

개인정보보호법 주요내용 및 적용사례

[상조업 중심]

2012년 2월



행정안전부

① 용어정의

개인정보

§ 성명, 주민번호 등을 통하여 살아있는 개인을 알아볼 수 있는 정보
§ 다른 정보와 용이하게 결합하여 개인을 알아볼 수 있는 정보
※ 성명, 주소, 전화번호 등 이외에 컴퓨터 IP주소, e-mail 등도 개인정보에 포함됨
※ 명함, 이메일 수집? 개인신용정보?

처리

§ 개인정보의 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기 기타 이와 유사한 행위

정보주체

§ 처리되는 정보에 의해 알아볼 수 있는 그 정보의 주체가 되는 사람
※ 정보통신망법 상의 이용자는 '영리목적으로 서비스를 이용하는 사람'이 해당되므로 개인정보보호법에 따른 정보주체와는 구분됨(신용정보법 상 신용정보주체)

개인정보 처리자

§ 업무를 목적으로 개인정보파일을 운용하기 위하여 개인정보를 처리하는 공공기관, 법인, 단체, 개인 등
※ 정보통신망법 상의 정보통신서비스제공자는 '영리를 목적으로 서비스를 제공하는 자'를 의미하므로 개인정보보호법의 개인정보처리자와 구분됨(신용정보법 상 신용정보업, 신용정보회사)

개인정보 파일

§ 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보 집합물

영상정보 처리기기

§ 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 전송하는 장치
※ 폐쇄회로 텔레비전(CCTV), 네트워크 카메라

② 법률 적용대상 및 범위

법 시행 이전

- ☹ 분야별 개별법이 있는 경우에 한해 개인정보 보호의무 적용(약 51만)
 - 공공기관 : 「공공기관 개인정보보호법」 - 신용정보 제공·이용자 : 「신용정보법」
 - 정보통신서비스제공자 : 「정보통신망법」 - 여행사, 백화점 등 준용사업자 : 「정보통신망법」

법 시행 이후

- ☹ 적용대상 : 공공·민간부문의 모든 개인정보처리자
 - 포털, 금융기관, 병원, 학원, 제조업, 서비스업 등 72개 업종 350만 전체 사업자
 - 국회·법원·헌법재판소·중앙선거관리위원회 등 헌법기관
 - 부처, 지자체, 공사,공단, 학교 등 2.8만 전체 공공기관
 - 사업자 협회·동창회 등 비영리단체
- ☹ 적용범위 : 전자파일 형태외에 동창회 명부, 민원서류, 이벤트 응모권 등 수기문서 포함

※ 법 적용 일부 제외(법58조)

- 영상정보처리기는 개인정보 수집이용(법 제15조), 동의 받는 방법(법 제22조), 영업양도 시 개인정보 이전 제한(법 제27조), 유출통지(법 제34조), 개인정보 처리정지권(법 제37조) 적용 제외
- 동창회, 동호회 등 친목도모 단체의 개인정보 처리는 개인정보 수집이용(법 제15조), 개인정보 처리방침(법 제30조), 개인정보 보호책임자 지정(법 제31조) 적용 제외

③ 개인정보 처리단계별 의무사항

<처리단계>

수집
이용

저장
관리

제공
위탁

파기

권리
보장

벌칙 및 경과조치

개인정보보호법령 규정

개인정보 수집 · 이용
개인정보 수집의 제한 (필요 최소한의 정보수집 등)
민감정보 및 고유식별정보 처리제한

인터넷상 주민번호 이외의 회원가입 방법 제공
영상정보처리기기 설치 · 운영, 개인정보처리방침 공개
개인정보보호책임자 지정
개인정보 안전성 확보조치

개인정보의 제3자 제공, 목적외 이용제공 금지
개인정보 처리위탁, 영업양도 등 개인정보 이전

개인정보 파기

개인정보 유출통지 · 신고 및 개인정보 침해신고
개인정보 열람, 정정 · 삭제, 처리정지권
분쟁조정위원회 및 집단분쟁조정
권리침해 중지 단체소송

④ 개인정보 수집 · 이용 및 제한

개인정보를 수집 · 이용할 수 있는 경우 (법 제15조)

1. 정보주체의 동의를 받은 경우
2. 법률의 특별한 규정, 법령상 의무 준수를 위해 불가피한 경우
3. 공공기관이 법령에서 정한 소관업무 수행을 위해 불가피한 경우
4. 정보주체와의 계약 체결·이행을 위해 불가피한 경우
5. 정보주체 등의 생명, 신체, 재산의 이익 보호 (사전동의 받기 곤란한 경우)
6. 개인정보처리자의 정당한 이익 달성을 위해 필요한 경우

처벌규정 위반 시 5천만원 이하의 과태료

필요 최소한의 개인정보 수집 (법 제16조)

- 개인정보처리자는 수집목적에 필요한 **최소한의 개인정보**를 수집
- 최소한의 개인정보 수집이라는 **입증책임**은 개인정보처리자가 부담
- 개인정보처리자는 정보주체가 필요 최소한의 정보 외의 개인정보 수집에 동의하지 않는다는 이유로 정보주체에게 **재화 또는 서비스의 제공을 거부 금지**

처벌규정 위반 시 3천만원 이하의 과태료

⑤ 민감정보 및 고유식별정보 처리제한

내용

- 민감정보 및 고유식별정보의 처리는 원칙적으로 금지 (법 제23조, 제24조)
- 정보주체에게 별도 동의를 얻거나, 법령에서 구체적으로 허용된 경우에 한하여 예외적으로 처리 허용

※ 민감정보 : 사상, 신념, 노동조합, 정당가입, 건강 등 사생활 침해 우려가 현저히 높은 개인정보

※ 고유식별정보 : 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보

세부사항

- 민감정보의 범위 (영 제18조)
 - ① 유전자 검사에 따른 유전정보
 - ② ‘형의 실효 등에 관한 법률’에 따른 범죄 경력 정보
- 고유식별정보의 범위 (영 제19조)
 - ① 주민등록번호 (「주민등록법」 제7조제3항) ② 여권번호 (「여권법」 제7조제1항제1호)
 - ③ 운전면허번호 (「도로교통법」 제80조) ④ 외국인등록번호 (「출입국관리법」 제31조제4항)

처벌규정

위반 시 5년 이하의 징역 또는 5천만원 이하의 벌금

⑥ 개인정보 수집 · 이용 · 제3자 제공 기준

개인정보 수집·이용

1. 정보주체의 **동의**를 받은 경우
2. **법률의 특별한 규정, 법령상 의무 준수**를 위해 불가피한 경우
3. 공공기관이 법령에서 정한 소관 소관업무를 위해 불가피한 경우
4. 정보주체와의 계약 체결이행에 불가피한 경우
5. 정보주체등의 생명, 신체, 재산의 이익 보호
6. 개인정보처리자의 정당한 이익 달성을 위해 필요한 경우

처벌규정

위반 시 5천만원 이하의 과태료

개인정보 제공

1. 정보주체의 **동의**를 받은 경우
 2. **법률의 특별한 규정, 법령상 의무 준수**를 위해 불가피한 경우
 3. 공공기관이 법령에서 정한 소관 소관업무를 위해 불가피한 경우
 5. 정보주체등의 생명, 신체, 재산의 이익 보호
- 수집 목적과 같은 범위에서 제3자에 제공(상조 보증 등)**

처벌규정

위반 시 5년 이하의 징역 또는 5천만원 이하의 벌금

목적외 이용·제공

1. 정보주체의 **별도 동의**를 받은 경우
2. 다른 **법률의 특별한 규정**
3. 명백히 정보주체 또는 제3자의 생명, 신체, 재산의 이익에 필요한 경우
4. 통계작성 및 학술연구 목적에 필요한 경우로 특정개인을 알아볼 수 없는 형태로 제공하는 경우

< 공공기관만 해당 >

5. 개인정보를 목적외로 이용하거나 제3자에게 제공하지 않으면 다른 법률에서 정하는 소관업무 수행 불가한 경우로 보호위원회의 심의·의결을 거친 경우
6. 조약, 국제협정 이행을 위해 외국정부 등 제공에 필요한 경우
7. 범죄수사 및 공소제기·유지
8. 법원의 재판업무 수행
9. 형 및 감호, 보호처분 집행

처벌규정

위반 시 5년 이하의 징역 또는 5천만원 이하의 벌금

※ 개인정보 수집·이용은 폭넓게 인정하되, 제공, 목적외 이용·제공 기준은 요건을 엄격히 규정하여 차등화

⑦ 개인정보 수집 · 이용 · 제공에 따른 동의

최소 수집

필수정보, 선택정보

서비스 거부금지

- 서비스 제공에 필요한 최소정보(필수정보) 수집
 ➔ 수집하는 개인정보가 최소정보라는 것은 개인정보처리자가 입증해야 함
- 선택정보 미동의로 재화나 서비스 거부 금지

일반 동의

수집 · 이용 동의

제3자 제공 동의

국외의 제3자 제공동의

14세미만 법정대리인 동의

- 개인정보 수집 · 이용 동의
- 수집목적내 제3자 제공동의
- 개인정보 국외이전시 제공 동의
- 만 14세 미만 아동의 개인정보 수집 시
- 법정 대리인의 동의 필요

별도 동의

목적 외 이용 · 제공 동의

민감정보 처리 동의

고유식별정보 처리 동의

- 수집 목적 외 이용 및 제3자 제공 시 정보주체의 별도 동의 필요
- 민감정보 및 주민번호 등 고유식별정보 처리 시 정보주체의 별도 동의 필요

<참고> 개인정보 동의획득 양식 (예시)

A사의 개인정보 수집 및 이용

회사는 회원가입, 고객상담, 서비스 제공을 위해 최초 회원가입 시 아래와 같은 개인정보를 수집하고 있습니다.

<필수정보> 성명, 생년월일, 성별, 아이디, 비밀번호, 필수연락처, 가입인증정보

수집한 개인정보는 회원 유지기간 및 A/S 기간동안 보관합니다.

회원께서는 개인정보 수집 동의를 거부하실 수 있으며 다만 이 경우 회원가입이 제한됩니다.

개인정보 수집 및 이용에 동의하십니까

☐ 동의함

☐ 동의하지 않음

일반동의

(필요시) 고유식별정보 처리 동의 (수집 또는 제공시의 고지사항 고지)

고유식별정보 처리에 동의하십니까

☐ 동의함

☐ 동의하지 않음

별도동의

(필요시) 민감정보 처리 동의 (수집 또는 제공시의 고지사항 고지)

민감정보 처리에 동의하십니까

☐ 동의함

☐ 동의하지 않음

별도동의

(필요시) 목적 외 제공 동의시 (목적 외 제공시의 고지사항 고지)

개인정보 목적외 이용에 동의하십니까

☐ 동의함

☐ 동의하지 않음

별도동의

<선택정보> 기혼 여부, 기념일, 병력, 취미, 소득수준, 자녀 정보

※ 선택정보 사항을 획득하지 못한 사유로 인해 서비스 제공을 거부할 수 있습니다.

선택적 개인정보 수집 및 이용에 동의하십니까

☐ 동의함

☐ 동의하지 않음

별도동의

⑧ 영상정보처리기기의 설치·운영 제한 - 1

내용

- 영상정보처리기기는 공개된 장소에 특정 목적으로만 설치·운영 (법 제25조제1항)

<영상정보처리기기 설치·운영 허용 사유>

- 1) 법령에서 구체적으로 허용하는 경우 2) 범죄예방 및 수사 3) 시설안전 및 화재예방
- 4) 교통단속 5) 교통정보의 수집·분석 및 제공

처벌규정 위반 시 3천만원 이하의 과태료

- 목욕실, 화장실, 탈의실 등 개인 사생활을 현저히 침해할 우려가 있는 장소에는 영상정보처리기기 설치·운영 금지 (법 제25조제2항)
 - 다만, 교정시설, 정신의료기관에는 설치·운영 허용 (영 제22조제1항)

처벌규정 위반 시 5천만원 이하의 과태료

- 영상정보처리기기 설치목적과 다른 목적으로 영상정보처리기기를 임의 조작, 다른 곳을 비추는 행위, 녹음기능 사용 금지 (법 제25조제5항)

처벌규정 위반 시 3천만원 이하 징역 또는 3천만원 이하 벌금

⑧ 영상정보처리기기의 설치 · 운영 제한 - 2

안내판 설치

- 정보주체가 쉽게 인식할 수 있도록 안내판 설치 (법 제25조제4항, 영 제24조)

<안내판 기재사항>

- 1) 설치목적 및 장소 2) 촬영범위 및 시간 3) 관리책임자 및 연락처

- 건물 안에 다수의 영상정보처리기기 설치시, 출입구 등 잘 보이는 곳에 해당 시설·장소 전체가 설치지역임을 표시하는 안내판 설치
- 다음의 경우, 안내판 설치에 갈음하여 인터넷 홈페이지에 기재사항 게재

<안내판 설치 예외>

- 1) 공공기관이 원거리 촬영, 과속, 신호위반단속 등 목적으로 설치하는 경우
- 2) 장소적 특성으로 안내판 설치가 불가능하거나 설치하더라도 정보주체가 쉽게 알아볼 수 없는 경우

처벌규정 위반 시 1천만원 이하의 과태료

영상정보처리기기 운영관리방침 수립

<운영관리방침 포함사항 (영 제25조)> ※ 개인정보 처리방침으로 대체 가능

- 1) 설치근거 및 설치목적 2) 설치대수, 설치위치, 촬영범위 3) 관리책임자, 담당부서 등
- 4) 촬영시간, 보관기간, 보관장소, 처리방법 5) 운영자의 영상정보 확인방법 및 장소
- 6) 정보주체의 영상정보 열람 등 요구에 대한 조치 7) 기술적,관리적,물리적 조치 등

⑨ 개인정보의 안전성 확보조치

내용

- 개인정보가 분실·도난·유출·변조·훼손되지 않도록 안전성 확보에 필요한 기술적·관리적·물리적 조치 이행 (법 제29조)

세부사항 (영 제30조)

- 관리적 보호조치
 - 내부관리계획 수립·시행
- 기술적 보호조치
 - 접근통제 및 접근권한 제한 조치
 - 개인정보의 안전한 저장·전송을 위한 암호화 또는 이에 상응하는 조치
 - 접속기록의 보관 및 위·변조 방지조치
 - 보안프로그램의 설치 및 갱신조치
- 물리적 보호조치
 - 개인정보 안전한 보관을 위한 보관시설 마련 또는 잠금장치 설치

처벌규정

미이행시 3천만원 이하의 과태료, 미이행으로 인한 유출시 2년 이하 징역 또는 1천만원 이하 벌금

<참고> 개인정보의 안전성 확보조치 고시(안)

※ 소상공인(5인 미만) 또는 중소기업자(50인 미만)가 내부직원의 개인정보망을 보유한 시스템은 적용 제외

구분	주요내용
내부관리계획(제3조)	<ul style="list-style-type: none"> • 보호책임자 지정 및 역할과 책임, 취급자 교육 등 ※ 소상공인은 내부관리계획 수립의무 면제
접근권한 관리(제4조)	<ul style="list-style-type: none"> • 업무수행에 필요한 최소한의 범위로 차등 부여 • 접근권한 부여기록은 최소 3년간 보관
비밀번호 관리(제5조)	<ul style="list-style-type: none"> • 비밀번호 작성규칙 수립 의무화
접근통제시스템(제6조)	<ul style="list-style-type: none"> • 방화벽 등 접근통제시스템 설치·운영 • 업무용 컴퓨터만을 이용해 개인정보 처리시, 접근통제시스템 설치의무 면제 (O/S, 보안프로그램의 접근통제기능 이용)
암호화(제7조)	<ul style="list-style-type: none"> • 암호화 대상 : 고유식별정보, 비밀번호, 바이오정보 • 암호화 기준 <ul style="list-style-type: none"> -(전송시) 정보통신망 송수신 등의 경우 암호화 -(저장시) ① 비밀번호 및 바이오정보 암호화 (비밀번호 일방향 암호화) ② 고유식별정보는 인터넷구간, DMZ구간 저장시 암호화하고 내부망 저장시 위험도 분석에 따라 암호화 적용여부, 적용범위 결정
접속기록 보관(제8조)	<ul style="list-style-type: none"> • 최소 6개월 이상 보관
보안프로그램(제9조)	<ul style="list-style-type: none"> • 백신소프트웨어 등 보안프로그램 설치, 자동 또는 일1회 이상 업데이트
물리적 접근방지(제10조)	<ul style="list-style-type: none"> • 개인정보 물리적 보관장소에 대한 출입통제절차 등

※ 안전성 확보조치 고시(안)은 개인정보보호 종합포털(www.privacy.go.kr) 게재

⑩ 개인정보 파기조치

내용

☺ 보유기간의 경과, 개인정보 처리목적 달성 등 개인정보가 불필요하게 되었을 때는 지체 없이 (5일 이내) 개인정보 파기 (법 제21조, 표준지침 제11조)

☺ 다만, 다른 법령에 따라 보존해야 하는 경우에는 미파기

- 소비자 분쟁처리 관련 기록(3년), 요금정산(5년), 계약 및 청약철회(5년) : 전자상거래법
- 의료기록부(10년), 진단서 등의 부분(3년) : 의료법 시행규칙

<법에 따른 보존시 일반 회원정보와 별도로 보관하여 잘못 처리되는 일이 없도록 특히 유의>

파기방법 (영 제 16조)

☺ 개인정보가 복구 또는 재생되지 아니하도록 파기

- 전자적 파일 형태 : 복원이 불가능한 방법으로 영구 삭제

※ 복원이 불가능한 방법 : 사회 통념상 현재 기술 수준에서 적절한 비용이 소요되는 방법 (표준지침 제11조제2항)

- 기록물, 인쇄물, 서면 등 : 파쇄 또는 소각

처벌규정

위반 시 3천만원 이하의 과태료

⑪ 정보주체의 열람, 정정·삭제, 처리정지권 보장

내용

- ☞ 정보주체는 자신의 개인정보에 대한 열람, 정정·삭제, 처리정지를 개인정보처리자에 대해 요구할 수 있음 (법 제35조~제37조)

조치사항

- ☞ 개인정보 열람 요구 대응조치 (영 제41조)
 - 내용적으로 10일 이내에 열람할 수 있도록 조치,
 - 열람할 수 없는 정당한 사유가 있을 경우 정보주체에게 그 사유를 알리고 열람 연기 (사유가 소멸하면 지체없이 열람)
- ☞ 개인정보 정정·삭제, 처리정지 요구 대응조치 (영 제43조)
 - 내용적으로 10일 이내에 조치

※ 정보주체 본인이나 위임을 받은 사람에게만 열람하여야 함

(홈쇼핑에서 이름, 주민번호만 확인하고 주소, 전화번호, 거래내역 등 추가 정보를 제공하여 불법 악용된 사례)

<열람 제한사유>

- 1) 법률의 규정
- 2) 타인의 생명, 신체, 재산 침해우려가 있는 경우
- 3) 공공기관의 조세부과 징수·환급, 교육기관 성적평가·입학자 선발, 채용 시험·보상금 산정·감사조사 업무

처벌규정

위반 시 3천만원 이하의 과태료

⑫ 개인정보 처리방침 수립 및 공개

내용

- 개인정보처리자는 개인정보처리방침을 수립·공개(법 제30조제1항, 영 제31조제1항)

<개인정보처리방침 포함사항>

- 1) 개인정보 처리목적
- 2) 개인정보 처리 및 보유기간
- 3) 개인정보 제3자 제공에 관한 사항
- 4) 개인정보 처리 위탁에 관한 사항
- 5) 정보주체의 권리·의무 및 행사방법에 관한 사항
- 6) 처리하는 개인정보항목
- 7) 개인정보 파기에 관한 사항
- 8) 개인정보 안전성 확보조치에 관한 사항

개인정보처리방침 공개방법

- 인터넷 홈페이지 첫화면 또는 첫화면과 직접 연결되는 화면에 게재

<인터넷 홈페이지 게재 불가시 공개방법 (영 제31조제3항)>

- 1) 사업장 등의 보기 쉬운 장소에 게시
- 2) 관보, 신문 게재
- 3) 연 2회 이상 발생하는 간행물, 소식지 등에 게재
- 4) 재화용역을 제공하기 위해 작성한 계약서에 게재하여 발급

처벌규정

위반 시 1천만원 이하의 과태료

<참고> 개인정보 처리방침 예시(병원 약식)

【 개인정보처리방침 】

_____병원(이하 병원 이라 함) 귀하의 개인정보보호를 매우 중요시하며, 『개인정보보호법』을 준수하고 있습니다. 병원은 개인정보처리방침을 통하여 귀하께서 제공하시는 개인정보가 어떠한 용도와 방식으로 이용되고 있으며 개인정보보호를 위해 어떠한 조치가 취해지고 있는지 알려드립니다.

이 개인정보처리방침의 순서는 다음과 같습니다.

- | | |
|----------------------------------|-------------------|
| 1. 수집하는 개인정보의 항목 및 수집방법 | |
| 2. 개인정보의 수집 및 이용목적 | |
| 3. 개인정보의 보유 및 이용기간 및 파기절차 및 파기방법 | |
| 4. 이용자 및 법정대리인의 권리와 그 행사방법 | |
| 5. 개인정보의 제공 및 공유 | 6. 개인정보의 위탁 |
| 7. 개인정보 보호책임자 | 8. 개인정보의 안전성 확보조치 |
| 9. 정책 변경에 따른 공지방법 | |

1. 수집하는 개인정보의 항목 및 수집방법

병원은 진료를 위해 **의료법에 의해 명시된 최소한의 개인정보만을** 수집합니다. 귀하가 병원의 진료 서비스를 이용하기 위해 작성하는 진료카드와 진료결과에 대한 기록을 관리합니다.

- 수집항목 : 성명, 주민등록번호, 주소, 연락처, 진료기록
- 수집방법 : 방문시 서면 또는 면담을 통해 수집

※ **의료법에 의해 고유식별정보 및 진료정보를 의무적으로 보유하여야 하여야 함(동의 불필요)**

2. 개인정보의 수집 및 이용목적

병원은 수집한 개인정보를 진료의 목적으로만 사용하며 이용 목적이 변경될 시에는 사전 동의를 구할 것입니다.

3. 개인정보의 보유 및 이용기간 및 파기절차 및 파기방법

병원은 의료법에서 정한 보유기간 동안 개인정보를 보유하며 그 이후에는 개인정보를 지체 없이 파기합니다.

- 보유기간 : 진료기록부 10년
- 파기절차 : 법정 보유기간 후 파기방법에 의하여 즉시 파기
- ※ 진료기록이 최종 기록된 후 10년이 경과한 해당 개인정보는 즉시 파기하여야 함
- 파기방법 : 전자적 파일형태로 저장된 개인정보는 기록을 재생할 수 없는 기술적 방법을 사용하여 삭제, 종이에 출력된 개인정보는 분쇄기로 분쇄하거나 소각

4. 이용자 및 법정대리인의 권리와 그 행사방법

이용자 및 법정대리인은 개인정보와 관련하여 인터넷, 전화, 서면 등을 이용하여 병원에 개인정보 열람 등의 권리를 행사할 수 있으며, 병원은 지체 없이 필요한 조치를 합니다.

※ 법에 의해 보관이 의무화된 개인정보는 요청이 있더라도 보관기간내에 수정·삭제할 수 없습니다.

5. 개인정보의 제3자 제공

병원은 국민건강보험법에 의거 건강보험심사평가원에 요양급여비용 청구를 위해 진료 기록을 제출합니다.

※ **법에 의해 의무적으로 제출하는 사항이므로 별도의 제공 동의 불필요**

6. 개인정보 처리의 위탁

병원은 개인정보관리시스템의 관리를 위해 다음 회사에 개인정보를 위탁하고 있습니다.

- 시스템 운영 및 유지보수 : _____(연락처 _____)

7. 개인정보 보호책임자

이름	직위	전화번호	메일
	원 장		

8. 개인정보의 안전성 확보조치

병원은 이용자의 개인정보보호를 위한 기술적 대책으로서 여러 보안장치를 마련하고 있습니다. 이용자께서 제공하신 모든 정보는 방화벽 등 보안장비에 의해 안전하게 보호/관리되고 있습니다.

또한 병원은 이용자의 개인정보보호를 위한 관리적 대책으로서 이용자의 개인정보에 대한 접근 및 관리에 필요한 절차를 마련하고, 이용자의 개인정보를 처리하는 인원을 최소한으로 제한하여 지속적인 보안교육을 실시하고 있습니다. 또한 개인정보 처리자에게 비밀번호를 부여하고 이를 정기적으로 갱신하겠습니다.

9. 정책 변경에 따른 공지방법

개인정보처리방침은 _____년 _____월 _____일에 제정되었으며 법령·정책 또는 보안 기술의 변경에 따라 내용의 추가·삭제 및 수정이 있을 시에는 변경되는 개인정보처리방침은 시행하기 최소 7일전에 병원 홈페이지를 통해 변경이유 및 내용 등을 공지하도록 하겠습니다.

공고일자 : _____년 _____월 _____일 / 시행일자 : _____년 _____월 _____일

www.privacy.go.kr에서 자동생성 기능을 이용하여 생성할 수 있음
본 예시는 병원에서 사용하는 오프라인용 서식임

<개인정보 처리방침 개선 예시>

개인정보 처리방침

제1조 (개인정보의 처리 목적)

당사는 개인정보를 다음의 목적을 위해 처리합니다. 처리한 개인정보는 다음의 목적이외의 용도로는 사용되지 않으며 이용 목적이 변경될 시에는 사전동의를 구할 예정입니다.

① 서비스 제공

콘텐츠 제공, 구매 및 요금 결제, 물품배송 또는 청구서 등 발송, 본인인증(금융거래, 금융서비스), 요금추심 등

② 회원 가입 및 관리

회원제 서비스 이용에 따른 본인확인, 개인 식별, 불량회원의 부정이용 방지와 비인가 사용방지, 가입의사 확인, 연령확인, 만14세 미만 아동 개인정보 수집 시 법정대리인 동의 여부 확인, 분쟁 조정을 위한 기록 보존, 불만처리 등 민원처리, 고지사항 전달 등

③ 마케팅 및 광고에의 활용

신규 서비스(제품) 개발 및 맞춤 서비스 제공, 이용자의 광고접촉 관리, 고객 만족도 조사, 서비스 개선, 신규 서비스 개발 및 맞춤 서비스 제공, 인구통계학적 특성에 따른 서비스 제공 및 광고 게재, 서비스의 유효성 확인, 접속 빈도 파악 또는 회원의 서비스 이용에 대한 통계

제2조 (처리하는 개인정보의 항목)

당사는 회원가입, 각종 서비스 제공을 위해 처리하는 개인정보의 항목 및 수집 방법은 다음과 같습니다.

① 개인정보 파일명 : 서비스 제공 및 회원관리

② 개인정보 항목

- 필수정보 : ID, 성명, 비밀번호, 생년월일, 자택주소, 전화번호, 성별
- 선택정보 : 휴대전화번호, 이메일, 회사명, 직책, 회사전화번호, 직업, 신체정보, 주민등록번호, 은행계좌정보, 신용카드정보, 접속 IP 정보, 쿠키, 서비스 이용 기록, 결제기록, 접속 로그, 법정대리인 휴대전화번호, 법정대리인 자택 주소, 법정대리인 이름, 법정대리인 자택 전화번호

③ 수집방법 : 홈페이지, 서면, 전화/팩스, 경품행사, 배송요청, 제휴사로부터 제공 받음, 생성정보 수집 등을 통한 수집

<처리목적>

- 수집할 때 동의를 구한 목적범위를 명확히 명시하여야 함
- 동의받은 범위를 벗어날 경우 목적외 이용에 해당
- 수집목적도 꼭 필요한 최소한으로 한정

본 처리방침 예시는 특정 업체에서 사용하는 서식으로 표준이 아님
잘못된 점을 지적하고 개선하기 위한 예시임

<개인정보 항목>

- 필수정보와 선택정보를 구분하여 관리
- 주민등록번호는 원칙적으로 사용을 금지
- 선택정보라도 불필요한 정보는 최대한 수집하지 않아야 함 (회사명, IP, 카드정보, 신체정보 등 정보는 축소를 검토)
- 관리하는 개인정보 파일별로 모두 나열하여 작성

<개인정보 처리방침 개선 예시>

제3조 (개인정보의 처리 및 보유 기간)

이용자 개인정보는 원칙적으로 개인정보의 처리목적이 달성되면 지체없이 파기합니다. 단, 다음의 정보에 대하여는 아래의 사유로 명시한 기간 동안 별도로 보존합니다.

① 개인정보 파일명 : 서비스 제공 및 회원관리

1. 개인정보 항목 : ID, 성명, 비밀번호, 성명, 생년월일, 자택주소, 전화번호, 성별, 휴대전화번호, 이메일, 회사명, 직책, 회사전화번호, 직업, 신체정보, 주민등록번호, 은행계좌정보, 신용카드정보, 접속 IP 정보, 쿠키, 서비스 이용 기록, 결제기록, 접속 로그, 법정대리인 휴대전화번호, 법정대리인 자택 주소, 법정대리인 이름, 법정대리인 자택 전화번호
2. 보유근거 및 기간
 - 가. 계약 또는 청약철회 등에 관한 기록 : 5년 (전자상거래에서의 소비자보호에 관한 법률)
 - 나. 대금결제 및 재화 등의 공급에 관한 기록 : 5년 (전자상거래에서의 소비자보호에 관한 법률)

제4조 (개인정보의 제3자 제공)

당사는 원칙적으로 이용자의 개인정보를 제1조 (개인정보의 처리 목적)에서 명시한 범위 내에서 처리하며, 이용자의 사전 동의 없이는 본래의 범위를 초과하여 처리하거나 제3자에게 제공하지 않습니다.

단, 다음의 경우는 할부거래에 관한 법률 제27조에 따라 다음과 같은 기관 및 자에게 개인정보를 제공하고 있으며, 제공 목적 및 범위는 다음과 같습니다.

1. OOOO(소비자피해보상보험사)

개인정보 파일명	서비스 제공 및 회원관리
개인정보 제공항목	이름, 주민등록번호, 자택전화번호, 휴대전화번호, 성별, 자택주소, 우편번호, 이메일, 증서번호(소비자계약번호), 계약일자, 계약만기일자, 월납입예정일, 최종납입일, 총계약금액, 월납입계약금액, 기납입금액, 총납입회차, 기납입회차, 상품명, 계약 형태 여부(신규가입, 해약 등), 은행계좌정보, 서비스 이용 기록
개인정보 제공목적	미성년자일 경우 법정대리인 휴대전화번호, 법정대리인 자택 주소, 법정대리인 이름, 법정대리인 자택 전화번호, 법정대리인 주민등록번호
개인정보 제공근거	할부거래에 관한 법률 제27조에 따른 소비자피해보상 보장

<보유기간>

- 처리목적이 달성되면 지체없이 파기하여야 함
- 가급적 보유기간을 명확히 명시
- 회원탈퇴 등 파기사유 발생시에도 다른 법률에 따라 계속 보관하는 경우 별도로 보관하여야 함

<제3자 제공>

- 법률의 근거가 있는 경우 동의 없이 제3자 제공 가능
- 단, 법률에 명시된 업무로만 사용하여야 함
- 법률의 근거가 없는 경우는 별도 동의 필요
- 재판, 수사 등 다른 법률에 의해 불규칙하게 제공되는 경우는 명시하지 않아도 됨

<개인정보 처리방침 개선 예시>

제5조 (개인정보처리 위탁) ↓

당사는 원칙적으로 이용자의 동의없이 해당 개인정보의 처리를 타인에게 위탁하지 않습니다. 다만, 이용자의 동의를 받아 당사가 현재 개인정보 처리를 위탁하는 사항은 다음과 같습니다. ↓

1. 우체국 ↓

위탁업무 내용 ↓	소비자 보증 증서(소비자피해보상증서) 발송, 물품배송 또는 청구서 등 발송, 요금추심, 불만처리 등 민원처리, 고지사항 전달, 이벤트 및 광고성 정보 제공 및 참여기회 제공, 신규 서비스(제품) 개발 및 맞춤 서비스 제공, 소비자피해보상증서 발송 ↓
위탁기간 ↓	개인정보 제공 동의 시부터 동의 철회 또는 계약 해제 시까지 ↓

1-1. 000000 ↓

위탁업무 내용 ↓	소비자피해보상증서 제작 ↓
위탁기간 ↓	개인정보 제공 동의 시부터 동의 철회 또는 계약 해제 시까지 ↓

2. 00업체 ↓

수탁업체 ↓	00업체 ↓
위탁업무 내용 ↓	당사 전산 관리 ↓
위탁기간 ↓	개인정보 제공 동의 시부터 동의 철회 또는 계약 해제 시까지 ↓

제6조 (정보주체의 권리, 의무 및 그 행사방법) ↓

이용자는 개인정보주체로서 다음과 같은 권리를 행사할 수 있습니다. ↓

1. 자신 및 14세 미만 아동의 개인정보의 조회, 수정 및 가입해지의 요청 ↓
2. 개인정보의 오류에 대한 정정 및 삭제의 요청 ↓
3. 개인정보의 조회, 수정 및 해지, 삭제 등의 요청은 '개인정보변경/회원정보수정 및 가입해지/회원탈퇴/동의철회' 등을 클릭하여 본인 확인 절차를 거친 후 직접 열람, 정정, 혹은 탈퇴가 가능합니다. ⇒ 온라인 회원 가입을 하는 회원사는 적용 ↓
4. 이용자가 개인정보의 오류에 대한 정정 및 삭제를 요청한 경우에는 정정 및 삭제를 완료할 때까지 당해 개인정보를 이용 또는 제공하지 않습니다. 이 경우, 잘못된 개인정보를 이용 또는 제공한 경우 지체없이 수정하겠습니다. ↓
5. 당사는 이용자의 요청에 의해 해지 또는 삭제되는 개인정보는 제3조 개인정보의 처리 및 보유 기간에 따라 처리합니다. ↓

<위탁>

- 위탁은 정보주체에게 반드시 고지하여야 하는 사항임
- 위탁내용과 위탁업체에 대한 내용을 명시
- 개인정보처리자를 대신하여 개인정보를 처리하는 경우 모두 위탁에 해당함
(별도 소속의 모집인도 위탁계약에 의한 수탁자가 될 수 있음)
- 위탁계약을 통해 책임을 명확히 하여야 하며 수탁자의 개인정보처리를 철저히 관리하여야 함

<권리 행사방법>

- 열람, 정정, 삭제, 처리정지권에 대한 안내

<개인정보 처리방침 개선 예시>

제7조 (개인정보의 파기)↓

당사는 원칙적으로 개인정보 처리목적이 달성된 경우에는 지체없이 해당 개인정보를 파기합니다. 다만, 다른 법률에 따라 보존하여야 하는 경우에는 그러하지 않습니다. 파기의 절차, 기한 및 방법은 다음과 같습니다. ↓

↓

① 파기절차 ↓

이용자가 입력한 정보는 목적 달성 후 별도의 DB에 옮겨져(종이의 경우 별도의 서류) 내부 방침 및 기타 관련 법령에 따라 일정기간 저장된 후 혹은 즉시 파기됩니다. 이 때, DB로 옮겨진 개인정보는 법률에 의한 경우가 아니고서는 다른 목적으로 이용되지 않습니다. ↓

↓

② 파기기한 ↓

이용자의 개인정보는 개인정보의 보유기간이 경과된 경우에는 보유기간의 종료일로부터 5일 이내에, 개인정보의 처리 목적 달성, 해당 서비스의 폐지, 사업의 종료 등 그 개인정보가 불필요하게 되었을 때에는 개인정보의 처리가 불필요한 것으로 인정되는 날로부터 5일 이내에 그 개인정보를 파기합니다. ↓

↓

③ 파기방법 ↓

1. 전자적 파일 형태의 정보는 기록을 재생할 수 없는 기술적 방법을 사용합니다. ↓
2. 종이에 출력된 개인정보는 분쇄기로 분쇄하거나 소각을 통하여 파기합니다. ↓

↓

제8조 (개인정보관리책임자 및 담당자의 연락처)↓

당사는 개인정보를 보호하고 개인정보와 관련한 불만을 처리하기 위하여 아래와 같이 개인정보 보호책임자 및 실무담당자를 지정하고 있습니다. (개인정보보호법 제31조 제1항에 따른 개인정보 보호책임자) ↓

↓

개인정보 보호책임자↓		개인정보 보호담당자↓	
이름↓	○○○↓	이름↓	□□□↓
담당부서↓	○○팀↓	담당부서↓	□□팀↓
연락처↓	000) 0000-0000↓	연락처↓	***) ****-****↓
이메일↓	aaaa@aaaaa.com↓	이메일↓	bbbb@bbbbbb.com↓

<파 기>

-파기 절차와 방법을 간략히 명시함

(처리방침은 공개가 필요한 사항들을 정보주체에게 알리는 문서이므로 회사내부적인 자세한 기술적 절차는 내부관리계획으로 작성하여 보관)

<개인정보관리책임자>

-최소한 개인정보관리책임자의 성명, 직위, 연락처 명시 필요

<개인정보 처리방침 개선 예시>

제9조 (개인정보의 안전성 확보 조치) ↓

당사는 「개인정보보호법」 제29조에 따라 다음과 같이 안전성 확보에 필요한 기술적, 관리적, 물리적 조치를 하고 있습니다. ↓

↓

① 내부관리계획의 수립 및 시행 ↓

공제조합의 내부관리계획 수립 및 시행은 행정안전부의 내부관리 지침을 준수하여 시행합니다. ↓

② 정기적인 자체 감사 실시 ↓

개인정보 취급 관련 안정성 확보를 위해 정기적(분기 1회)으로 자체 감사를 실시하고 있습니다. ↓

③ 개인정보 취급 담당자의 최소화 및 교육 ↓

개인정보를 취급하는 담당자를 지정하고 최소화하여 개인정보를 관리하는 대책을 시행하고 있습니다. ↓

④ 개인정보에 대한 접근 제한 ↓

개인정보를 처리하는 데이터베이스시스템에 대한 접근권한의 부여, 변경, 말소를 통하여 개인정보에 대한 접근통제를 위하여 필요한 조치를 하고 있으며 침입차단시스템을 이용하여 외부로부터의 무단 접근을 통제하고 있습니다. ↓

⑤ 접속기록의 보관 및 위변조 방지 ↓

개인정보처리시스템에 접속한 기록(웹 로그, 요약정보 등)을 최소 6개월 이상 보관, 관리하고 있으며, 접속 기록이 위변조 및 도난, 분실되지 않도록 보안기능을 사용하고 있습니다. ↓

⑥ 개인정보의 암호화 ↓

이용자의 개인정보 및 비밀번호는 암호화 되어 저장 및 관리되고 있습니다. 그러므로 비밀번호는 본인만 알 수 있으며, 중요한 데이터는 저장 및 전송 시 암호화하거나 파일 잠금기능을 사용하는 등의 별도 보안기능을 사용하고 있습니다. ↓

⑦ 해킹 등에 대비한 기술적 대책 ↓

공제조합은 해킹이나 컴퓨터 바이러스 등에 의한 개인정보 유출 및 훼손을 막기 위하여 보안프로그램을 설치하고 주기적인 갱신·점검을 하며 외부로부터 접근이 통제된 구역에 시스템을 설치하고 기술적/물리적으로 감시 및 차단하고 있습니다. 또한 네트워크 트래픽의 통제(Monitoring)는 물론 불법적으로 정보를 변경하는 등의 시도를 탐지하고 있습니다. ↓

⑧ 비인가자에 대한 출입 통제 ↓

개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 이에 대해 출입통제 절차를 수립, 운영하고 있습니다. ↓

⑨ 문서보안을 위한 잠금장치 사용 ↓

개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하고 있습니다. ↓

<안전성 확보조치에 관한 사항>

-개인정보를 안전하게 관리하기 위해 필수적인 안전성 확보조치를 시행하고 있음을 정보주체에게 알림

(처리방침은 공개가 필요한 사항들을 정보주체에게 알리는 문서이므로 회사내부적인 자세한 기술적 절차는 내부관리계획으로 작성하여 보관)

-내부관리계획은 처리방침의 내용에 구체적인 안전성 확보 조치내용과 업무절차, 개인정보책임자, 취급자 등의 책임과 역할 등 회사내에서만 사용하는 내용들을 추가하여 수립

(내부관리방침은 내부적으로 수립하여 운영하고 공개 의무는 없음)

<개인정보 처리방침 개선 예시>

제10조 (영상정보처리기기 운영·관리 방침) ↓

당사는 다음과 같이 영상정보처리기기를 운영·관리하고 있습니다. ↓

1. 설치 목적 : 범죄예방 ↓

2. 개인정보상정보 보호책임자 및 영상정보에 대한 접근 권한자 : 제8조의 개인정보 보호책임자 ↓

3. 영상정보 설치 및 관리 사항 ↓

↓ 설치대수 ↓	4대 ↓
↓ 설치위치 ↓	당사 사무실 입구 및 내부 ↓
↓ 촬영범위 ↓	설치 7m 이내 지역, 각도 : 최대 120° ↓
↓ 촬영시간 ↓	24시간 ↓
↓ 보관기간 ↓	최대 1년 ↓
↓ 보관장소 ↓	당사 서버실 내 CCTV 하드디스크 ↓
↓ 처리방법 ↓	도난 및 보안 사고 발생 시 활용 ↓
↓ 영상정보 확인 방법 ↓	영상 재생 ↓
↓ 영상정보 확인 장소 ↓	당사 사무실 ↓

제11조 (개인정보 처리방침의 변경) ↓

이 개인정보처리방침은 시행일로부터 적용되며, 법령 및 방침에 따른 변경내용의 추가, 삭제 및 정정이 있는 경우에는 가능한 변경사항의 시행 7일 전부터 공지사항을 통하여 고지할 것입니다. ↓

공고일자 : 2011년 00월 00일 ↓

시행일자 : 2011년 00월 00일 ↓

↓

↓

<영상정보처리기기에 관한 사항>

-영상정보처리기기 운영시 별도 관리방침을 수립하거나 다른 개인정보처리방침에 포함하여 수립, 공개

-설치대수, 목적, 위치, 촬영범위, 촬영시간, 보관기간, 책임자 연락처, 처리방법 등을 명시

<처리방침의 변경 절차>

-처리방침의 공고 및 시행에 관한 안내사항 명시

⑬ 벌칙 및 경과조치 (1) 벌칙 및 과태료

실체법 위반은 징역형 또는 벌금, 절차법 위반은 과태료 부과

구분	주요내용	처벌 및 벌칙	구분	주요내용	처벌 및 벌칙	구분	주요내용	처벌 및 벌칙
수집·이용	정보주체의 동의 없는 개인정보 제3자 제공(17조)	5년 이하 징역 또는 5천만원 이하 벌금	제정·구속	동의 없는 개인정보 제3자 제공(17조)	5년 이하 징역 또는 5천만원 이하 벌금	정보주체 권리보호	개인정보의 정정·삭제요청에 대한 필요한 조치를 취하지 않고, 개인정보를 계속 이용하거나 제3자에게 제공한 자(제36조)	2년 이하 징역 또는 1천만원 이하 벌금
	개인정보의 목적 외 이용·제공(18조, 제19조, 제26조)			직접마케팅 업무위탁으로 인한 개인정보 제공 시 정보주체에게 알려야 할 사항을 알리지 아니한 자(제15조, 제17조, 제18, 제26조)	3천만원 이하 과태료		개인정보의 처리정지 요구에 따라 처리를 중단하지 않고 계속 이용하거나 제3자에게 제공한 자(제37조)	2년 이하 징역 또는 1천만원 이하 벌금
	민감정보 처리기준 위반(제23조)			업무위탁 시 공개의무 위반(제26조)	1천만원 이하 과태료		개인정보 유출사실 미통지(제34조)	3천만원 이하 과태료
	고유식별정보 처리기준 위반(제24조)			개인정보의 누설 또는 타인 이용에 제공 (제59조)	5년 이하 징역 또는 5천만원 이하 벌금		정보주체의 열람 요구의 부당한 제한·거절(제35조)	1천만원 이하 과태료
	부정한 수단이나 방법에 의해 개인정보를 취득하거나 개인정보처리에 관한 동의를 얻는 행위를 한 자(제59조)	3년 이하 징역 또는 3천만원 이하 벌금	개인정보의 훼손, 멸실, 변경, 위조, 유출 (제59조)	정보주체의 정정삭제요구에 따라 필요 조치를 취하지 아니한 자(제36조)				
	개인정보의 수집기준 위반(제15조)	5천만원 이하 과태료	영상정보처리기기 설치목적과 다른 목적으로 임의 조작하거나 다른 곳을 비추는 자 또는 녹음기능을 사용한 자(제25조)	3년 이하 징역 또는 3천만원 이하 벌금	처리정지된 개인정보에 대해 파기 등의 조치를 하지 않은 자(제37조)			
	만 14세 미만 아동의 개인정보 수집 시 법정대리인 동의획득의무 위반 (제22조)		직무상 알게 된 비밀을 누설하거나 직무상 목적 외 사용한 자(제60조)	2년 이하 징역 또는 1천만원 이하 벌금	시정명령 불이행(제64조)			
	탈의실·목욕실 등 영상정보처리기기 설치 금지 위반(제25조)		안전성 확보에 필요한 보호조치를 취하지 않아 개인정보를 도난·유출·변조 또는 훼손당하거나 분실한 자(제24조, 제25조, 제29조 위반)	3천만원 이하 과태료	정보주체의 열람, 정정·삭제, 처리정지 요구 거부 시 통지의무 불이행 (제35조, 제36조, 제37조)			
	직접마케팅 업무위탁으로 인한 개인정보 제공 시 정보주체에게 알려야 할 사항을 알리지 아니한 자 (제15조, 제17조, 제18, 제26조)	3천만원 이하 과태료	개인정보 안전관리	안전성 확보에 필요한 조치의무 불이행 (제24조, 제25조, 제29조)	3천만원 이하 과태료		관계물품·서류 등의 미제출 또는 허위 제출(제63조)	
	최소한의 개인정보 외 정보의 미동의를 이유로 재화 또는 서비스 제공을 거부한 자(제16조, 제22조)			영상정보처리기기 설치·운영기준 위반 (제25조)	1천만원 이하 과태료		출입·검사를 거부·방해 또는 기피한 자 (제63조)	
	주민등록번호를 제공하지 아니할 수 있는 방법 미제공(제21조)			개인정보를 분리해서 저장·관리하지 아니한 자(제21조)		파기	개인정보 미파기(제21조)	
	동의획득방법 위반하여 동의 받은 자 (제22조)			개인정보처리방침 미공개(제30조)			영상정보처리기기 안내판 설치 등 필요조치 불이행(제25조)	
			개인정보관리책임자 미지정(제31조)					

⑭ 시행일 및 경과조치

시행일

- 개인정보보호법은 '11.9.30(공포 후 6개월 경과일)부터 시행 (부칙 1조)
- 주민등록번호 외의 회원가입 방법(i-PIN등) 적용(법 제24조제2항)은 '12.3.30(공포 후 1년 경과일)부터 시행 (부칙 1조)

경과조치 (영 부칙)

- 개인정보 암호화는 고시 수립일로부터 3개월 이내에 암호화 계획 수립, '12.12.31까지 암호화 적용 (영 제4조)
- 개인정보 영향평가는 고시 수립일로부터 3개월 이내에 영향평가 계획 수립, '16.9.30(5년 이내)까지 영향평가 완료 (개인정보 영향평가 고시 부칙 제2조)
- 법 시행 이전에 다른 법령에 따라 적법하게 처리된 개인정보, 근거 법령없이 처리된 개인정보는 이 법에 따라 처리된 것으로 간주(소급 불인정)
다만, 9.30 이후 새롭게 개인정보를 처리하는 경우 개인정보보호법 적용



감사합니다

- 개인정보보호 종합포털 : www.privacy.go.kr
- 개인정보침해신고센터 : (국번없이) 118, (홈페이지) privacy.kisa.or.kr