개인정보를 이용하는 경우, 환자 등이 그 사실을 명확하게 인지할 수 있도록 알리고 별도의 동의를 받은 후 시행하여야 함

Thank YOU