

의료기관의 개인정보 보호

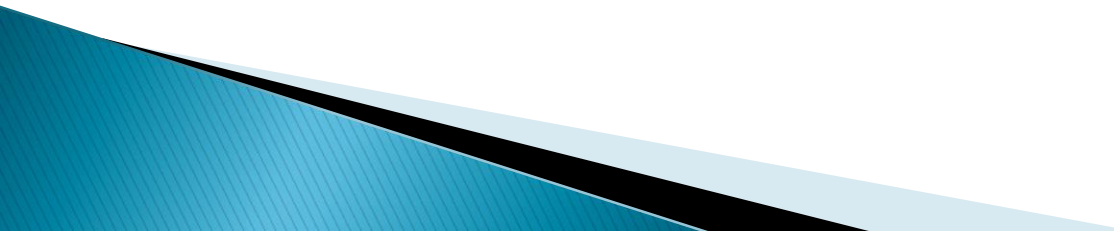
『의료기관 개인정보보호 가이드라인』 중심

2014. 4.1(수)

한국보건사회연구원

보건복지 개인정보통합관제센터

목 차

- I. 개인정보보호법 주요내용
 - II. 의료기관 개인정보 처리 기준
 - III. 개인정보 처리단계별 조치기준
- 

I . 개인정보보호법 주요내용

개인정보보호법 제정 및 시행

개인정보보호 3.0 시대의 개막

- ▶ 개인정보보호법은 약 350만개 모든 공공기관과 사업자를 규율 대상으로 확대하여, 법 적용 사각지대 해소
- ▶ 대통령 소속으로 '개인정보보호위원회'를 구성하여, 주요 정책사안 심의 및 의결
- ▶ '공공기관의 개인정보보호에 관한 법률' 폐지와 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'의 일부조항 흡수

법률 적용대상 및 적용범위 확대

법 시행 이전

- ▶ 공공기관, 정보통신사업자, 신용정보 제공·이용자 등 분야별 개별법이 있는 경우에 한하여 개인정보보호 의무 적용
 - 공공기관: 공공기관 개인정보보호법
 - 정보통신사업자(영리사업자, 온라인 사업자): 정보통신망법

법 시행 이후

- ▶ 적용 대상 확대: 공공기관과 민간기관에 대한 통합 적용
 - 국회·법원·헌법재판소·중앙선거관리위원회 등 공공기관 대상 확대
 - 의료기관, 협회·동창회 등 비영리단체 대상 확대
 - 온라인사업자에서 오프라인 사업자까지 대상 확대
- ▶ 적용범위 확대: 전자기록뿐 아니라 수기 기록 개인정보도 보호대상 확대

고유식별정보 처리 제한

법 시행 이전

- ▶ 주민등록번호 등 고유식별정보의 민간사용 사전적 제한 규정 없음
- ▶ 인터넷상에서 주민등록번호 외의 회원가입 방법 제공 의무화 (정보통신사업자 한정)

법 시행 이후

- ▶ 원칙적 처리금지
 - 정보주체의 별도 동의, 법령의 근거가 있는 경우 등 예외 허용
- ▶ 인터넷상 주민등록번호 외 회원가입 방법 제공 의무화 대상 확대 (정보통신사업자 → 공공기관, 일 1만명 이상 개인정보처리자)
- ▶ 주민등록번호 등 고유식별정보 처리시 암호화 등 안전조치 확보의무

영상정보처리기기 규제

법 시행 이전

- ▶ 공공기관 설치·운영 폐쇄회로텔레비전(CCTV)
 - 범죄예방 및 교통단속 등 공익을 위하여 필요한 경우
 - 녹음기능, 임의조작 금지

법 시행 이후

- ▶ 공공기관에서 민간기관까지 확대
 - 법령, 범죄예방·수사, 시설안전 및 화재예방, 교통단속 등
 - 녹음기능, 임의조작 금지
- ▶ 규율대상 확대
 - 기존 '폐쇄회로텔레비전(CCTV)'에서 네트워크카메라 포함

유출통지, 집단분쟁조정 및 단체소송

법 시행 이전

- ▶ 관련 제도 없음

법 시행 이후

- ▶ 개인정보 유출사실 통지 의무화
- ▶ 집단분쟁조정도입(재판상 화해 효력 부여)
 - 개인정보 피해가 대부분 ·소액 사건인 점 고려
- ▶ 단체소송(권리침해 중지) 도입
 - 재산피해 단체소송은 제외

개인정보보호위원회 및 분쟁조정위원회

법 시행 이전

- ▶ 공공기관개인정보보호심의위원회
 - 공공부문 정책 심의
 - 국무총리 소속
- ▶ 개인정보분쟁조정위원회
 - 민간분야 분쟁조정

법 시행 이후

- ▶ 개인정보보호위원회 설치
 - 공공 및 민간부문 정책 심의 · 의결
 - 대통령 소속
- ▶ 개인정보분쟁조정위원회 기능 확대
(기존) 15인 이내(민간 한정) →
(확대) 20인 이내(모든 공공·민간 포함)

주민번호 수집 법정주의(법 개정)

현행법 제24조 제1항

- ▶ 정보주체로부터 별도 동의를 받은 경우
- ▶ 법령에서 구체적으로 주민등록번호 처리를 요구·허용한 경우

개정법 제24조의2 제1항

- ▶ 법령에서 구체적으로 주민등록번호 처리를 요구·허용한 경우
- ▶ 정보주체 또는제3자의 급박한 생명, 신체, 재산·이익을 위해 명백히 필요하다고 인정되는 경우
- ▶ 기타 이에 준하는 경우로서 안전행정부령으로 정하는 경우
- ✱ 기 보유 주민번호 중 법령상 근거가 없는 경우 법 시행 후 2년 이내 파기

과징금 및 징계권고 제도(법 개정)

현행법

- ▶ 관련 제도 없음

개정법 제34조의 2, 제76조, 제65조

- ▶ 주민등록번호 분실 · 도난 · 유출 · 변조 또는 훼손된 경우 5억원 이하 과징금 부과 · 징수 단, 주민번호 안전성 확보조치 이행시 과징금 면제
- ▶ 과징금 부과한 행위에 대해 과태료 부과 금지(과태료 규정 적용 특례)
- ▶ 안전행정부장관의 징계 권고 대상에 개인정보처리자의 대표자(CEO) 및 책임있는 임원이 포함되는 징계권고 제도 도입

개인정보보호법과 의료법

의료법과의 적용 관계

- ▶ 개인정보보호법은 일반법이므로 다른 법률에 특별한 규정이 있는 경우를 제외하고는 개인정보보호법 적용
- ▶ 의료법에 따른 진료기록부, 조산기록부, 간호기록부, 환자명부, 수술기록부, 처방전 등을 위한 개인정보 수집·열람·제공은 의료법 규정이 우선적용
- ▶ 의료법에 규정되어 있지 않은 사항은 개인정보보호법에 따라 처리
 - 영상정보처리기기 설치운영 제한, 유출통지제, 집단분쟁조정제, 권리침해 중지 단체소송 등은 의료법 수범자에게도 모두 적용

II. 의료기관 개인정보 처리기준

기존 의료기관 개인정보보호 가이드라인

개요

- ▶ '12년 9월 보건복지부와 안전행정부가 공동으로 '의료기관 개인정보보호 가이드라인'을 개발·보급
- ▶ 개인정보 처리원칙 및 처리단계별 조치요령 중심으로 작성

기존 가이드라인 목차

- I. 가이드라인의 개요
- II. 개인정보 처리 기본원칙
- III. 개인정보 처리단계별 조치요령
 - 1. 개인정보의 수집·이용
 - 2. 개인정보의 관리
 - 3. 개인정보의 .제공·열람
 - 4. 정정·삭제 등 정보주체의 요구사항 처리
 - 5. 개인정보 파기
 - 6. 폐업 및 의료기관 허가사항 변경 시 조치사항
 - 7. 개인정보 유출·침해 시 조치방법
 - 8. 영상정보처리기기의 설치 및 운영

한계

- ▶ 실제 발생하는 사건 흐름 중심의 개인정보 보호방안 제시 필요
- ▶ 환자 이외의 정보주체에 대한 개인정보 처리기준 제시 필요
- ▶ 공공 및 민간 의료기관 유형 반영 필요
- ▶ 의료기관 관련 법령의 추가적인 검토 필요

신규 의료기관 가이드라인의 특징

1. 주요 업무 프로세스 중심 개인정보 처리 기준 마련

- ▶ ‘진료신청과정 → 진료과정 → 처방과정’ 단계의 환자 개인정보 처리기준

2. 의료기관 근로자 개인정보 처리 기준 제시

- ▶ 의료기관 근로자 ‘채용준비 → 채용결정 → 고용유지 → 고용종료’ 단계별 개인정보 처리 기준

3. 의료기관 유형별 개인정보 처리 기준의 마련

- ▶ 업무 통일성 제고를 위한 민간 및 공공 의료기관의 개인정보 처리기준

4. 개인영상정보 보호 등의 내용 구체화

- ▶ 영상정보 처리기기 설치·운영 및 그에 따른 개인영상정보의 보호

신규 의료기관 가이드라인의 구성

■ 용어의 정의

- I. 가이드라인의 개요
 - II. 환자의 개인정보 처리 기준
 - 1. 진료신청과정에서 환자의 개인정보 처리기준
 - 2. 진료과정에서 환자의 개인정보 처리기준
 - 3. 처방과정에서 환자의 개인정보 처리기준
 - III. 개인영상정보 처리기준
 - IV. 의료기관 근로자의 개인정보 처리 기준
 - 1. 채용준비 단계
 - 2. 채용결정 단계
 - 3. 고용유지 단계
 - 4. 고용종료 단계
 - V. 개인정보 처리단계별 조치기준
 - 1. 개인정보 개요
 - 2. 개인정보의 수집 · 이용
 -
 - 13. 피해 구제 방법
- <참고>
- 1. 표준서식
 - 2. 개인정보보호법
 - 3. 의료분야 관련 법령

환자의 개인정보 처리기준

1. 진료신청과정에서 환자의 개인정보 처리기준

- ▶ 진료 신청시 동의 없이 수집할 수 있는 개인정보
 - 인터넷, 전화 등에 의한 진료 예약시 : 성명, 생년월일, 주소, 연락처
 - 방문에 의한 진료 신청시 : 성명, 주민등록번호, 주소, 전화번호, 진료과목
- ▶ 정보주체의 동의 없이 수집 가능한 진료목적의 범위
 - 진료와 직접 관련된 진료신청, 진단, 검사, 치료, 수납 등 업무
 - 진료신청 문자발송, 검사결과 통보 등의 업무
 - 진료와 연결된 예방접종
 - 병원 이전 또는 휴업에 관한 정보
- ▶ 14세 미만의 경우 법정대리인의 동의를 받아 개인정보 수집

환자의 개인정보 처리기준

FAQ 인터넷 진료예약 시 주민등록번호를 요구하는 것이 개인정보보호법에 저촉되나요?

- 인터넷 진료예약 시 환자의 주민등록번호 수집 불가
- 인터넷 진료예약에서는 성명, 전화번호, 생년월일 등 최소한의 정보를 수집하고, 진료를 받기 위해 환자가 내원하는 경우 주민등록번호 포함 진료기록부 작성

FAQ 예방접종 안내를 위해 환자에게 SMS를 동의 없이 보낼 수 있나요?

- 진료목적 범위에 있는 예약내용의 안내, 간염 1차 접종을 받은 사람에게 2차 접종을 안내하는 등 동일 진료와 연결된 예방접종 사항은 동의 없이 SMS 보내는 것 가능
- 당해 진료와 관계없는 예방접종 안내 등을 위해서는 정보주체 또는 법정대리인의 동의를 받은 후에 SMS 보내는 방식 필요

환자의 개인정보 처리기준

2. 진료과정에서 환자의 개인정보 처리기준

▶ 진료과정에서 환자 동의 없이 수집하는 개인정보

- 진료기록부: 성명, 주소, 연락처, 주민등록번호 등 인적 사항, 주된 증상(병력, 가족력 추가 기록 가능), 진단결과, 치료 내용, 진료 일시
- 처방전: 환자의 성명 및 주민등록번호, 처방의약품의 명칭·분량·용법 및 용량 등

▶ 법률에 따른 의료인의 개인정보 제공 의무

- 진료환자의 진료기록의 송부(환자나 환자 보호자의 동의를 받은 경우, 의료법 제21조)
- 감염병 환자 등 신고(감염병 예방 및 관리에 관한 법률 제11조)
- 응급환자의 이송(응급의료에 관한 법률 제11조)
- 감염인 진단 검안사실의 신고(후천성면역결핍증예방법 제5조)
- 특정수혈부작용 신고(혈액관리법 제10조)
- 뇌사추정자 신고(장기 등 이식에 관한 법률 제17조)

환자의 개인정보 처리기준

FAQ 의학 · 치과의학 · 한방의학 또는 간호학을 전공하는 학생이 진료 과정을 참관하고자 하는 경우, 환자에게 동의를 받아야 하나요?

- 의료행위 보조자로서의 의학 등 전공학생은 지도교수 또는 의료인의 지도·감독을 받아 법령이 인정하는 의료행위는 환자의 동의를 받지 않고도 참관 및 의료행위 가능
- 법령에서 인정하는 의료행위(의료법제27조제1항제3호)
 - ① 전공 분야와 관련되는 실습을 하기 위하여 지도교수의 지도·감독을 받아 행하는 의료행위
 - ② 국민에 대한 의료봉사활동으로서 의료인의 지도·감독을 받아 행하는 의료행위
 - ③ 전시·사변이나 그 밖에 이에 준하는 국가비상사태 시에 국가나 지방자치단체의 요청에 따라 의료인의 지도·감독을 받아 행하는 의료행위

환자의 개인정보 처리기준

2. 진료과정에서 환자의 개인정보 처리기준

- ▶ 법률의 규정에 따라 환자정보 제공 가능
 - 국민건강보험공단, 건강보험심사평가원, 법원, 국민연금공단, 보험회사 등
- ▶ 의료법에 따른 보존기간이 경과하지 않은 개인정보는 삭제 요구 불가

3. 처방과정에서 환자의 개인정보 처리기준

- ▶ 처방과정에서 처방전의 작성·교부·발급
 - 환자정보 보호를 위한 안전성 확보조치 필요
- ▶ 진료비 수납을 위한 최소한의 정보(카드번호, 카드승인번호 등)는 수집 가능

환자의 개인정보 처리기준

FAQ 병원에서 진료를 받기 위해서 반드시 환자가 개인정보 활용 동의서에 서명해야 하나요?

- 의료법에서 진료기록부 작성, 처방전 작성 및 교부, 의료행위 등을 규정하고 있으므로, 진료목적에 필요한 성명, 주민등록번호, 주소 등의 개인정보는 환자의 동의 없이 수집 및 이용 가능

FAQ 전화로 병원에 입원하고 있는지 여부를 문의 받을 경우 알려줘도 되나요?

- 환자 입원정보는 개인정보로 환자의 동의 없이는 알려주지 않아야 함
- 환자 본인이나 보호자와 직접 연락할 수 있도록 안내하는 것이 바람직함
- 의료법 제19조에 따라 의료인은 이 법이나 다른 법령에 특별히 규정된 경우 외에는 의료·조산 또는 간호를 하면서 알게 된 다른 사람의 비밀을 누설하지 못하므로, 환자의 개인정보인 입원 여부를 환자의 동의 없이 알려 주는 경우 의료법에 저촉 가능

의료인력 개인정보 처리기준

1. 채용 준비단계

- ▶ 인재선발을 위해 필요한 개인정보는 정보주체 동의 없이 수집·이용 가능
 - 의료기관은 지원자의 요구가 있는 경우, 개인정보의 수집 출처, 개인정보 처리 목적, 개인정보 처리 정지 요구권 고지
- ▶ 주민등록번호의 수집은 법령에서 구체적으로 허용한 경우에만 수집 가능
- ▶ 지원자 개인정보의 안전한 관리
 - 채용전형단계별 개인정보취급자 최소한 지정
 - 채용대행업체에 위탁할 경우 위탁계약을 문서로 하고, 안전한 관리 및 감독

의료인력 개인정보 처리기준

2. 채용 결정단계

- ▶ 근로계약서, 임금대장 등을 위한 개인정보 수집은 정보주체 동의 없이 가능
 - 주민등록번호 수집도 동의 없이 수집 가능(근로기준법 시행령 제27조)
 - 민감정보 수집은 별도 동의 필요
 - 업무상 반드시 필요한 개인정보 제3자 제공 및 공개는 정보주체 동의 확보
- ▶ 법령상 의무준수를 위한 주민등록번호 수집·이용은 동의 없이 처리 가능
 - 소득세법에 따른 연말정산 등
- ▶ 가족의 동의 없이 개인정보를 수집·이용 가능
 - 근로자 가족 복리후생을 위한 업무 처리

의료인력 개인정보 처리기준

3. 고용유지단계

- ▶ 근로계약 이행에 필요한 개인정보는 근로자의 동의 없이 활용 가능
 - 인력배치 및 전보, 파견, 휴직 등
 - 징계처분, 해고 등 불이익 처분을 공개하고자 하는 경우, 근로자의 동의 필요
- ▶ 근로자 객관적인 성과·실적 등 인사평가정보는 정보주체에게 공개
- ▶ 급여 등을 노동조합, 공공기관 등 제3자 제공시 정보주체 동의 필요
- ▶ 외부기관에 교육을 위탁하기 위해 개인정보를 제공하는 경우, 문서로 시행

의료인력 개인정보 처리기준

4. 고용종료단계

- ▶ 퇴직 의료인력의 개인정보 지체없이 파기
 - 의료인력의 경력 증명 등에 관한 정보는 퇴직 후 최소 3년간 별도 보관 (근로기준법 제39조 및 같은 법 시행령 제19조)
 - 퇴직 근로자의 경력증명 정보를 3년 이상 보관하고자 하는 경우, 퇴직 시점에 퇴직 근로자의 동의를 받아 보관
- ▶ 퇴직 근로자의 개인정보 제3자 제공 시, 정보주체 동의 필요
 - 순수 친목단체 퇴직 근로자 모임은 동의 없이 개인정보 수집가능
 - 단, 의료기관이 제공하고자 할 경우에는 퇴직 근로자 동의 필요

의료인력 개인정보 처리기준

FAQ 의료기관이 입사지원자의 개인정보를 수집하고자 할 때 개인정보의 수집 동의를 별도로 받아야 하나요?

- 입사지원은 근로계약 체결의 일부로 입사지원자의 동의 없이 채용에 필요한 최소한의 정보 수집 가능
- 단, 주민등록번호는 입사 후 수집 가능

FAQ 임직원 복리후생을 위해 가족의 개인정보를 수집하는 경우 가족구성원의 동의를 받아야 하는지요?

- 의료기관은 임직원 및 임직원의 가족에 대한 복리후생 제공을 위하여 가족의 개인정보 수집 및 이용이 가능하며, 가족구성원의 동의를 필요로 하지 않음
- 단, 주민등록번호 등 고유식별번호와 건강정보 등 민감정보는 동의 필요

의료인력 개인정보 처리기준

FAQ 개인정보보호법 시행 전부터 보관하고 있던 퇴직 근로자 개인정보의 보관을 위하여 별도의 동의를 받아야 하나요? 아니면 파기하여야 하나요?

- 경력증명 등을 위한 목적으로 보관·이용하고 있던 퇴직근로자 개인정보는 법령에서 규정한 퇴직 후 3년간 별도로 보관
- 법령에서 정한 기간 이후에는 퇴직근로자의 동의를 받은 경우 보관

FAQ 퇴직한 근로자의 개인정보는 언제 파기하여야 하나요?

- 보존기간이 종료된 후 5일 이내에 파기
- 근로기준법 제39조에 따르면 의료기관의 장은 근로자가 퇴직한 후라도 사용기간, 업무 종류, 지위와 임금, 그 밖에 필요한 사항에 관한 증명서 발급
- 사용증명서를 청구할 수 있는 기한은 퇴직 후 3년 이내(근로기준법 시행령 제19조)

III. 개인정보 처리 단계별 조치기준

1. 개인정보의 수집 · 이용 [1]

동의 없이 수집 · 이용이 가능한 경우

- ▶ 진료목적 개인정보는 환자의 동의 없이 수집·이용가능
 - 진료신청서: 성명, 주민등록번호, 진료과목, 전화번호, 환자등록번호 등
 - 선택진료신청서
 - 진료기록부
 - 조산기록부
 - 간호기록부
 - 환자명부
 - 처방전
 - 검사소견서
 - 진단서
 - 영양급여의뢰서 등

1. 개인정보의 수집 · 이용 [2]

법률에 따른 의료인의 개인정보 제공 의무

- ▶ 감염병 환자, 감염병 의사환자 또는 병원체 보유자 신고 의무
 - 성명, 주민등록번호, 전화번호, 직업, 성별, 주소, 감염병명, 발병일 등
- ▶ 응급환자 이송 의무
 - 환자 성명, 주민등록번호, 주소, 응급처치 후 환자상태, 응급처치사항 등
- ▶ 감염인 진단 검안사실 신고의무
 - 사망자 성명, 주민등록번호, 주소, 검사소견, 추정감염경로 등
- ▶ 특정수혈부작용 신고 의무
 - 수혈자의 성명, 내원 당시 질환명, 수혈 의료기관명, 수혈 전 검사결과 등
- ▶ 뇌사추정자 신고 의무
 - 뇌사추정자의 성명, 생년월일 및 주소, 뇌사추정자의 상태 및 발생원인

1. 개인정보의 수집 · 이용 (3)

동의를 받아야 수집 · 이용이 가능한 경우

- ▶ 고객관리를 위한 개인정보는 별도의 동의 필요
 - 수집목적: DM, SMS 등을 통한 홍보 및 마케팅
 - 수집항목: 환자 인적사항 등
 - 수집방법: 고객정보 수집 · 이용에 동의한 환자의 정보만 수집
- ▶ 홈페이지 회원 개인정보 수집시, 정보주체의 동의 필요
 - 수집목적: 홈페이지 회원관리
 - 수집항목: 필수정보(성명, ID, 비밀번호), 선택정보(생년월일, 전화번호, 이메일, 관심정보 등)

※ 주의: 홈페이지 회원정보로 주민등록번호는 수집하지 않도록 해야 함

개인정보의 수집 · 이용 처리기준

FAQ 개인정보 수집·이용·제공 동의시 자필 서명이 아닌 전자 서명으로 하여도 효력이 동일한가요?

- 전자서명법 제3조제3항에 따르면 “전자서명은 당사자간의 약정에 따른 서명, 서명날인 또는 기명날인으로서의 효력을 가진다.”고 규정
- 환자 본인의 전자서명은 자필서명과 같은 효력

FAQ 동의를 받아야 하는 경우 반드시 서면으로 받아야 하나요?

- 반드시 서면으로 받을 필요는 없으며, 「개인정보보호법」에 따른 다음의 방법
 - 직접 또는 우편, 팩스 등 방법으로 전달하고, 정보주체가 서명한 동의서 받는 방법
 - 전화를 통하여 동의 내용을 정보주체에게 알리고 동의의 의사표시를 확인하는 방법
 - 전화를 통하여 동의 내용을 정보주체에게 알리고, 인터넷주소 등을 통하여 동의 사항을 확인하도록 한 후 다시 전화를 통하여 그 동의의 의사표시를 확인하는 방법
 - 인터넷 홈페이지 등에 동의 내용을 게재하고 정보주체가 동의 여부를 표시
 - 동의 내용을 전자우편으로 발송하고, 정보주체로부터 동의 전자우편을 받는 방법

2. 개인정보의 위탁관리 (1)

개인정보 처리 위탁시 문서화

▶ 문서화에 포함되어야 할 내용

- 위탁업무 목적 외 개인정보 처리금지에 관한 사항
- 개인정보의 기술적·관리적 보호조치에 관한 사항
- 위탁업무의 목적 및 범위
- 재 위탁 제한에 관한 사항
- 개인정보에 대한 접근 제한 등 안전성 확보조치에 관한 사항
- 위탁업무관련 개인정보의 관리현황 점검 등 감독에 관한 사항
- 수탁자가 준수하여야 할 의무 위반 시 손해배상 등 책임에 관한 사항

2. 개인정보의 위탁관리 [2]

개인정보 처리 위탁시 공개 및 관리감독 등

▶ 위탁 사실 공개

- 인터넷 홈페이지
- 사업장 등 보기 쉬운 장소에 게시

▶ 위탁에 대한 관리 감독

- 개인정보 분실, 도난, 유출, 변조, 훼손 되지 않도록 수탁자 감독

▶ 손해배상 책임

- 수탁자가 개인정보보호 법을 위반하여 손해배상 책임이 있는 경우 개인정보처리자(위탁자)의 소속직원으로 간주

3. 영업의 양도

개인정보 이전을 위한 통지

- ▶ 개인정보 이전하기 전에 정보주체에게 통지
 - 개인정보를 이전하려는 사실
 - 개인정보를 이전받는 자의 성명, 주소, 전화번호 및 그 밖의 연락처
 - 정보주체가 개인정보의 이전을 원하지 아니하는 경우 조치할 수 있는 방법 및 절차
- ▶ 영업 양도 등에 따른 통지방법
 - 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법
 - 통지사항을 정보주체에게 알릴 수 없는 경우에는 해당 사항을 인터넷 홈페이지에 30일 이상 게재

개인정보의 제공 처리기준

FAQ 환자분의 편의를 위하여 검사결과를 전화 또는 문자로 알려주고 있는데 개인정보보호법상 문제가 되나요?

- 환자 본인이 확인된 경우, 환자의 검사결과 통보는 진료목적의 범위에 해당하므로 별도의 동의없이 환자에게 전화 또는 문자 통지 가능
- 다만, 다른 사람에게 환자 기록을 알려주는 것은 의료법에 해당하는 경우로 제한

FAQ 다른 의료기관 또는 검사기관에 검사를 의뢰하여 검사를 하는 경우 정보주체의 동의를 받아야 하나요?

- 진료 목적으로 다른 의료기관 또는 검사기관에 검사를 위탁하는 등 개인정보 처리를 위탁하는 경우 정보주체인 환자의 동의를 받을 필요는 없으나,
- 위탁하는 경우 계약서를 문서화하고, 위탁하는 업무의 내용과 수탁자를 공개하고, 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 수탁자 교육 및 감독

4. 영상정보처리기기의 설치 및 운영[1]

▶ 공개된 장소의 영상정보처리기기 설치

- 법령에서 구체적으로 허용한 경우
- 범죄의 예방 및 수사를 위하여 필요한 경우
- 시설안전 및 화재 예방을 위하여 필요한 경우
- 교통단속, 교통정보의 수집·분석 및 제공을 위하여 필요한 경우

※ 공개된 장소: 정보주체가 접근하거나 통행시 제한을 받지 아니한 장소
(병원내 대기실, 접수대, 휴게실, 주차장 등)

※ 비공개 장소: 설치하는 가능하나, 정보주체(환자)로부터 동의를 받아야 함
(진료실, 입원실, 수술실 등 치료목적 공간)

▶ 영상정보처리기기 임의조작 및 녹음 금지

4. 영상정보처리기기의 설치 및 운영[2]

▶ 안내판 설치를 통한 설치 · 운영 사실 공개

- 설치 목적 및 장소
- 촬영 범위 및 시간
- 관리책임자의 성명(직책) 및 연락처
- (영상정보처리기기설치 · 운영을 위탁한 경우) 위탁받는 자의 명칭 및 연락처

▶ 영상정보처리기기 운영 및 영상정보의 관리

- 녹음은 정보주체의 동의를 받은 경우 가능(통신비밀보호법 제3조)
- 촬영자료는 개인정보처리방침, 안전성확보조치 등 개인정보보호법상의 모든 규정 적용

※ 영상정보처리기기 운영·관리 방침을 별도로 수립하여 홈페이지에 게시하거나 개인정보 처리방침에 포함해 공개

본 건물 내부는

_____ 목적으로

영상정보처리기기를 운영하고 있습니다.

• 설치장소 및 대수 : _____

• 촬영 범위 : _____

• 촬영 시간 : _____

• 관리책임자 : _____

(전화 _____)



영상정보처리기기 개인정보 처리기준

FAQ 의료기관의 입원실이나 진료실에서 폭행 사고를 대비하여 CCTV를 설치하는 것이 가능한지요?

- 의료기관의 입원실과 진료실은 의료인과 환자만이 출입할 수 있으므로 불특정 다수가 출입할 수 있는 공개된 장소가 아님
- CCTV 등 영상정보처리기기를 설치하여 촬영하기 위해서는 진료실에 출입하는 모든 사람의 동의를 받아야만 녹화 가능

FAQ 의료기관에서 CCTV를 설치하는 장소는 어느 곳인지요?

- 병원, 응급실 내의 접수창구, 대기실, 복도 등은 환자 및 보호자가 비교적 제약없이 출입할 수 있는 장소이므로 개인정보보호법에 따른 '공개된 장소'에 해당함
- 공개된 장소는 범죄예방 및 수사, 시설안전 및 화재예방 등 목적으로 CCTV 설치 가능

5. 개인정보의 안전성 확보[1]

▶ 내부관리 계획 수립 및 시행

- 개인정보 보호책임자의 지정에 관한 사항
- 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항
- 개인정보의 안전성 확보에 관한 사항
- 개인정보취급자에 대한 교육에 관한 사항
- 그 밖에 개인정보 보호를 위하여 필요한 사항

※ 예외) 상시 근로자의 수가 5명 미만인 소규모 의료기관의 경우에는
내부관리 계획을 수립하지 아니할 수 있음

▶ 접근 권한 관리

- 업무별 사용자 그룹별 접근권한 설정
- 접근권한 부여, 변경, 말소 내역 기록

〈참고〉 개인정보보호 내부관리계획 가이드

제1장 총칙

제1조(목적)

제2조(적용범위)

제3조(용어 정의)

제2장 내부관리계획의 수립 및 시행

제4조(내부관리계획의 수립 및 승인)

제5조(내부관리계획의 공표)

제3장 개인정보보호책임자의 의무와 책임

제6조(개인정보보호책임자의 지정)

제7조(개인정보보호책임자의 의무와 책임)

제8조(개인정보취급자의 범위 및 의무와 책임)

제4장 개인정보의 처리단계별 기술적·관리적 안전조치

제9조(개인정보취급자 접근 권한 관리 및 인증)

제10조(접근통제)

제11조(개인정보의 암호화)

제12조(접근기록의 위·변조 방지)

제13조(보안프로그램의 설치 및 운영)

제14조(물리적 접근제한)

제5장 개인정보보호 교육

제6장 개인정보 침해대응 및 피해구제

5. 개인정보의 안전성 확보[2]

▶ 비밀번호 관리

- 안전한 비밀번호 작성규칙 수립 및 적용
- 비밀번호 분실시, SMS 등 본인확인 절차를 거쳐 비밀번호 재설정

▶ 접근통제 시스템의 설치 · 운영 및 암호화

- 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위하여 침입차단 시스템(Firewall) 또는 침입방지시스템(IPS) 등 설치 및 운영
- 외부에서 개인정보처리시스템에 접속하려는 경우, 가상사설망(VPN) 또는 전용선 등 안전한 접속수단 적용
- 개인정보 암호화 계획 수립 및 적용

5. 개인정보의 안전성 확보(3)

- ▶ 접속기록의 보관 및 위·변조
 - 접속기록 최소 6개월 보관·관리
 - 위·변조 및 도난, 분실되지 않도록 안전하게 보관
- ▶ 보안프로그램 설치 및 운영
 - 백신 소프트웨어 등의 보안 프로그램을 설치·운영
 - 자동 업데이트 기능을 사용하거나 일 1회 이상 업데이트 실시
- ▶ 물리적 보안
 - 원무실, 전산실, 의무기록실 등 출입통제 계획 마련 및 시행
 - 잠금 장치가 있는 안전한 장소 보관
 - 물리적 접근통제장치를 설치·운영하고, 출입내역 기록
 - 보안 사고 예방 및 사고 발생 시 증거를 확보할 수 있도록 개인정보 보관시설에는 CCTV 설치 권고

개인정보 안전성 확보 처리기준

FAQ 홈페이지 비밀번호를 전화로 문의 시 본인 확인은 어느 수준까지 하나요?

- 홈페이지의 비밀번호는 '개인정보 안전성 확보조치 기준'에 따라 암호화
- 암호화된 비밀번호는 알려줄 수 없는 개인정보
- 본인확인을 거쳐 임시로 비밀번호 부여
- '비밀번호 작성규칙'에 따라 본인이 직접 비밀번호를 새로이 작성한 후 이용
- 의료기관은 비밀번호가 복호화 되지 않도록 일방향 암호화

FAQ 의료기관에서 보호자와의 분쟁에 대비하기 위하여 음성녹음을 저장할 경우 암호화의 대상이 되나요? 그리고 녹음에 대한 동의를 따로 받아야 하나요?

- 음성녹음을 저장할 경우, 암호화 필요
- 진료를 목적으로 환자 및 그 보호자를 대상으로 녹음하는 것은 동의 없이 가능
- 암호화 대상 중에서 CT영상 등 의료행위 관련 바이오정보는 암호화 대상에서 제외

개인정보 안전성 확보 처리기준

FAQ 직원들의 출입 시 사용하는 지문도 생체정보에 해당하는데 이를 암호화하여 저장해야 하나요?

- 개인정보보호법에 따라 바이오정보는 암호화 대상이 되는 정보
- 정보통신망을 통하여 송·수신하거나 보조저장매체를 통하여 전달하는 경우 암호화
- 암호화를 하는 경우에는 안전한 암호알고리즘으로 암호화하여 저장

FAQ 개인정보의 안전성을 확보하기 위하여 의료기록 서류를 별도의 보관시설이나 잠금장치의 설치 등과 같은 물리적 조치를 하여야 하나요?

- 개인정보의 안전한 보관을 위하여 보관시설을 마련하거나 잠금장치 설치
- 업무시간 중에 수시로 사용하는 진료기록은 잠금장치를 해제한 채 사용 가능
- 업무시간이 종료된 이후에는 잠금장치를 통해 물리적 보호조치

6. 개인정보의 파기 (1)

▶ 개인정보의 파기 사유

- 개인정보의 보유기간이 경과된 경우
- 개인정보의 처리목적 달성
- 해당 의료 서비스의 폐지
- 의료기관의 폐업

▶ 진료기록의 보존기간

1. 환자명부: 5년	2. 진료기록부: 10년
3. 처방전: 2년	4. 수술기록: 10년
5. 검사소견기록: 5년	6. 방사선 사진 및 그 소견서: 5년
7. 간호기록부: 5년	8. 조산기록부: 5년
9. 진단서 등의 부분(진단서, 사망진단서, 시체 검안서 등을 따로 구분하여 보존할 것): 3년	

6. 개인정보의 파기 (2)

- ▶ 진료목적상 필요한 경우, 법정 보존기간이 경과한 진료정보의 처리
 - 공공의료기관은 기록물관리 전문요원의 심사와 기록물평가심의회 심의를 거쳐 평가심의서를 작성하고, 기록물의 보존기한 연장여부 혹은 파기여부 결정
 - 민간의료기관의 경우 의무기록심의회와 같은 내부 심의를 거쳐 진료정보의 보존기간 연장여부 혹은 파기여부 결정
 - 매년 1회 이상 보존기간 연장여부 혹은 파기여부 결정 가능
 - 진료기록 종류별로 보존기간 연장여부 혹은 파기여부 결정 가능

개인정보 파기 처리기준

FAQ 의료기관에서 연속적인 진료의 연계 및 과거병력의 중요성 등을 감안해 보존기간을 연장하고자 하는 경우, 어떤 절차를 통해 연장하여 보존할 수 있나요?

- 보존기간이 경과하거나 목적 달성 진료기록을 매년 1회 이상 보존기간 연장여부 혹은 파기여부를 결정할 수 있음
 - 공공의료기관은 기록물관리 전문요원의 심사와 기록물평가심의회 심의를 거쳐 기록물의 보존기한 연장여부 혹은 파기여부 결정
 - 민간의료기관의 경우도 공공의료기관에 준하는 절차로 연장 혹은 파기여부 결정
 - 진료에 관한 기록 종류별로 보존기간 연장여부 혹은 파기여부를 결정
 - 연장사유를 근거로 최소 필요 기간 동안 연장
 - 연장 보존에 관한 사항을 의료기관 홈페이지나 의료기관 내부에 게시 권고
- 환자의 진료정보에 대해 별도로 정보주체의 동의를 받은 경우에도 보존기간 연장

7. 개인정보 처리방침

- ▶ 개인정보 처리방침 수립 및 홈페이지 등을 통해 공개
 - 개인정보의 처리 목적
 - 개인정보의 처리 및 보유 기간
 - 개인정보의 제3자 제공에 관한 사항(해당되는 경우)
 - 개인정보처리의 위탁에 관한 사항(해당되는 경우)
 - 정보주체의 권리·의무 및 그 행사방법에 관한 사항
 - 처리하는 개인정보의 항목
 - 개인정보의 파기에 관한 사항
 - 개인정보 보호책임자에 관한 사항
 - 개인정보 처리방침의 변경에 관한 사항
 - 개인정보의 안전성 확보조치에 관한 사항

개인정보처리방침

_____는 귀하의 개인정보를 매우 중요시하며, 『개인정보보호법』을 준수하고 있습니다. 본 개인정보처리방침은 귀하께서 제공하시는 개인정보가 어떠한 용도와 방식으로 이용되고 있으며 개인정보 보호를 위해 어떠한 조치가 취해지고 있는지 알려드립니다.

1. 수집하는 개인정보의 항목 및 수집방법

개인정보파일명 : _____
수집항목 : _____
수집방법 : _____

2. 개인정보의 수집 및 이용목적

수집하는 개인정보는 _____에만 사용하며 이용 목적이 변경될 시에는 사전 동의를 구할 것입니다.

3. 개인정보의 보유 및 이용기간 및 파기절차 및 파기방법

다음에 정한 보유기간 동안 개인정보를 보유하며 그 이후는 지체 없이 파기합니다.

보유기간 : _____

파기절차 : 법정 보유기간 후 파기방법에 의하여 즉시 파기

파기방법 : 전자적 파일은 재생할 수 없는 기술적 방법을 사용하여 삭제하고 종이자료는 분쇄기로 분쇄하거나 소각

4. 이용자 및 법정대리인의 권리와 그 행사방법

이용자 및 법정대리인은 개인정보와 관련하여 전화, 서면 등을 이용하여 개인정보 열람·정정·삭제·처리정지 등의 권리를 행사할 수 있습니다.

5. 개인정보의 제3자 제공

수집된 개인정보는 법령의 근거가 있는 경우 외에는 제3자에게 제공하지 않습니다.

6. 개인정보 처리의 위탁

개인정보 처리를 위해 다음의 회사에 위탁하고 있습니다.

회사명 : _____ (연락처 : _____)

위탁업무 내용 : _____

7. 개인정보 보호책임자

이 름	소 속	전화번호	메 일

8. 개인정보의 안전성 확보조치

이용자께서 제공하신 모든 정보는 방화벽 등 보안장비에 의해 안전하게 보호되고 있습니다. 또한 개인정보를 처리하는 인원을 최소한으로 제한하고 정기적인 교육과 비밀번호를 갱신을 통해 개인정보가 유출되지 않도록 안전하게 관리하고 있습니다.

9. 정책 변경에 따른 공지 의무

이 개인정보처리방침은 _____년 _____월 _____일에 제정되었으며 법령·정책 또는 보안기술의 변경에 따라 내용의 추가·삭제 및 수정이 있을 시에는 변경되는 개인정보처리방침을 시행하기 최소 7일전 홈페이지 또는 접수 창구에 변경이유 및 내용 등을 공지하도록 하겠습니다.

공고일자 : _____년 _____월 _____일 / 시행일자 : _____년 _____월 _____일

8. 개인정보 보호책임자

- ▶ 개인정보 보호책임자로 의료기관의 대표자 또는 개인정보 처리 관련 업무 부서의 장 또는 개인정보 보호에 관한 소양이 있는 사람 지정
 - 개인정보 보호 계획의 수립 및 시행
 - 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
 - 개인정보 처리와 관련한 불만의 처리 및 피해 구제
 - 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
 - 개인정보 보호 교육 계획의 수립 및 시행
 - 개인정보파일의 보호 및 관리·감독
 - 개인정보 처리방침 수립·변경 및 시행
 - 개인정보 보호 관련 자료의 관리
 - 처리목적이 달성되거나 보유기간이 경과한 개인정보 파기
 - 개인정보침해 관련 민원의 접수·처리
 - 그 밖에 개인정보 보호를 위하여 필요한 업무

9. 정보주체의 권익보호[1]

- ▶ **환자 등 정보주체 이외로부터 수집한 개인정보에 대한 정보주체의 요구**
 - 3일 이내에 고지
 - 개인정보의 수집 출처 및 개인정보의 처리 목적
 - 개인정보의 처리정지를 요구할 권리가 있다는 사실
- ▶ **정보주체의 열람 요구 10일 이내에 조치**
 - 10일 이내에 조치
 - 진료정보의 열람은 의료법에서 허용하는 경우에만 허용
 - 10일 이내 열람할 수 없는 정당한 사유가 있는 경우, 열람 연기
 - 열람 제한·거절사유에 해당하는 경우, 정보주체에게 그 사유를 알리고 열람을 제한하거나 거절

9. 정보주체의 권익보호(2)

▶ 개인정보 제3자 제공·열람 가능 사례: 환자·친족·대리인 신청

환자정보 제공·열람 신청인	요건	근거
환자 본인	①본인 신분증	의료법 시행규칙 제13조의2제4항
환자의 임의대리인 (환자가 지정한 친구, 동료, 지인 등)	①신청인 신분증 사본 ②환자 자필서명 동의서 ③환자 자필서명 위임장(만14세미만인 경우 법정대리인이 작성하고, 가족관계증명서 등 서류 첨부) ④환자 신분증 사본	의료법 제21조제2항제2호 의료법 시행규칙 제13조의2제2항
환자의 친족	①신청인 신분증 사본 ②신청인이 환자의 친족임을 확인할 수 있는 서류 ③환자 자필서명 동의서(만14세미만인 경우 제외) ④환자 신분증 사본	의료법 제21조제2항제1호 의료법 시행규칙 제13조의2제1항
.	.	
.	.	
.	.	

9. 정보주체의 권익보호(3)

▶ 개인정보 열람 또는 사본의 교부 등 허용 사유

제공·열람 신청자	사 유
국민건강보험공단, 건강보험심사평가원	급여비용심사·지급·대상여부 확인·사후관리 등을 위한 업무
시군구, 국민건강보험공단, 건강보험심사평가원	의료급여 수급권자 확인, 급여비용의 심사·지급·사후관리 등 의료급여 업무
법원·수사기관 (형사소송)	관련법령에 따라 압수, 수색, 검증하는 경우
법원 (민사소송)	관련법령에 따라 법원이 제출을 명령한 경우
근로복지공단	근로자를 진료한 산재보험 의료기관(의사 포함)에 대하여 그 근로자의 진료에 관한 보고 또는 서류 등 제출을 요구하거나 조사하는 경우
보험회사	자동차보험진료수가를 청구받은 보험회사 등이 그 의료기관에 대하여 관계 진료기록의 열람을 청구한 경우
지방병무청	지방병무청장이 징병검사 관련 질병 또는 심신장애 확인을 위하여 의료기관의 장에게 징병검사대상자의 진료기록·치료 관련 기록의 제출을 요구한 경우
학교안전공제회	공제회가 공제급여의 지급 여부 결정을 위하여 「국민건강보험법」 제42조에 따른 요양기관에 대하여 진료기록의 열람 또는 자료의 제출을 요청하는 경우
보훈병원	의료기관의 장이 진료기록 및 임상소견서를 보훈병원장에게 보내는 경우
한국의료분쟁조정중재원	감정위원 또는 조사관이 의료사고가 발생한 보건의료기관에 출입하여 관련 문서 또는 물건을 조사·열람 또는 복사하는 경우
국민연금공단	국민연금공단이 부양가족연금, 장애연금 및 유족연금 급여의 지급심사와 관련하여 가입자 또는 가입자였던 사람을 진료한 의료기관에 해당 진료에 관한 사항의 열람 또는 사본 교부를 요청하는 경우

9. 정보주체의 권익보호(4)

▶ 개인정보의 정정·삭제 요구

- **의료법**에 근거하여 수집되는 진료정보는 그 삭제를 요청할 수 없음
(진료기록부, 조산기록부, 간호기록부 등)
- 단, 의료법의 **보존기간이 경과한 진료기록**은 정정·삭제 요구 가능
- 진료정보 이외 **회원정보** 등은 10일 이내 조치 및 결과 통지

▶ 개인정보 유출 시 통지

- 정보주체에게 **지체없이 (5일 이내)** 유출항목, 유출시점 및 경위, 유출에 따른 피해최소화 정보, 개인정보처리자의 대응조치, 피해신고부서 및 연락처 등 고지
- **1만명 이상** 개인정보 유출시 안전행정부나 한국정보화진흥원(NIA), 한국인터넷진흥원(KISA)에 신고

환자의 개인정보 처리기준

FAQ 정보주체가 병원 진료기록 삭제를 요청하는 경우, 어떻게 처리하나요?

- 병원을 더 이상 이용할 계획이 없는 환자가 병원에 자신의 개인정보를 삭제해 달라고 요청하는 경우에도 병원은 의료법에 따라 진료기록을 10년간 보존
- 10년간은 진료기록부에 기재된 개인정보를 환자의 요청에 따라 삭제할 수 없음

FAQ 의료법에서 명시한 보존기간에 대해 적절한 절차를 거쳐 보존기간을 연장한 경우, 정보주체가 삭제 요청을 하는 경우, 어떻게 처리하나요?

- 의료법 시행규칙 제15조에서 정한 기간이 지난 진료정보를 연장하여 보관
- 정보주체가 의료기관에게 그 개인정보의 삭제 요청
- 개인정보보호법 제36조에 따라 필요한 조치(삭제)를 취하고
- 그 결과를 정보주체에게 통보

10. 개인정보 보호 법령의 적용[1]

- ▶ 개인정보보호법은 개인정보 처리에 관한 사항을 규정한 일반법이나,
- ▶ 의료분야를 규율하는 법령 등에 환자나 의료기관 등의 개인정보 처리와 관련된 특별한 규정이 있으면 해당법령이 우선 적용

구 분	조치사항	적용법령
일반원칙	○ 의료법, 국민건강보험법 등에 규정이 있는 경우 해당 법령을 우선 적용 - 규정이 없는 경우 개인정보보호법 적용	○ 개인정보보호법을 적용
수집·이용	○ 진료기록부, 조산기록부, 간호기록부, 환자명부, 처방전, 검사소견서 등은 동의 없이 수집·이용 - 홈페이지 회원정보는 반드시 동의 필요	○ 의료법 제22조 - 의료법시행규칙 제15조
관리	○ 위탁시 문서로 하고 위탁사실 공개 ○ 안전한 관리를 위한 보호조치 이행 - 비밀번호설정, 백신 설치, 암호화 등 ○ 개인정보 처리방침 수립·공개	○ 개인정보보호법 제26조, 제29조, 제30조

10. 개인정보 보호 법령의 적용(2)

구 분	조치사항	적용법령
제3자 제공	○ 개인정보보호법에서 지정하는 경우*외에는 제공이나 열람할 수 없음 * 동의, 법률근거, 급박한 생명·신체의 이익 등	○ 개인정보보호법 제18조 - 국민건강보험법 제47조
열람·정정 삭제	○ 정보주체의 열람 등 요청이 있을 경우 10일 이내 처리 - 법에 따라 수집하는 정보는 정정·삭제 요청 불가 ○ 조제기록부는 환자의 배우자, 직계 존비속 등 가족도 열람요청 가능(의료법 적용)	○ 개인정보보호법 제35조, 제36조 - 국민건강보험법 시행규칙 제58조 - 의료법 제22조
보관 및 파기	○ 보유목적이 달성되면 파기 * 보유기간 : 환자명부 5년, 진료기록부 10년, 처방전 2년 등	○ 개인정보보호법 제21조 - 국민건강보험법 시행규칙 제58조 - 의료법 제22조

10. 개인정보 보호 법령의 적용(3)

구 분	조치사항	적용법령
유출, 침해 대응	○ 정보주체에게 유출사실을 알리고 1만건 이상 유출 시 안전행정부 또는 전문기관(KISA, NIA)에 신고	○ 개인정보보호법 제34조
폐업	○ 민간 의료기관 개설자가 폐업 또는 휴업 신고를 할 때에는 기록·보존하고 있는 진료기록부, 조산기록부, 간호기록부, 그 밖의 진료에 관한 기록을 관할 보건소장에게 이관 ○ 공공 의료기관이 폐업한 경우 그 사무를 승계하는 기관이 없을 때에는 폐업하는 의료기관의 장은 지체 없이 그 기관의 기록물을 소관 영구기록물관리기관으로 이관	○ 의료법 제40조
영상정보 처리기기 운영	○ 공개된 장소에 CCTV 설치시 안내판 설치 및 영상 정보 안전관리	○ 개인정보보호법 제25조

감사합니다

