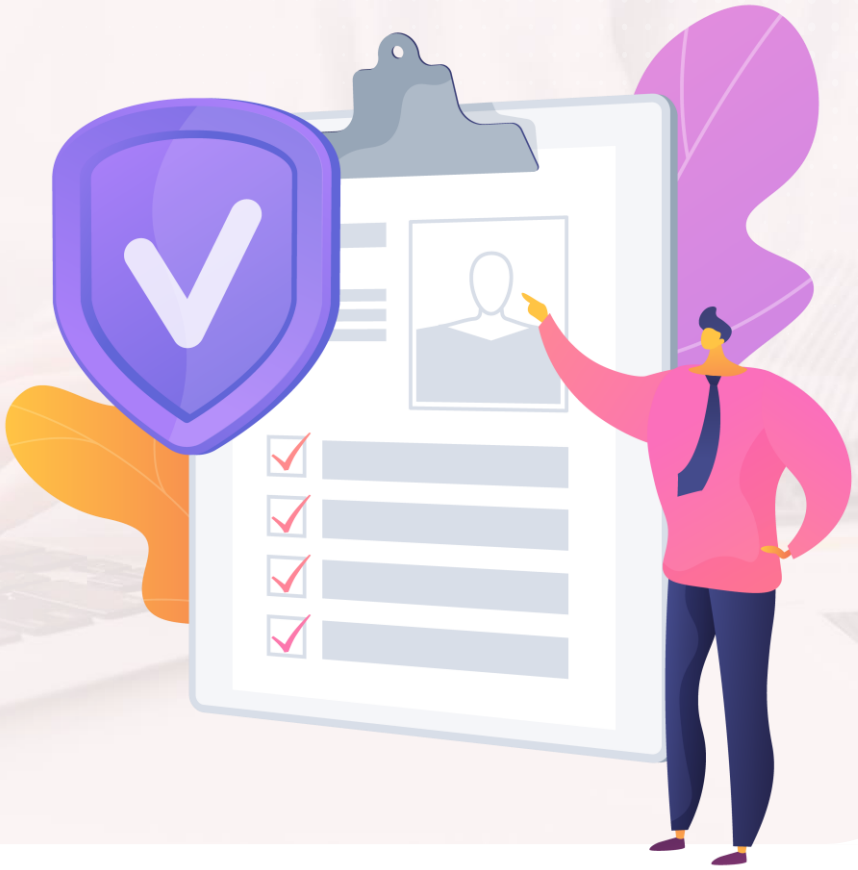
개인정보보호 교육

Institutions Providing Assistance with Health Professionals



보건복지부

h·well 국민건강보험공단

CONTENTS

개인정보보호 교육

Institutions Providing Assistance with Health Professionals

h·well 국민건강보험공단

I. 배경 및 목적

II. 환자의 개인정보 처리기준
1. 진료 신청과정에서 환자의 개인정보 처리기준
2. 진료과정에서 환자의 개인정보 처리기준
3. 처방과정에서 환자의 개인정보 처리기준

III. 개인영상정보 처리기준
1. 공개된 장소
2. 비공개 장소
3. 열람 등 요구 대응

IV. 개인정보 처리 단계별 조치기준
1. 개인정보 개념
2. 개인정보의 수집·이용
3. 개인정보 제3자 제공
4. 개인정보 처리 업무위탁
5. 영업의 양도
6. 영상정보처리기기의 설치 및 운영
7. 개인정보의 안전성 확보
8. 개인정보의 파기
9. 개인정보 처리방침의 수립 및 공개
10. 개인정보 보호책임자 지정
11. 피해 구제방법

V. 참고자료

Ⅰ 배경 및 목적

h·well 국민건강보험공단

배경

환자의 개인정보 보호에 대한 사회적 요구 증가



목적



01 • 의료기관의 업무특성을 고려한 개인정보 처리기준 마련

02 • 의료기관의 개인정보 처리업무 지원

03 • 개인정보 침해 관련 분쟁 예방 및 침해 사고 방지

환자의 개인정보 처리기준

1. 진료 신청과정에서 환자의 개인정보 처리기준

01 • 인터넷, 전화 등을 통한 진료 · 검사 예약 시 개인정보 수집

– 수집할 수 있는 개인정보

① 성명	④ 연락처
② 주민등록번호	⑤ 진료과목
③ 주소	

※ 단, 단순 예약(시간 약속)을 위한 주민등록번호 수집은 원칙적으로 불가

전화 이용 시 주의점

- 통화 내용을 녹취하고 녹취할 때에는 녹취 사실을 정보주체에게 알려야 하며 해당 녹취 파일에 대하여 안전성 확보 조치 필요

인터넷 또는 팩스 이용 시 주의점

- 개인정보의 안전성 확보를 위해 이를 취급할 수 있는 '개인정보 취급자' 최소화
- 수집한 주민등록번호는 암호화하여야 하며 수집한 개인정보는 안전하게 보관 및 관리 필요

환자의 개인정보 처리기준

1. 진료 신청과정에서 환자의 개인정보 처리기준

02 • 진료를 목적으로 하는 개인정보 수집



– 진료 목적의 범위

① 진료와 직접 관련된 진료 신청, 진단, 검사, 치료, 수납 등의 업무
② 진료 신청 문자 발송, 검사 결과 통보 등의 업무
③ 진료와 연결된 예방접종 – 단, 일반적인 접종 안내는 진료 목적의 범위에 미포함
④ 병원 이전 또는 휴업에 관한 정보 – 각종 검사 등과 연결되므로 진료 목적의 범위에 포함

– 방문을 통한 진료 신청 시 정보 주체의 동의 없이 수집할 수 있는 개인정보

① 환자 이름 ② 주민등록번호 ③ 주소 ④ 전화번호 ⑤ 진료과목

※ 단, 진료 목적 외로 의료기관이 홍보 서비스(최신 의학정보, 각종 건강행사 등)를 제공하기 위해서는 정보주체의 별도 동의 필요

h·well 국민건강보험공단

1. 진료 신청과정에서 환자의 개인정보 처리기준

03 요양급여의뢰서에 의한 진료 신청

- 환자가 상급 종합병원에서 2단계 요양급여를 받고자 할 때, 요양급여의뢰서 또는 '상급 종합병원에서의 요양급여가 필요하다' 는 의사소견이 기재된 건강진단, 건강검진결과서를 아래의 개인정보와 함께 제출

① 건강보험증번호	⑤ 상병명
② 가입자 · 세대주 · 환자의 성명 및 주민등록번호	⑥ 상병분류기호
③ 주소	⑦ 진료기관
④ 전화번호	⑧ 환자상태 및 진료소견

- 상급 종합병원에서 1단계 요양급여를 받을 수 있는 경우

① 「응급의료에 관한 법률」 제2조제1호에 해당하는 응급환자인 경우	⑤ 가정의학과에서 요양급여를 받는 경우
② 분만의 경우	⑥ 당해 요양기관에서 근무하는 가입자가 요양급여를 받는 경우
③ 치과에서 요양급여를 받는 경우	⑦ 혈우병환자가 요양급여를 받는 경우
④ 「장애인복지법」 제32조에 따른 등록 장애인 또는 단순 물리치료가 아닌 작업치료 · 운동치료 등의 재활치료가 필요하다고 인정되는 자가 재활의학과에서 요양급여를 받는 경우	

2. 진료과정에서 환자의 개인정보 처리기준

01 진료과정에서 수집하는 개인정보

- 의사가 환자를 진료하면서 수집하는 정보는 법률에 근거한 정보이므로 **환자의 동의 불필요**
- 법률에 근거하여 진료과정에서 수집하는 개인정보

진료기록부	① 진료를 받은 사람의 주소·성명·연락처·주민등록번호 등 인적사항 ② 주된 증상 (이 경우 의사가 필요하다고 인정하면 주된 증상과 관련한 병력·가족력을 추가로 기록 가능) ③ 진단결과 또는 진단명 ④ 진료경과 (외래환자는 재진환자로서 증상·상태, 치료내용이 변동되어 의사가 그 변동을 기록할 필요가 있다고 인정하는 환자만 해당) ⑤ 치료 내용 (주사·투약·처치 등) ⑥ 진료일시	
간호기록부	① 간호를 받는 사람의 성명 ② 체온·맥박·호흡·혈압에 관한 사항 ③ 투약에 관한 사항	④ 섭취 및 배설물에 관한 사항 ⑤ 처치와 간호에 관한 사항 ⑥ 간호일시
수술기록부	① 환자의 성명 ② 수술명	③ 수술기록 ④ 수술의사의 성명

2. 진료과정에서 환자의 개인정보 처리기준

01 진료과정에서 수집하는 개인정보



- 법률에 근거하지 않은 개인정보를 수집하기 위해서는 환자의 동의 필요
- 환자의 동의를 받을 때 알려야 하는 사항

① 개인정보의 수집. 이용목적

② 수집하려는 개인정보의 항목

③ 개인정보의 보유 및 이용 기간

④ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

h·well 국민건강보험공단

2. 진료과정에서 환자의 개인정보 처리기준

02 진료정보의 목적 외 이용 및 제3자 제공



[진료정보] 수집한 의료기관에서 **진료 목적으로만 이용**하여야 하며,
그 범위를 초과하여 이용하거나 제 3자에게 제공하는 것은 금지

[진료정보 외 개인정보] 진료정보 외 개인정보를 목적 외 이용하거나 제3자에게 제공할 경우에는 정보주체로부터 별도의 동의 필요

- **정보주체의 동의를 받을 때 알려야 하는 사항**

① 개인정보를 제공받는 자
② 개인정보의 이용 목적 (제공 시에는 제공받는 자의 이용 목적)
③ 이용 또는 제공하는 개인정보의 항목
④ 개인정보의 보유 및 이용 기간 (제공 시에는 제공받는 자의 보유 및 이용기간)
⑤ 동의를 거부할 권리가 있다는 사실과 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

h·well 국민건강보험공단

2. 진료과정에서 환자의 개인정보 처리기준

03 다른 법률에 특별한 규정이 있는 경우 : 다른 법률의 특별한 규정에 의한 의료인의 신고의무

환자 진료기록 확인

- 자신이 진료했거나 진료하고 있는 환자의 진료기록 내용을 확인하거나 소견 등을 송부할 것을 요청 받은 경우, 해당 환자나 환자 보호자의 동의 필요
- 다만, 해당 환자의 의식이 없거나 응급환자인 경우, 환자의 보호자가 없어 동의를 받을 수 없는 경우에는 환자나 보호자의 동의 없이 송부 가능 (「의료법」 제21조 제3항)

h·well 국민건강보험공단

2. 진료과정에서 환자의 개인정보 처리기준

03 다른 법률에 특별한 규정이 있는 경우 : 다른 법률의 특별한 규정에 의한 의료인의 신고의무

감염병 환자 등 신고 → **소속 의료기관장에게 보고**

의사 및 한의사	의료기관장
① 감염병 환자, 감염병 의사환자 또는 병원체보유자를 진단하거나 그 사체를 검안한 경우 ② 예방접종, 예방접종 후 이상반응자를 진단하거나 그 사체를 검안한 경우 ③ 감염병 환자 등이 제1군 감염병부터 제4군 감염병까지에 해당하는 감염병으로 사망한 경우	**제 1군 감염병 ~ 제 4군 감염병** : 지체없이 관할 보건소장에게 신고 **제 5군 감염병 ~ 지정 감염병** : 7일 이내에 관할 보건소장에게 신고

- 신고 시 아래의 진료기록을 포함하여 ‘감염병발생신고서’ 작성

① 감염병 환자 · 감염병 의사환자 · 병원체보유자의 성명	④ 직업	⑧ 발병일	⑪ 입원여부
② 주민등록번호	⑤ 성별	⑨ 확진 검사결과	⑫ 추정감염경로
③ 전화번호	⑥ 주소	⑩ 환자 등 분류	⑬ 사망여부 등
	⑦ 감염병명		

h·well 국민건강보험공단

2. 진료과정에서 환자의 개인정보 처리기준

03 • 다른 법률에 특별한 규정이 있는 경우 : 다른 법률의 특별한 규정에 의한 의료인의 신고의무

응급환자의 이송

- 의료인은 해당 능력으로 응급환자에 대하여 적절한 응급의료를 할 수 없다고 판단하는 경우 지체 없이 환자를 응급의료가 가능한 다른 의료기관으로 이송
- **응급환자 이송 시** : 응급환자의 안전한 이송에 필요한 의료기구와 인력 제공
  : 응급환자를 이송 받는 기관에 '응급환자진료의뢰서' 및 진료에 필요한 의무기록 송부 필요

특정수혈부작용 신고

- 의료기관의 장은 특정수혈부작용이 발생한 경우 '특정수혈부작용발생신고서'를 작성하여 보건복지부장관에게 신고

뇌사추정자 신고

뇌사로 추정되는 사람을 진료한 의료기관장 ▶▶▶ 장기구득기관의 장 ▶▶▶ 국립장기이식관리기관장

① 의료기관의 명칭 및 알리는 사람의 성명
② 뇌사추정자의 성명, 생년월일 및 주소
③ 뇌사추정자의 상태 및 발생원인

해당 사실 신고

신고 접수

3. 처방과정에서 환자의 개인정보 처리기준

01 처방전의 교부

- 진료과정이 끝나면 의사나 치과의사는 처방전을 작성하여 교부 또는 발송하고 의료기관은 진료가 끝난 환자의 개인정보를 보호하기 위한 안전성 확보조치 진행
- 의사나 치과의사는 처방전 2부를 발급하여 환자에게 직접 교부
- 환자가 처방전을 추가로 발급하여 줄 것을 요구하는 경우에는 환자가 원하는 약국으로 처방전 송부 가능
- 처방전은 2년간 보존할 수 있으며 필름 등에 원본대로 수록하여 보존 가능
- 처방전을 보존하는 경우, 필름촬영책임자가 필름의 표지에 촬영 일시와 본인의 성명을 적고 서명 또는 날인
- 처방전 기재 사항

① 환자의 성명 및 주민등록번호 ② 의료기관의 명칭 및 전화번호 ③ 「통계법」 제22조 제1항 전단에 따른 한국표준질병 · 사인 분류에 따른 질병분류기호	④ 의료인의 성명·면허종류 및 번호 ⑤ 처방 의약품의 명칭(일반명칭, 제품명이나 대한약전에서 정한 명칭) · 분량 · 용법 및 용량 ⑥ 처방전 발급 연월일 및 사용기간 ⑦ 의약품 조제 시 참고 사항

환자의 개인정보 처리기준

3. 처방과정에서 환자의 개인정보 처리기준

02 · 진료비의 수납

- 일련의 진료과정을 마친 후 진료비 수납을 위해 필요한 최소한의 정보(카드사 및 카드번호, 카드승인번호 등) 수집 가능
- 수집한 수납정보의 안전성 확보를 위한 조치 필요

03 · 환자의 개인정보관리

- 환자의 개인정보는 관리적 · 기술적 · 물리적 보호조치를 통하여 안전하게 관리
- 보존기간이 경과하고 수집이용목적이 달성된 개인정보는 5일 이내 파기
- 환자 개인정보의 정확성 및 최신성을 확보할 수 있도록 열람 보장
- 의료인이 거짓으로 작성하거나 고의로 사실과 다르게 기록한 사항에 대하여 정정 삭제 등을 허용하는 대책 마련 필요
- 환자로부터 환자의 개인정보에 대한 열람, 정정삭제, 처리정지 요구서를 받은 경우 10일 이내 처리 결과 통지

개인영상정보 처리기준

공개된 장소

의료기관의 불특정 다수에게 공개된 장소에 영상정보처리기기를 설치 · 운영하고자 하는 경우 아래 사항 준수

- 영상정보처리기기 설치 · 운영 제한 및 필요한 최소한의 촬영
- 영상정보처리기기 임의조작 · 녹음 금지
- 안내판 설치를 통한 설치 사실 공지
- 영상정보처리기기 운영 · 관리 방침 수립 공개 및 책임자 지정
- 영상정보의 목적 외 이용 · 제공 제한 및 보관 · 파기 철저
- 영상정보처리기기의 설치 · 운영 위탁 시 관리 · 감독 철저
- 개인영상정보의 안전성 확보 조치 및 자체 점검 실시

- 불특정 다수가 이용하는 목욕실, 화장실, 발한실, 탈의실 등 개인의 사생활을 침해할 우려가 있는 장소의 내부를 볼 수 있도록 하는 영상정보처리기기의 설치 · 운영은 금지되지만 법령으로 정하는 시설은 예외로 허용

비공개 장소

의료기관의 출입제한이 있는 공간에 영상정보처리기기를 설치하여 개인정보를 수집하는 경우에는 정보주체의 수집이용 동의 필요

- 동의를 받을 때는 영상정보 수집의 목적, 보유기간 등을 알리고 동의를 받아야 하며 반드시 수집 목적으로만 이용

열람 등 요구대응

정보주체는 자신이 촬영된 개인영상정보 및 정보주체의 이익을 위해 필요한 개인영상정보를 요구할 권리 보유

- 의료기관은 개인영상정보의 열람 또는 존재확인 요구를 받은 경우 지체 없이 해당 조치 실시
  [본인 혹은 정당한 대리인: 신분증명서 확인]

- 보관기간이 경과하여 파기한 경우, 정보주체의 열람요구를 거부할 정당한 사유가 존재하는 경우 제외
  – 열람 거부 시 거부사유를 10일 이내에 서면으로 해당정보주체에게 통지

- 열람 등의 조치를 취할 때 정보주체 이외의 사람의 사생활 침해가 우려될 경우 정보주체 이외의 사람의 개인영상정보를 알아보지 못하도록 조치

개인정보 처리단계별 조치기준

1. 개인정보의 개념

01 개인정보란

- 가명 처리하여 원래의 상태로 복원하기 위한 추가 정보의 사용 · 결합 없이는 특정 개인을 알아볼 수 없는 정보

- 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려

- 해당 정보를 처리하는 자의 입장에서 합리적으로 활용될 가능성이 있는 수단 고려



- 자연인에 관한 정보만 해당
- 국적이나 신분에 관계 없이 법 적용대상 (Ex. 외국인, 피의자 정보)

- 법인 또는 단체의 정보는 해당되지 않으나 연관성에 따라 개인정보로 취급 가능 (Ex. 대표자 성명, 담당자 전화번호)

- 전자, 수기 등 형태와 처리방식은 무관
- 주관적 평가, 허위정보라도 상황에 따라 해당 가능 (Ex. 평가표, 예명)

1. 개인정보의 개념

02 개인정보 보호원칙

- 「개인정보보호법」은 정보주체의 '개인정보 자기결정권' 보장
- '개인정보 자기결정권'을 보장하기 위하여
  개인정보의 수집 · 이용 · 제공 등이 정당한 절차에 따라 이루어지며
  개인정보가 내부자의 고의나 관리 부주의 또는 외부의 공격으로
  유출 · 변조 · 훼손되지 않도록 안전한 관리 필요
- 개인정보 보호 원칙

개인정보보호법	OECD 가이드라인
목적에 필요한 최소한의 범위 안에서 적법하고 정당하게 수집	수집 제한의 원칙
처리목적 범위 안에서 정확성·안전성·최신성 보장	정보 정확성의 원칙
처리목적의 명확화	목적 명확화 원칙
필요목적 범위 안에서 적법하게 처리, 목적 외 활용 금지	이용 제한의 원칙
정보주체의 권리침해 위험성 등을 고려, 안전성 확보	안전 보호의 원칙
개인정보 처리사항 공개	공개의 원칙
열람청구권 등 정보주체의 권리보장	개인 참여의 원칙
개인정보처리자의 책임준수·실천, 신뢰성 확보 노력	책임의 원칙

03 법령의 적용

- 의료기관에서 개인정보를 규율하고 있는 다른 법령에 환자, 의료인, 직원의 개인정보 처리와 관련된 특별한 규정이 있으면
  해당 법령이 우선적으로 적용되며, 그렇지 않은 경우 「개인정보보호법」 적용

2. 개인정보의 수집 · 이용

01 개인정보 수집 요건

- 의료기관이 개인정보를 수집 · 이용하기 전,
  ①법률에 특별한 규정이 있거나 ②법령상 의무 준수를 위해 불가피한 경우가 있는지 선확인 필요



FAQ 동의를 받아야 하는 경우 반드시 서면으로 받아야 하나요?

- **반드시 서면으로 받을 필요는 없습니다.**
  「개인정보보호법」
  시행령 제17조에 따르면
  다음과 같은 방법으로
  동의를 받을 수도 있습니다.

① 동의 내용이 적힌 서면을 정보주체에게 직접 발급하거나 우편 또는 팩스 등의 방법으로 전달하고, 정보주체가 서명하거나 날인한 동의서를 받는 방법
② 전화를 통하여 동의 내용을 정보주체에게 알리고 동의의 의사표시를 확인하는 방법
③ 전화를 통하여 동의 내용을 정보주체에게 알리고 정보주체에게 인터넷주소 등을 통하여 동의 사항을 확인하도록 한 후 다시 전화를 통하여 그 동의 사항에 대한 동의의 의사표시를 확인하는 방법
④ 인터넷 홈페이지 등에 동의 내용을 게재하고 정보주체가 동의 여부를 표시하도록 하는 방법
⑤ 동의 내용이 적힌 전자우편을 발송하여 정보주체로부터 동의의 의사표시가 적힌 전자우편을 받는 방법
⑥ 그 밖에 ①~⑤에 따른 규정에 준하는 방법으로 동의 내용을 알리고 동의의 의사표시를 확인하는 방법

2. 개인정보의 수집 · 이용

02 수집 제한과 입증책임

- 개인정보를 수집할 때에는 필요한 최소한의 개인정보 수집
- 필요한 최소한의 개인정보 수집이라는 입증책임은 해당 개인정보를 수집한 의료기관이 부담
- 필요한 최소한의 개인정보 외의 수집에 동의하지 아니한다는 이유로 정보주체에게 서비스 제공을 거부해서는 안됨

03 고유식별정보 및 민감정보의 수집

고유식별정보	주민등록번호, 운전면허번호, 여권번호, 외국인등록번호
민감정보	사상 · 신념, 노동조합 · 정당의 가입 · 탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 유전정보, 범죄경력자료 등

- 고유식별정보 및 민감정보를 수집 · 이용하는 경우에는 법령에 구체적인 수집 · 이용근거가 있는지 확인 필요
- 의료기관은 법령에 따라 진료목적을 위하여 고유식별정보 및 민감정보를 수집하고 진료 목적을 위해 이용 가능

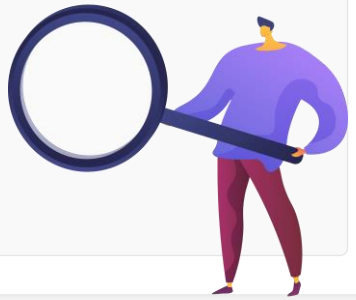
2. 개인정보의 수집 · 이용

04 금지되는 개인정보 수집 · 이용

- 부정한 수단이나 방법을 통한 개인정보의 수집 · 이용
- 거짓이나 그 밖의 부정한 수단이나 방법으로 개인정보를 취득하거나 처리에 관한 동의를 받아서는 안됨

FAQ 경찰이 문서로 환자의 인적사항 제공을 요구할 경우 어떤 조치를 취해야 하나요?

- **경찰로부터 환자의 인적사항 요구가 있는 경우에는 정보주체인 환자로부터 별도의 동의를 받아 해당 개인정보를 제공할 수 있습니다.**
  이 경우 정보주체인 환자에게 [①개인정보를 제공받는 자, ②개인정보를 제공받는 자의 이용 목적, ③제공하는 개인정보의 항목, ④개인정보를 제공받는 자의 보유 및 이용 기간, ⑤동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용]을 알려야 하고, 이와 같은 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 합니다.
- 경찰이 「형사소송법」 제106조 또는 제215조, 제218조에 따른 압수 · 수색영장에 의하여
  해당 환자의 개인정보를 압수하는 것은 「민사소송법」 제347조에 의하여
  “다른 법률에 특별한 규정이 있는 경우” 에 해당하므로 환자의 동의 없이 해당 개인정보를 제공할 수 있습니다.



h·well 국민건강보험공단

3. 개인정보 제3자 제공

01 · 제3자 제공 조건 : 의료기관이 환자 등의 개인정보를 제3자에게 제공하기 위해서 확인해야 하는 해당 요건

① 환자 등 정보주체의 동의를 받은 경우
② 환자 등 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태이거나 주소불명 등으로 사전동의를 받을 수 없는 경우
③ 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위해 불가피한 경우
④ 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우

02 · 제3자 제공 조건 : 개인정보를 수집 목적 외로 사용하거나 제3자에게 제공하기 위해서 확인해야 하는 해당 사유

① 정보주체로부터 별도의 동의를 받은 경우
② 다른 법률에 특별한 규정이 있는 경우
③ 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
④ 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우
⑤ 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의 · 의결을 거친 경우
⑥ 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우
⑦ 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
⑧ 법원의 재판업무 수행을 위하여 필요한 경우
⑨ 형 및 감호, 보호처분의 집행을 위하여 필요한 경우

4. 개인정보 처리위탁

01 위탁 방법

- 의료기관에서 환자 등의 개인정보 처리업무를 위탁하는 경우 문서에 포함되어야 하는 사항

개인정보처리 위탁계약서 기재사항	① 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항 ② 개인정보의 기술적·관리적 보호조치에 관한 사항 ③ 위탁업무의 목적 및 범위 ④ 재위탁 제한에 관한 사항 ⑤ 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항 ⑥ 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항 ⑦ 법 제26조 제2항에 따른 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

02 위탁업무 등의 공개

- 개인정보 처리업무를 위탁하는 의료기관은 개인정보 처리업무를 위탁 받아 처리하는 수탁자를 환자 등 정보주체가 언제든지 자유롭게 확인할 수 있도록 홈페이지에 '개인정보 처리방침' 지속적으로 게재
- 인터넷 홈페이지에 게재할 수 없는 경우, 다음의 방법 중 하나 이상의 방법으로 위탁하는 업무의 내용과 수탁자 공개

인터넷 이외의 방법에 의한 위탁업무 공개방법	① 위탁자의 사업장 · 영업소 · 사무소 · 점포 등(이하 "사업장 등")의 보기 쉬운 장소에 게시하는 방법 ② 관보나 위탁자의 사업장 등이 있는 시 · 도 이상의 지역을 주된 보급지역으로 하는 「신문 등의 진흥에 관한 법률」 제2조 제1호 가목 · 다목 및 같은 조 제2호에 따른 일반일간신문, 일반주간신문 또는 인터넷신문에 싣는 방법 ③ 같은 제목으로 연 2회 이상 발행하여 정보주체에게 배포하는 간행물 · 소식지 · 홍보지 또는 청구서 등에 지속적으로 싣는 방법 ④ 재화나 용역을 제공하기 위하여 위탁자와 정보주체가 작성한 계약서 등에 실어 정보주체에게 발급하는 방법

h·well 국민건강보험공단

4. 개인정보 처리위탁

03 수탁자 교육 및 감독

- 개인정보 처리업무를 위탁한 의료기관은 수탁자에 대하여 개인정보가 분실 · 도난 · 유출 · 변조 · 훼손되지 않도록 교육
- 개인정보 처리업무를 위탁한 의료기관은 수탁자가 의료기관이 준수하여야 하는 사항을 준수하고 있는지 감독

수탁자 준수사항	① 보호조치에 관한 사항 ② 위탁업무의 목적 및 범위 ③ 재위탁 제한에 관한 사항 ④ 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항 ⑤ 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항

04 손해배상 책임

- 수탁자가 위탁 받은 업무와 관련하여 개인정보를 처리하는 과정에 「개인정보보호법」을 위반하여 발생한 손해배상 책임에 대하여 수탁자를 의료기관의 소속 직원으로 간주

5. 영업의 양도

- 영업의 양도, 합병 등으로 정보주체의 개인정보를 다른 의료기관에게 이전하여야 하는 때에는 개인정보를 이전하기 전에 환자 등 해당 정보주체에게 다음의 방법으로 내용 통지

통지사항	통지방법
① 개인정보를 이전하려는 사실 ② 개인정보를 이전 받는 자(영업양수자 등)의 성명 (법인의 경우에는 법인의 명칭), 주소, 전화번호 및 그 밖의 연락처 ③ 정보주체가 개인정보의 이전을 원하지 아니하는 경우 조치할 수 있는 방법 및 절차	① 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법 ② 개인정보를 이전하려는 의료기관이 과실 없이 서면 등에 따른 방법으로 통지사항을 정보주체에게 알릴 수 없는 경우, 해당 사항을 인터넷 홈페이지에 30일 이상 게재 ▶ 다만, 인터넷 홈페이지를 운영하지 아니하는 의료기관은 사업장 등의 보기 쉬운 장소에 30일 이상 게시

- 영업의 양도, 합병 등으로 개인정보를 이전 받은 경우 이전 당시의 본래 목적으로만 개인정보를 이용할 수 있으며 「개인정보보호법」의 개인정보처리자로서의 권리와 의무 발생

6. 영상정보처리기기의 설치 및 운영

01 영상정보처리기기 설치 및 운영 제한

- 공개된 장소에서의 영상정보처리기기 설치는 원칙적으로 금지되지만 다음 사유에 해당하는 경우 설치 가능

① 법령에서 구체적으로 허용하고 있는 경우
② 범죄의 예방 및 수사를 위하여 필요한 경우
③ 시설 안전 및 화재 예방을 위하여 필요한 경우
④ 교통단속을 위하여 필요한 경우
⑤ 교통정보의 수집·분석 및 제공을 위하여 필요한 경우

- 목욕탕, 화장실 등 개인의 사생활을 현저히 침해할 우려가 있는 장소는 영상정보처리기기의 설치 및 운영 금지
- 영상정보처리기기를 설치목적과 다른 목적으로 임의로 조작하거나 다른 곳을 비추거나 녹음기능을 사용하는 것 금지

02 영상정보처리기기 설치 시 의견 수렴

공공기관이 공개된 장소에 영상정보처리기기 설치 시	개인 사생활 침해 우려 장소에 영상정보처리기기 설치 시 (교정시설, 정신의료기관 등)
• 「행정절차법」에 따른 행정예고의 실시 또는 의견 청취 • 해당 영상정보처리기기의 설치로 직접 영향을 받는 지역 주민 등을 대상으로 하는 설명회, 설문조사, 여론조사	• 관계 전문가 • 해당시설에 종사하는 사람, 해당 시설에 구금되어 있거나 보호받고 있는 사람 또는 그 사람의 보호자 등 이해관계인

h·well 국민건강보험공단

6. 영상정보처리기기의 설치 및 운영

03 안내판 설치를 통한 설치 및 운영 사실 공개

- 의료기관이 공개된 장소에 영상정보처리기기를 설치 및 운영할 때 정보주체가 쉽게 알아볼 수 있도록 안내판 설치

안내판에 기재하여야 할 사항	① 설치 목적 및 장소 ② 촬영 범위 및 시간 ③ 관리책임자의 성명(또는 직책) 및 연락처 ④ (영상정보처리기기 설치 · 운영을 위탁한 경우) 수탁관리자 성명(또는 직책), 업체명 및 연락처

04 영상정보처리기기 운영 및 관리 방침

- 영상정보처리기기를 운영하는 의료기관은 영상정보처리기기 운영관리 방침을 수립하여 홈페이지, 게시판 등에 공개
- 개인영상정보처리에 관한 업무를 총괄하여 책임질 '개인영상정보 관리책임자' 지정

6. 영상정보처리기기의 설치 및 운영

05 영상정보의 목적 외 이용 · 제공 제한 및 보관 · 파기 철저



- 아래의 경우를 제외하고 개인영상정보를 수집목적 이외로 이용 또는 제3자에게 제공 금지

개인영상정보 이용 및 제3자 제공의 허용

① 정보주체의 별도의 동의를 얻은 경우
② 다른 법률에 특별한 규정이 있는 경우
③ 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
④ 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인영상정보를 제공하는 경우
⑤ 개인영상정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 개인정보 보호위원회의 심의·의결을 거친 경우
⑥ 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우
⑦ 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
⑧ 법원의 재판업무 수행을 위하여 필요한 경우
⑨ 형 및 감호, 보호처분의 집행을 위하여 필요한 경우

- 영상정보의 보관기간은 개인영상정보 수집 후 30일 이내로 하고, 이 기간이 종료되면 파기

h·well 국민건강보험공단

6. 영상정보처리기기의 설치 및 운영

06 개인영상정보 열람 · 존재확인 · 파기 청구권 보장

- 영상정보처리기기를 운영하는 의료기관은 정보주체로부터 개인영상정보의 열람, 존재확인, 또는 파기를 요청 받은 경우 지체없이 필요한 조치 실시
- 다만, 의료인 폭행 등과 같이 정보주체의 요구를 거부할 만한 정당한 사유가 존재하는 경우에는 거부사유를 10일 이내에 서면으로 정보주체에게 통지하고 열람 거부

07 개인영상정보의 안전성 확보 조치 및 자체 점검 실시

- 영상정보처리기기를 운영하는 의료기관은 개인영상정보가 분실 · 도난 · 유출 · 변조 또는 훼손되지 않도록 안전성 확보
- 영상정보처리기기를 운영하는 보건복지부 소관 공공의료기관은 「보건복지부 개인정보 보호 기본지침」 준수 여부에 대한 자체점검을 통해 개인영상정보의 침해 방지를 위한 노력 필요

개인정보 처리단계별 조치기준

7. 개인정보의 안전성 확보

내부관리 계획 수립 · 시행

- 환자 등 정보주체의 개인정보를 안전하게 처리하기 위해 내부관리 계획 수립 · 시행

내부관리 계획 필수 기재사항

① 개인정보 보호책임자의 지정에 관한 사항

② 개인정보 보호책임자 및 개인정보 취급자의 역할 및 책임에 관한 사항

③ 개인정보의 안전성 확보에 관한 사항

④ 개인정보취급자에 대한 교육에 관한 사항

⑤ 그 밖에 개인정보 보호를 위하여 필요한 사항

접근권한 관리

- 개인정보처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에게 차등 부여
- 퇴직 등 인사변동이 발생하여 개인정보 취급자가 변경된 경우, 지체 없이 시스템 접근권한 변경 또는 말소
- 접근권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년 동안 보관
- 개인정보처리시스템에 접근할 수 있는 사용자 계정은 취급자 별로 발급하여야 하며 다른 취급자와 공유되지 않도록 관리

비밀번호 관리

- 개인정보취급자가 안전한 비밀번호를 설정할 수 있도록 '비밀번호 작성규칙' 수립
- 비밀번호 분실 시, SMS 등을 통해 본인 확인 절차를 거쳐 비밀번호를 재설정 하도록 관리
- 일정횟수 이상 비밀번호 입력 오류 시 계정 잠금 등을 통해 로그인 시도 차단

개인정보 처리단계별 조치기준

7. 개인정보의 안전성 확보

접속기록의 보관 및 위변조 방지

- 환자 등 정보주체의 개인정보를 안전하게 처리하기 위해 내부관리 계획 수립 · 시행

접속기록의 의의

– 접속기록은 개인정보의 중요한 정보를 기록하는 로그파일을 생성하여 불법적인 접근 또는 행동을 확인 할 수 있는 중요한 자료이며 접속기록의 백업은 개인정보 DB의 무결성을 유지하기 위한 중요 요소

보안프로그램의 설치 및 운영

- 의료기관은 악성 프로그램 등을 방지 · 치료할 수 있는 백신 소프트웨어 등의 보안프로그램 설치 · 운영

보안프로그램 설치 및 운영 방법

① 백신 소프트웨어 등 보안프로그램 반드시 설치 · 운영

② 자동 업데이트 기능을 사용하거나 일 1회 이상 업데이트 실시

③ 악성 프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트 실시

개인정보 보관시설

- 의료기관은 개인정보를 보관하는 장소에 대한 출입통제 계획 확보

- 보안사고 예방 및 사고 발생 시 증적을 확보할 수 있도록 보관시설에 CCTV 설치 권고

8. 개인정보의 파기

- 의료기관은 보유기간이 경과되었거나 개인정보의 처리목적 달성 등 개인정보가 불필요하게 되었을 때 지체 없이 해당 개인정보 파기
- 파기할 때는 복구 또는 재생되지 않도록 조치

진료기록의 보존기간	
환자명부	5년
진료기록부	10년
처방전	2년
수술기록	10년
검사소견기록	5년
방사선 사진 및 그 소견서	5년
간호기록부	5년
조산기록부	5년
진단서 등의 부본	3년

진료기록 보존방법

① 마이크로필름이나 광디스크 등에 원본대로 수록하여 보존

② 위와 같은 방법으로 진료기록을 보존하는 경우, 필름촬영책임자가 필름의 표지에 촬영 일시와 본인의 성명을 적고 서명 또는 날인

진료기록 파기방법

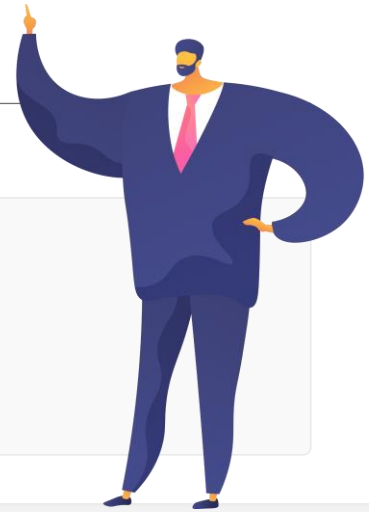
① 전자적 파일 형태인 경우 : 복원이 불가능한 방법으로 영구 삭제

② 전자적 파일 이외의 기록물, 인쇄물, 서면, 그 밖의 기록매체 : 파쇄 또는 소각

9. 개인정보 처리방침의 수립 및 공개

– 의료기관은 다음의 사항이 포함된 개인정보 처리방침 수립 및 홈페이지 등을 통하여 공개

필수 기재사항	① 개인정보의 처리 목적 ② 개인정보의 처리 및 보유 기간 ③ 개인정보의 제3자 제공에 관한 사항 (해당되는 경우에만 수립) ④ 개인정보처리의 위탁에 관한 사항 (해당되는 경우에만 수립) ⑤ 정보주체의 권리·의무 및 그 행사방법에 관한 사항 ⑥ 처리하는 개인정보의 항목 ⑦ 개인정보의 파기에 관한 사항 ⑧ 개인정보 보호책임자에 관한 사항 ⑨ 개인정보 처리방침의 변경에 관한 사항 ⑩ 개인정보의 안전성 확보 조치에 관한 사항
선택적 기재사항	① 정보주체의 권익침해에 대한 구제방법 ② 개인정보의 열람청구를 접수 · 처리하는 부서



– 인터넷 홈페이지를 운영하지 않거나 인터넷 홈페이지 관리가 어려운 경우 아래의 방법으로 개인정보 처리방침 공개

① 개인정보처리자의 사업장 등 보기 쉬운 장소에 게시
② 일반일간신문, 일반주간신문 또는 인터넷신문
③ 연 2회 이상 발행하여 정보주체에게 배포하는 간행물 · 소식지 · 홍보지 또는 청구서
④ 재화나 용역을 제공하기 위하여 개인정보처리자와 정보주체가 작성한 계약서 등에 실어 정보주체에게 발급

10. 개인정보 보호책임자 지정

- 개인정보 처리에 관한 업무 총괄 및 다음의 업무 수행을 위한 개인정보 보호책임자 지정
- 개인정보 보호책임자 지정 및 변경한 경우: 개인정보보호책임자의 지정 및 변경사실, 부서명, 전화번호 등 공개

개인정보 보호책임자의 업무	① 개인정보 보호 계획의 수립 및 시행 ② 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선 ③ 개인정보 처리와 관련한 불만의 처리 및 피해 구제 ④ 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축 ⑤ 개인정보 보호 교육 계획의 수립 및 시행 ⑥ 개인정보파일의 보호 및 관리·감독 ⑦ 개인정보 처리방침 수립·변경 및 시행 ⑧ 개인정보 보호 관련 자료의 관리 ⑨ 처리목적이 달성되거나 보유기간이 경과한 개인정보 파기 ⑩ 개인정보침해 관련 민원의 접수 · 처리 ⑪ 개인정보취급자가 등록 또는 변경등록 신청한 개인정보파일의 등록 또는 변경등록 사항의 적정성에 대한 판단 및 행정자치부 등록 ⑫ 그 밖에 개인정보 보호를 위하여 필요한 업무
개인정보 보호책임자의 자격 및 권한	자격 • 의료기관의 대표자 또는 개인정보 처리 관련 업무를 담당하는 부서의 장 또는 개인정보보호에 관한 소양이 있는 사람 권한 • 개인정보의 처리 현황, 처리 체계 등에 대하여 수시로 조사 또는 관계 당사자로부터 보고 청취

개인정보 처리단계별 조치기준

11. 피해 구제방법 – 개인정보 침해사실 신고처리절차



01 → 02 → 03 → 04

신고

신고인

- 행정자치부장관에게 신고

행정자치부장관

- 신고접수
- 해당기관장에게 접수사실 통보

사실확인

행정자치부장관

- 신고사실 확인 위해 관련 기관장에게 협조요청
- 신고인 등 의견제출 가능

처리

해당 기관장

- 관련 징계고발 및 안전성 확보조치 등 처리
- 처리결과 행정자치부장관에게 통보

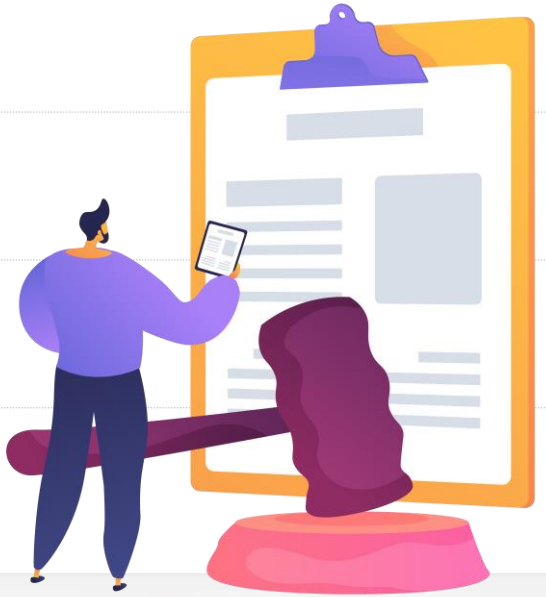
처리결과 통지

행정자치부장관

- 통보 받은 처리결과를 신고인에게 통지

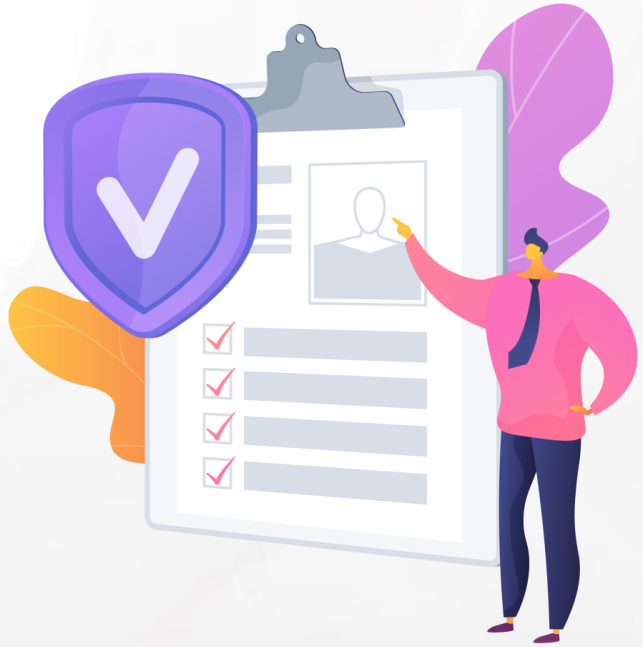
참고자료 의료분야 관련 법령

- **의료법**
  - 제 17조 진단서 등
  - 제 19조 비밀누설금지
  - 제 21조 기록열람 등
- **의료법 시행규칙**
  - 제 13조의 2(기록 열람 등의 요건)
  - 제 14조 진료기록부 등의 기재사항
  - 제 28조 의료기관 개설허가 사항의 변경허가
  - 제 30조 폐업 및 휴업의 신고
- **감염병 예방 및 관리에 관한 법률 시행규칙**
  - 제 6조 의사 등의 감염병 발생 신고
- **응급의료에 관한 법률**
  - 제 11조 응급환자의 이송
- **혈액관리법 시행규칙**
  - 제 13조 특정수혈부작용의 신고 등
- **장기 등 이식에 관한 법률**
  - 제 10조 국립장기이식관리기관



출처

- 개인정보보호 가이드라인 [의료기관편], 2015, 보건복지부/행정자치부
- 초급과정_개인정보보호법_주요내용, 2021, 개인정보보호위원회/KISA



보건복지부

h·well 국민건강보험공단