요양기관 개인정보보호 상담사례집

건강보험심사평가원
HEALTH INSURANCE REVIEW & ASSESSMENT SERVICE

Contents

I.

소개

IV.

요양기관 개인정보보호 상담사례

1. 공통사항

1.1 요양기관 개인정보 자율보호서비스 이용 방법 08

1.2 개인정보 일반(Q1~3) 17

1.3 개인정보 보호책임자의 지정(Q4) 21

1.4 개인정보 처리방침의 수립 및 공개(Q5) 23

1.5 개인정보 유출방지(Q6) 25

2. 개인정보의 수집

2.1 개인정보의 수집(Q7~12) 27

II.

요양기관 개인정보보호 이것만은 꼭~!

III.

용어 정의

3. 개인정보의 보관

3.1 물리적 접근방지(Q13) 34

3.2 접근권한 관리 및 접근 통제(Q14~23) 36

3.3 개인정보 암호화(Q24~25) 47

3.4 접속기록 보관(Q26~27) 50

3.5 보안프로그램 설치운영(Q28) 53

4. 개인정보의 이용·제공

4.1 개인정보의 이용(Q29~31) 55

4.2 개인정보의 제공(Q32~35) 59

5. 개인정보의 파기

5.1 개인정보의 파기(Q36~39) 64

6. 영상정보처리기기(CCTV)

6.1 영상정보처리기기 설치·운영(Q40~44) 69

[첨부] 요양기관 구비 법정서식

❶ 개인정보 처리방침(예시) 75

❷ 통제구역 출입관리대장(예시) 77

❸ 표준 개인정보처리위탁 계약서(예시) 78

❹ 개인정보 파기 관리대장(예시) 80

❺ CCTV 설치 안내판(예시) 80

I. 소개

동 상담사례집에는 요양기관 스스로 「개인정보 보호법」을 준수하기 위한 노력에 더해 이해를 돕고, 적용할 수 있도록 현장의 목소리를 담았습니다.

건강보험심사평가원(이하 '심평원') 및 의약단체는 「개인정보보호 자율규제단체 지정 등에 관한 규정」에 따라 요양기관의 개인정보보호 자율보호 활동을 지원하고 있습니다. 이는 요양기관이 개인정보보호위원회(이하 '보호위원회')로부터 자료제출 요구 및 검사를 1년간 면제받을 수 있는 조건이기도 합니다.

※자율보호 활동은?

온라인 자율점검 서비스, 현장지원 컨설팅, 온·오프라인 교육 등 일련의 활동을 말함

아울러, 요양기관업무포털(biz.hira.or.kr) 참고자료실을 통해 자율점검 표준가이드, 상담사례집을 파일로 공유·제공하고 있습니다.

이번 상담사례집은 2017, 2018, 2019, 2020년 발간 본에 이은 최신 본으로 관련 법령의 개정사항을 반영하였습니다. 또한, 요양기관이 준수하여야 할 자율보호 항목을 질의응답 형식의 쉬운 용어로 재해석하여 이해를 돕고자 하였습니다.

「개인정보 보호법」의 강화 추세와 요양기관의 관리 소홀에 따른 개인정보 유출 사고가 가져올 사회적 파장을 생각하면 예방적 차원의 자율보호 활동이 보다 절실하다 하겠습니다.

본 상담사례집이 미약하게나마 요양기관에 도움이 되길 바라며, 심평원은 앞으로도 의약단체와 함께 곁에서 도움이 될 수 있도록 꾸준히 매진해 나가겠습니다.

- 상담사례집은 요양기관이 개인정보보호와 관련하여 심평원에 문의한 주요 상담내용을 질문·답변 형식으로 구성한 것입니다.
- 일부 답변 내용은 해당 사례에만 국한되어 일반적으로 적용하기 어려운 경우도 있으므로, 지나친 확대 해석이나 일반화는 피하여야 합니다.
- 답변에 활용된 법령 및 지침 등은 상담사례집 제작 시점의 내용을 준수한 것으로 해당 법령 및 지침이 개정된 경우에는 개정 후 조치사항을 준수하여야 합니다.
- 본 자료는 요양기관업무포털(biz.hira.or.kr)에서 다운로드 받으실 수 있습니다.
- 상담사례집과 관련하여 궁금한 사항은 심평원 고객센터(☎ 1644-2000)으로 문의 주시기 바랍니다.

II. 요양기관 개인정보보호 이것만은 꼭~!

❶ 환자동의

진료(조제)목적 외 개인정보 수집은 자제하되, 수집 필요시엔 꼭 동의 받으세요~!

❷ 법령확인

환자가 아닌 다른 사람(기관)이 개인정보(진료기록부 사본 등)를 요구할 땐 근거법령을 확인하세요~!

❸ 잠금보관

환자의 개인정보가 포함된 자료(처방전, 차트, USB 등)를 보관할 땐 꼭 잠금 처리하세요~!

❹ 완전파기

보존기한이 지났거나 수집 목적이 달성된 개인정보는 복구 또는 재생되지 않도록 파기하세요~!

❺ 위탁작성

타 기관에 환자 개인정보를 위탁 처리 한다면, "개인정보 처리위탁 계약서"를 작성하세요~!

❻ 방침게시

개인정보 처리방침을 작성하고 보기 쉬운 장소(홈페이지, 접수대 등)에 게시하세요~!

❼ CCTV안내

CCTV를 설치하여 운영하는 경우, 접수대 등 환자가 보기 쉬운 장소에 안내판을 설치하세요~!

❽ 비밀번호

청구SW, 전자차트, 조제지원SW에 담당자별 ID(1인1계정)를 생성하고 안전한 비밀번호를 사용하세요~!

❾ 백신점검

기업용 PC 백신 프로그램을 사용하고 최신 업데이트 및 실시간 검사되고 있는지 확인하세요~!

❿ 정기백업

악성코드 감염 등 보안 사고에 대비하여 진료기록 등을 주기적으로 백업하세요~!

⓫ 교육이수

개인정보 유출 방지를 위해 개인정보보호 교육을 1년에 1회 이상 꼭 실시하세요~!

⓬ 관리계획

개인정보 분실·도난·유출·위조·변조·훼손 등을 막기 위해 내부관리계획을 수립하세요~!

※ 위 내용은 「개인정보 보호법」 준수사항을 모두 포함한 것이 아닌, 요양기관 개인정보보호를 위한 최소한의 수칙만을 기재한 것입니다.

III. 용어 정의

1. **"개인정보"**란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.

2. **"진료정보"**란 진료를 목적으로 수집하여 처리하는 개인정보가 포함된 정보로 진료기록부, 수술기록, 조산기록부, 간호기록부, 환자명부 등으로 관리되는 정보를 말한다.

3. **"개인정보의 처리"**란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.

4. **"정보주체"**란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.

5. **"개인정보파일"**이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.

6. **"영상정보처리기기"**란 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 일체의 장치로써 「개인정보 보호법 시행령」 제3조에 따른 폐쇄회로 텔레비전(CCTV) 및 네트워크 카메라를 말한다.

7. **"개인정보처리자"**란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.

8. **"개인정보 보호책임자"**란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지는 자로서, 「개인정보 보호법 시행령」 제32조(개인정보 보호책임자의 업무 및 지정요건 등)제2항에 해당하는 자를 말한다.

9. **"개인정보취급자"**란 개인정보 처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을 말한다.

10. **"내부관리계획"**이란 요양기관이 개인정보를 안전하게 처리하기 위하여 내부 의사결정 절차를 통하여 수립 시행하는 내부 기준을 말한다.

11. **"개인정보처리시스템"**이란 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템을 말한다.

출처: 「개인정보 보호법」, 「의료법 시행규칙」, 「개인정보의 안전성 확보조치 기준」

12. **"비밀번호"**란 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망 등에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.

13. **"정보통신망"**이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다.

14. **"공개된 무선망"**이란 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.

15. **"모바일 기기"**란 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿PC 등 개인정보 처리에 이용되는 휴대용 기기를 말한다.

16. **"바이오정보"**란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.

17. **"보조저장매체"**란 이동형 하드디스크, USB메모리, CD(Compact Disk), DVD(Digital Versatile Disk)등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 용이하게 연결·분리할 수 있는 저장매체를 말한다.

18. **"내부망"**이란 물리적 망분리, 접근 통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.

19. **"접속기록"**이란 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무내역에 대하여 개인정보취급자 등의 계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우 "접속"이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신이 가능한 상태를 말한다.

20. **"관리용 단말기"**란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리시스템에 직접 접속하는 단말기를 말한다.

Ⅳ.

요양기관 개인정보보호 상담사례

1. 공통사항

1.1 요양기관 개인정보 자율보호서비스 이용 방법

1. '요양기관업무포털' 접속하기

요양기관업무포털(biz.hira.or.kr)은 요양기관이 필요로 하는 다양한 서비스를 제공하고 있습니다. 특히, 개인정보 자율보호서비스를 온라인에서 만나볼 수 있는 창구이기도 합니다.

❶ 접속환경 확인하기

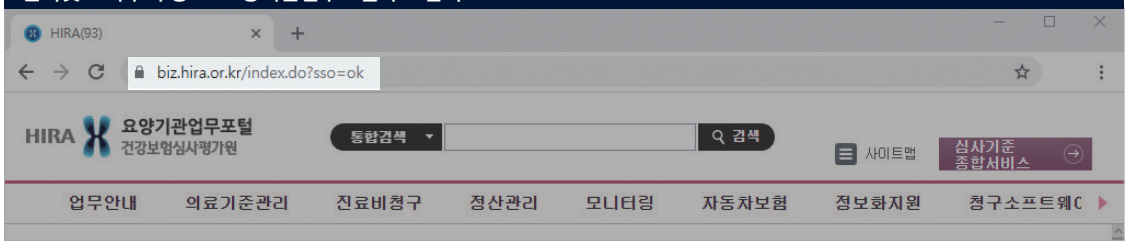
컴퓨터 시작 → 인터넷 브라우저 선택

인터넷 익스플로러 (Explorer) | 크롬 (Chrome) | 마이크로 소프트 엣지(Edge) | 사파리 (Safari)

컴퓨터 부팅 후 인터넷에 접속할 수 있는 브라우저를 선택합니다. 요양기관 업무포털은 **explorer11**과 **chrome**에 최적화 되어 있습니다. 그 외 다른 브라우저 사용 시 일부 기능이 정상적으로 동작하지 않을 수 있습니다.

❷ 메인화면 접속하기

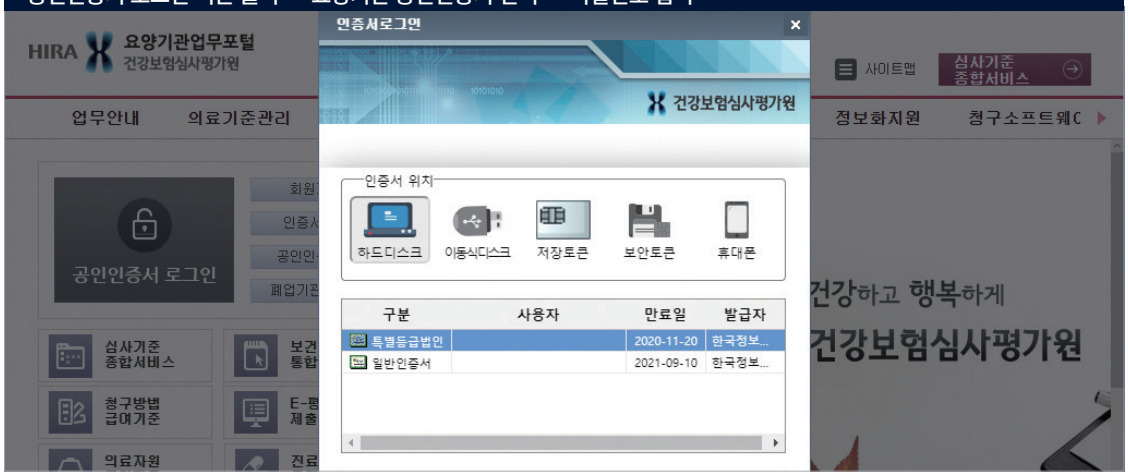
인터넷 브라우저 창 → 요양기관업무포털 주소입력



인터넷 창에 biz.hira.or.kr을 입력하여 접속합니다.

❸ 공인인증서 로그인하기

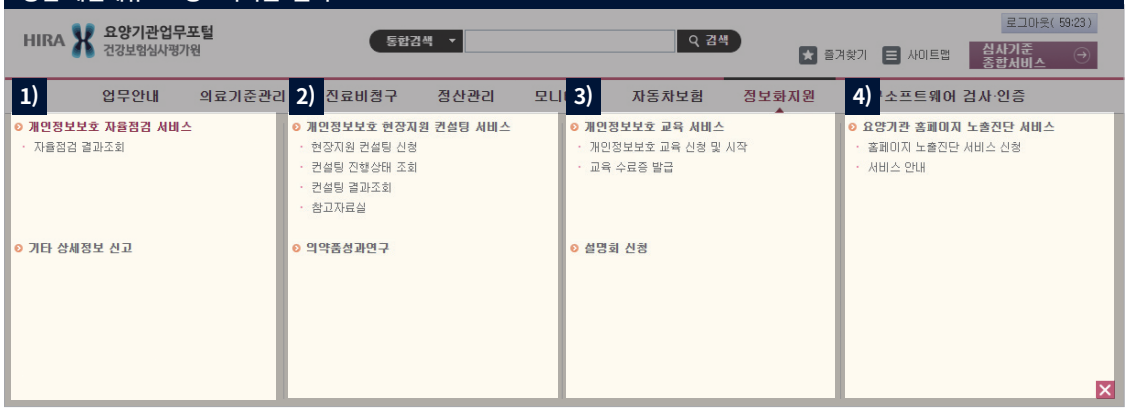
'공인인증서 로그인'버튼 클릭 → 요양기관 공인인증서 선택 → 비밀번호 입력



요양기관업무포털 메인 좌측 상단에 공인인증서 로그인 클릭 후 요양기관 인증서를 선택하여 로그인을 합니다.

❹ 개인정보 자율보호 관련 메뉴 확인하기

상단 메인메뉴 → '정보화지원' 클릭



건강보험심사평가원의 대표적인 개인정보 자율보호 서비스는 다음과 같습니다.

1) 개인정보보호 자율점검 서비스 2) 개인정보보호 현장지원 컨설팅 서비스

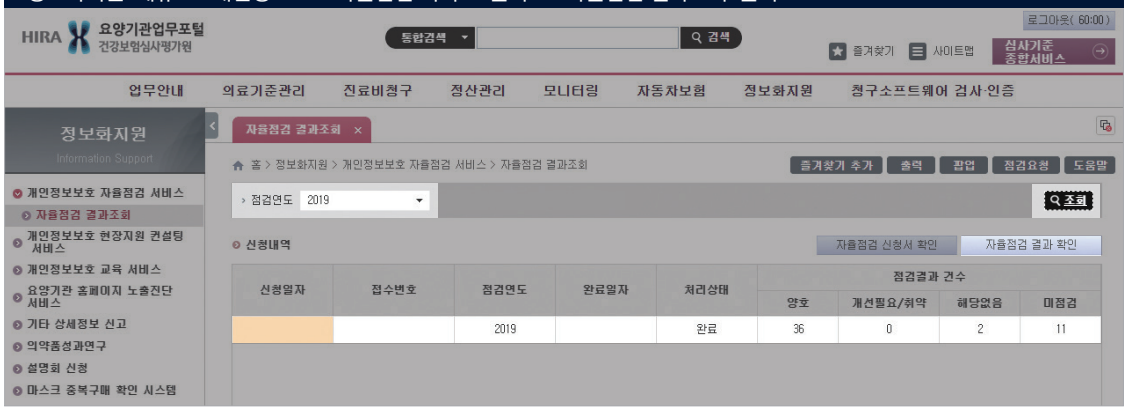
3) 개인정보보호 교육 서비스 4) 요양기관 홈페이지 노출진단서비스

2. '개인정보보호 자율점검 서비스' 이용하기

개인정보보호 자율점검 서비스는 요양기관이 개인정보 관련 된 사항을 적법하게 잘 준수하고 있는지 스스로 점검해 볼 수 있는 기회를 제공합니다. 해당 서비스는 2019년부터 자율규제단체(의약단체)가 각 회원사에게 제공하는 방식으로 변경되어 건강보험심사평가원에서는 결과 조회만 가능합니다.

❶ 자율점검 내역 조회하기

'정보화지원' 메뉴 → '개인정보보호 자율점검 서비스' 클릭 → '자율점검 결과조회' 클릭



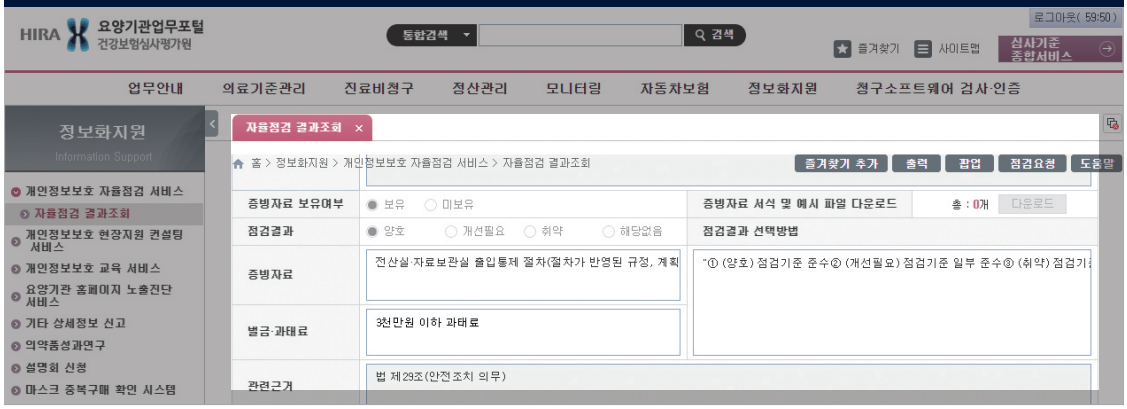
(점검이력조회) '점검연도' 선택 → '조회' 버튼 클릭

(상세결과조회) '신청일자' 선택 → '자율점검 결과 확인' 버튼 클릭

* 2019년부터는 의약단체에서 자율점검을 진행하여 당해 진행한 자율점검 결과는 다음해에 확인이 가능합니다.

❷ 자율점검 상세결과 조회하기

'정보화지원' 메뉴 → '개인정보보호 자율점검 서비스' 클릭 → '자율점검 결과조회' 클릭



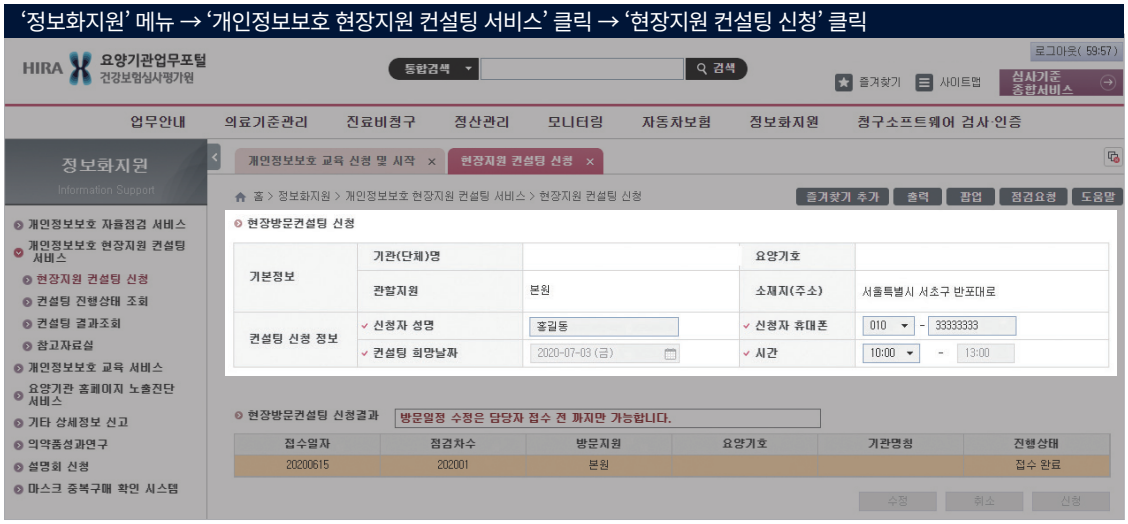
상세결과 조회를 통해 과거에 진행했던 자율점검 결과를 확인해볼 수 있습니다.

3. '개인정보보호 현장지원 컨설팅' 이용하기

개인정보보호 자율점검을 진행 시 궁금한 부분이 있거나 전반적인 내용이 어려운 분들을 지원하기 위해 건강보험심사평가원에서는 개인정보 관련 전문 인력을 양성하여 현장지원 컨설팅을 진행하고 있습니다.

❶ 현장지원 컨설팅 신청하기

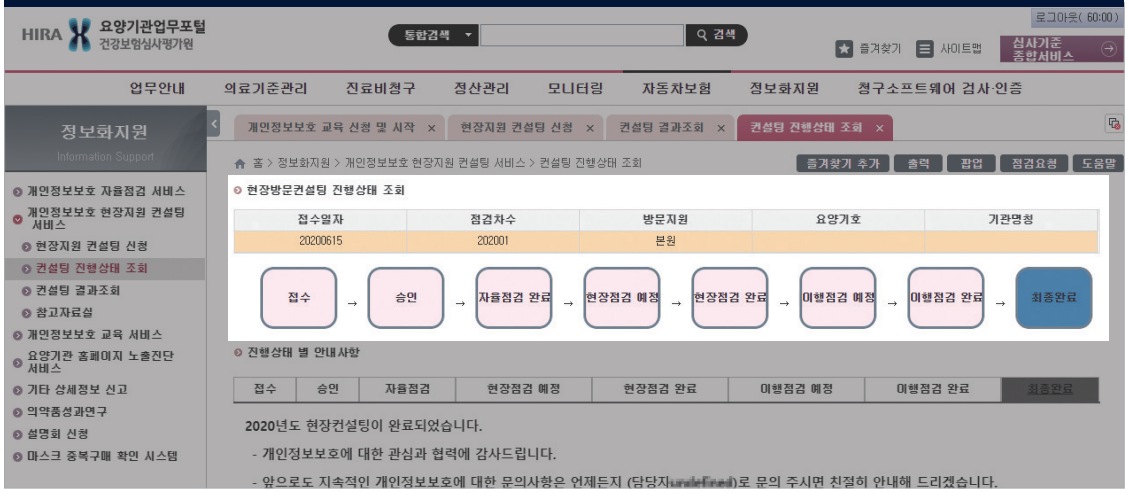
'정보화지원' 메뉴 → '개인정보보호 현장지원 컨설팅 서비스' 클릭 → '현장지원 컨설팅 신청' 클릭



(컨설팅 신청방법) 신청자 성명, 신청자 휴대폰, 컨설팅 희망날짜, 시간 입력 → '신청' 버튼 클릭 → 담당자 확인 후 연락

❷ 현장지원 컨설팅 결과 조회하기

'정보화지원' 메뉴 → '개인정보보호 현장지원 컨설팅 서비스' 클릭 → '컨설팅 진행상태 조회' 클릭



현장지원 컨설팅의 각 단계별 진행사항을 확인할 수 있습니다.

❸ 참고자료실 활용하기

'정보화지원' 메뉴 → '개인정보보호 현장지원 컨설팅 서비스' 클릭 → '참고자료실' 클릭

개인정보보호 표준 점검표, 표준가이드, 상담사례집 등 개인정보 자율보호 관련 참고자료를 다운받을 수 있습니다.

4. ‘개인정보보호 교육 서비스’ 이용하기

개인정보보호 교육 서비스는 2019년부터 시작하였습니다. 기존 오프라인 교육 대비 수강자의 접근성 및 편이성이 높아졌고 교육에 따르는 비용과 시간을 절약할 수 있습니다. 이수 시 법정의무교육을 인정받아 수료증이 발급되며 이 교육을 통하여 개인정보취급자가 받아야 할 개인정보 교육 요건을 충족할 수 있습니다. 교육 과정은 정규과정과 핵심요약 과정이 준비되어 있습니다.

❶ 개인정보보호 교육 서비스 신청하기

‘정보화지원’ 메뉴 → ‘개인정보보호 교육 서비스’ 클릭 → ‘개인정보교육 신청 및 시작’ 클릭

(사용자등록) ‘신규등록’ 버튼 클릭 후 ‘사용자 성명’ 입력 → ‘교육 과정*’ 선택 → ‘저장’ 버튼 클릭

* ‘정규’과정은 전체 내용의 상세 설명이며, ‘핵심요약’과정은 필수 요약사항으로 수준에 맞게 선택

(사용자삭제) 등록된 사용자 성명 클릭 → ‘정보삭제’ 버튼 클릭 → ‘삭제’ 버튼 클릭

(교육수강) 등록된 사용자 성명 클릭 → ‘확인’ 버튼 클릭

❷ 교육 동영상 시청하기

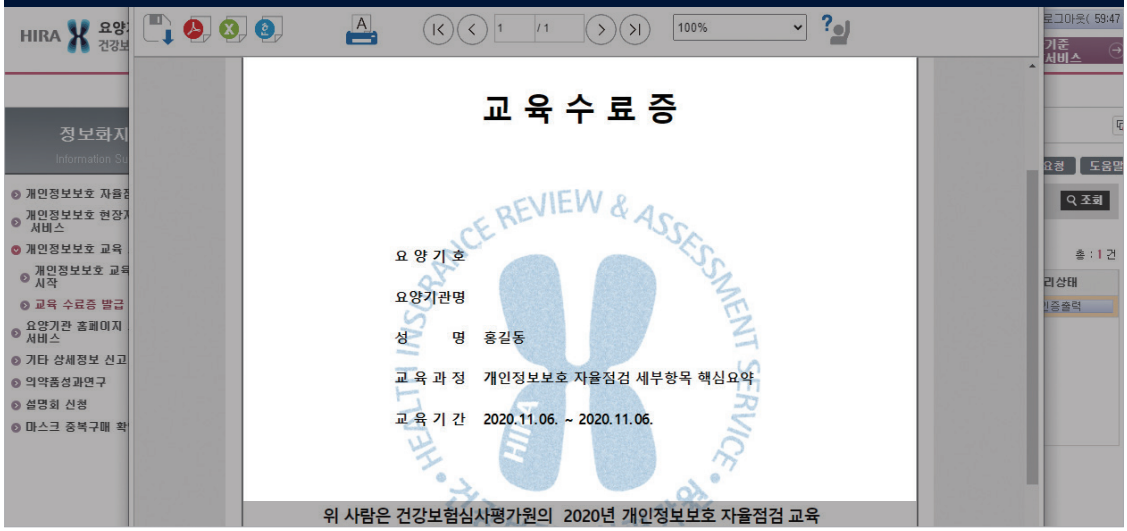
‘개인정보보호 교육 신청 및 시작’ 클릭 → ‘사용자 로그인’ 등록사용자 선택 → 목차 선택

(동영상 시청) 교육목차 확인 → ‘시청하기’ 버튼 클릭 → 모든 강의 완료 후 종료

* 강의 재생 중에 종료를 하거나 건너뛰기 등의 사용자 조작 시 수료 인정이 되지 않습니다.

❸ 수료증 발급하기

'정보화지원' 메뉴 → '개인정보보호 교육 서비스' 클릭 → '교육 수료증 발급' 클릭



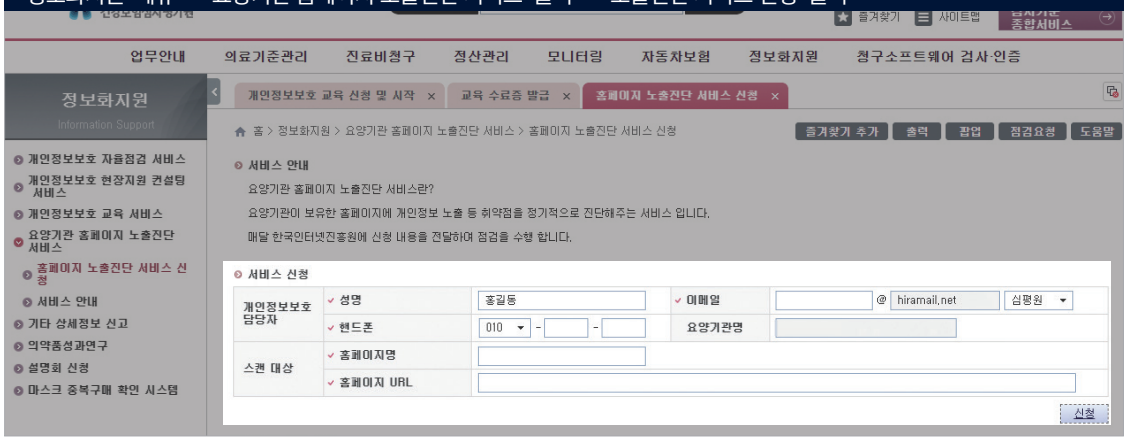
모든 강의를 수료한 후 수료증 발급 버튼을 통하여 교육 수료 확인이 가능합니다. 이후에도 언제든 필요 시 교육수료증을 발급 받으실 수 있습니다.

5. '홈페이지 노출진단 서비스' 이용하기

요양기관이 운영하고 있는 홈페이지에 대하여 개인정보 노출 등 취약점을 정기적으로 진단해주는 서비스입니다.

❶ 노출진단 서비스 신청하기

'정보화지원' 메뉴 → '요양기관 홈페이지 노출진단 서비스' 클릭 → '노출진단 서비스 신청' 클릭



(서비스 신청) 성명, 핸드폰, 이메일, 홈페이지명, 홈페이지 주소(URL) 입력 → '신청' 버튼 클릭

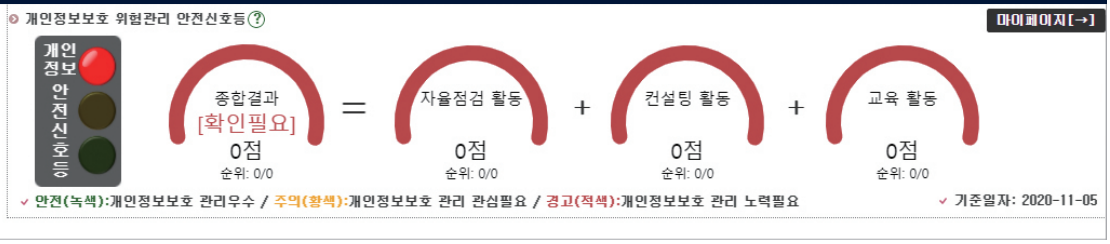
(서비스 해지) 서비스 신청 내역의 해지를 희망하는 홈페이지 클릭 → '해지' 버튼 클릭

6. ‘개인정보보호 위험관리 예측서비스(안전신호등)’ 이용하기

요양기관에서 개인정보 자율보호에 얼마나 힘쓰고 있는지 색과 점수를 통하여 직관적으로 확인 할 수 있게 도와줍니다.

❶ 안전신호등 확인하기

‘정보화지원’ 메뉴 → 각 메뉴 상단에 표시

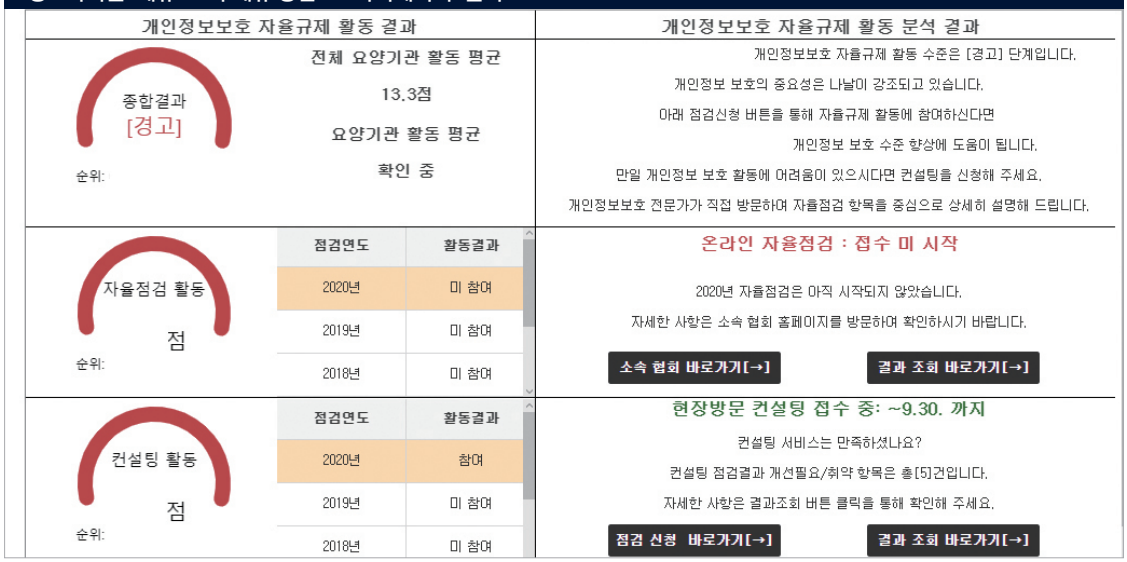


정보화지원 관련 메뉴 접근 시 노출 되며 개인정보 자율보호 활동내역을 수치와 색으로 환산 하여 나타납니다.

수치화 되는 요소는 자율점검 활동, 컨설팅 활동, 교육 활동 등의 내역을 포함합니다.

❷ 안전신호등 상세내용 확인하기

‘정보화지원’ 메뉴 → 각 메뉴 상단 → ‘마이페이지’ 클릭



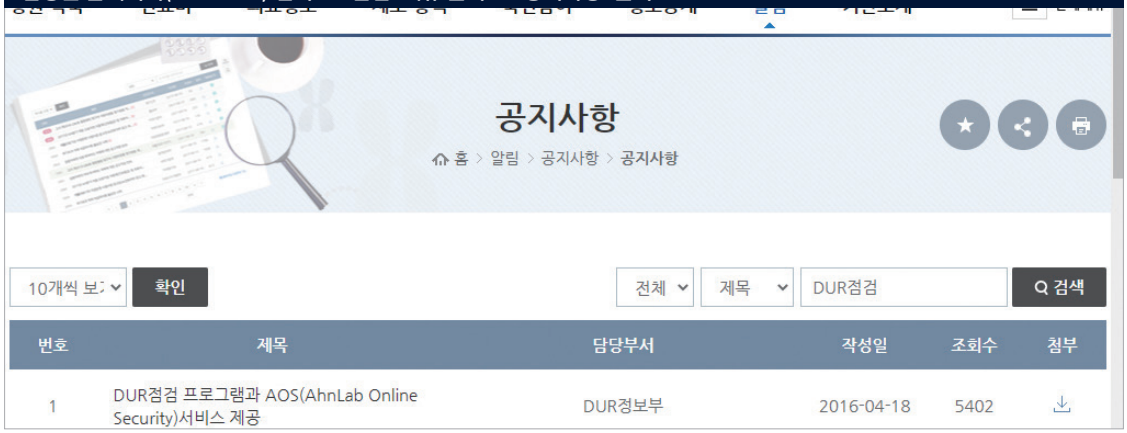
마이페이지를 통해 개인정보 자율보호 활동 내용을 확인할 수 있으며 확인 결과에 따라 온라인 자율점검, 현장지원 컨설팅, 교육 등 요양기관의 부족한 활동과 연결된 서비스로 이동되도록 구성하였습니다.

7. ‘AOS 서비스(안티바이러스, PC방화벽)’ 이용하기

심평원이 제공하는 DUR 점검프로그램 설치 시 AOS서비스(안티바이러스, PC방화벽)를 무상으로 사용할 수 있습니다. 기존에 DUR 점검프로그램을 사용하지 않는 요양기관에서도 아래 설치 방법을 통하여 사용할 수 있습니다.

❶ 심평원 홈페이지 접근하기

심평원 홈페이지(hira.or.kr) 접속 → ‘알림’ 메뉴 클릭 → ‘공지사항’ 클릭



“DUR점검”을 검색하여 “DUR점검 프로그램과 AOS(AhnLab Online Security)서비스 제공” 글을 클릭합니다.

❷ DUR점검 프로그램 다운로드 및 설치하기

‘DUR점검 프로그램과 AOS(AhnLab Online Security)서비스 제공’ 클릭 → ‘첨부파일’ 실행

첨부파일	AOS 서비스 제공 알림 표준창사용_파일 AOS구동확인 및 조치방법 DUR_Service설치방법 DurService메뉴얼_최종

(DUR 프로그램 설치 방법) ‘표준창사용_파일’ 다운 → 압축풀기 → DUR 설치프로그램 실행 → 설치

❸ AOS 설치 확인하기

윈도우 시작표시줄 아이콘 → 마우스 우클릭 → AOS 정보 확인

(AOS 비정상 실행 시) 요양기관업무포털 → 정보화지원 → 현장지원컨설팅 → ‘참고자료실’38번 글을 참고하여 설정 진행

Ⅳ.

요양기관 개인정보보호 상담사례

1. 공통사항

1.2 개인정보 일반

점검항목 **공통사항**

Q1.

우리 의원은 원장님 및 간호사 총 2명으로 운영되고 있는 소규모 의원입니다. 인력 부족에 따른 업무 부담으로 개인정보보호 활동을 수행하기 어렵습니다. 소규모 의료기관도 「개인정보 보호법」을 준수해야 할까요?

A.

「개인정보 보호법」은 개인정보의 수집·유출·오용·남용으로부터 사생활의 비밀 등을 보호함으로써 국민의 권리와 이익을 증진하고, 나아가 개인의 존엄과 가치를 구현하기 위하여 개인정보 처리에 관한 사항을 규정함을 목적으로 합니다. 이에 따라 **의료기관은 환자의 개인정보를 처리하는 기관으로써 규모에 관계없이 자율적 개인정보보호 활동을 통해 개인정보를 안전하게 관리해야 합니다.** 업무 부담에 따른 어려움도 있으시겠지만 「개인정보 보호법」을 준수하여 주시기 바랍니다.

「개인정보 보호법」 제3조(개인정보 보호 원칙) 1~4항

① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.

② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적법하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 안 된다.

③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.

④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다.

Q2.

OO 치과의원에 근무하고 있는 직원입니다. 환자로부터 원장님의 성명을 알려달라는 전화문의를 받았습니다. 성명은 개인정보라고 알고 있는데, 환자에게 알려줘도 될까요?

A.

의료기관의 대표자명은 법인이나 단체에 관한 정보로 개인정보가 아닙니다. 따라서 원장님 성명을 알려주셔도 됩니다.

하지만, 의료진이나 행정담당자의 성명, 업무상 전화가 아닌 개인 휴대전화번호, 개인 이메일은 개인정보에 해당되므로 제공 시 당사자의 동의가 필요합니다.

「개인정보 보호법」 제2조(정의)제1호

이 법에서 사용하는 용어의 뜻은 다음과 같다.

1. "개인정보"란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보)를 말한다.

'개인정보보호 법령 및 지침·고시 해설서'

법인 또는 단체에 관한 정보는 개인정보에 해당하지 않는다. 따라서 법인 또는 단체의 이름, 소재지 주소, 대표 연락처(이메일 주소 또는 전화번호), 업무별 연락처, 영업실적 등은 개인정보에 해당하지 않는다. 또한, 개인사업자의 상호명, 사업장 주소, 전화번호, 사업자등록번호, 매출액, 납세액 등은 사업체의 운영과 관련한 정보로서 원칙적으로 개인정보에 해당하지 않는다.

점검항목 **3.1.1**

Q3.

우리 의원은 최근에 개업하여 약 7,000여명의 환자 개인정보를 보유하고 있으며, 직원은 6명입니다. 저희 의원은 내부관리계획을 수립해야 하나요?

A.

내부관리계획 수립 대상에서 제외되려면 '1만 명 미만의 정보주체(환자)에 관한 개인정보를 보유'하고, 동시에 '상시근로자가 5인 미만'이어야 합니다. 귀 의원은 1만 명 미만의 환자 개인정보를 보유하고 있으나, 5명이 넘는 직원이 근무하고 있으므로 반드시 내부관리계획을 수립해야 합니다.

「개인정보 보호법」 제29조(안전조치의무)

개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

「개인정보의 안전성 확보조치 기준」 제3조(안전조치 기준 적용)

개인정보처리자가 개인정보의 안전성 확보에 필요한 조치를 하는 경우에는 [별표] 개인정보처리자 유형 및 개인정보 보유량에 따른 안전조치 기준을 적용하여야 한다. 이 경우 개인정보처리자가 어느 유형에 해당하는지에 대한 입증책임은 당해 개인정보처리자가 부담한다. * [별표] 유형1(완화) 적용대상: 1만명 미만의 정보주체에 관한 개인정보를 보유한 소상공인, 단체, 개인

「개인정보의 안전성 확보조치 기준」 제4조(내부 관리계획의 수립·시행)제1항

① 개인정보처리자는 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 다음 각 호의 사항을 포함하는 내부 관리계획을 수립·시행하여야 한다.

Ⅳ.

요양기관 개인정보보호 상담사례

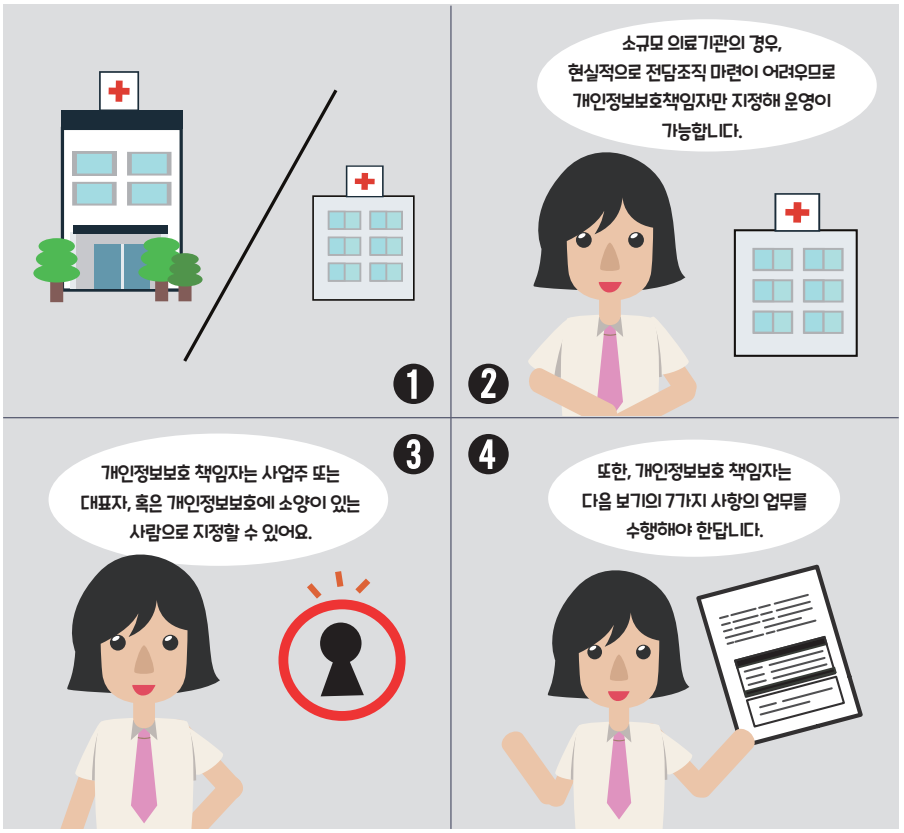
1. 공통사항

1.3 개인정보 보호책임자의 지정

점검항목 **3.8.1**

Q4.

5인 미만의 직원이 상주하여 근무하는 소규모 의원입니다. 인력 부족으로 전담조직을 구성하기 쉽지 않습니다. 개인정보 보호책임자만 지정해도 괜찮을까요?



A.

소규모 의료기관의 경우, 현실적으로 전담조직 마련이 어려우므로 개인정보 보호책임자만 지정하는 것으로 운영이 가능합니다. 개인정보 보호책임자의 지정은 다음 2가지 사항만 가능합니다.
① 사업주 또는 대표자, ② 정보주체의 개인정보 보호업무를 위해 조직된 부서의 장 또는 개인정보 보호에 관한 소양이 있는 사람으로 지정할 수 있습니다.
또한, 개인정보 보호책임자로 지정된 사람은 다음 7가지 사항의 업무를 수행해야 합니다.

「개인정보 보호법」 제31조(개인정보 보호책임자의 지정)제1항, 제2항

① 개인정보처리자는 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 지정하여야 한다.
② 개인정보 보호책임자는 다음 각 호의 업무를 수행한다.

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. 그 밖에 개인정보의 적절한 처리를 위하여 대통령령으로 정한 업무

Ⅳ.

요양기관 개인정보보호 상담사례

1. 공통사항

1.4 개인정보 처리방침의 수립 및 공개

점검항목 **3.7.1**

Q5.

최근 수강한 개인정보보호 교육을 통해 개인정보처리방침을 작성해야 한다고 들었습니다. 개인정보처리방침에는 어떠한 내용들이 들어가나요?

A.

의료기관에서는 환자(정보주체)가 자신의 개인정보가 어떻게 처리되고 있는지를 확인할 수 있도록 개인정보 처리방침을 수립해야 합니다. **☑ 개인정보 처리방침 예시자료는 [첨부] ① 참조**

「개인정보 보호법」 30조(개인정보 처리방침의 수립 및 공개)제1항, 제2항

① 개인정보처리자는 다음 각 호의 사항이 포함된 개인정보의 처리 방침을 정하여야 한다. 이 경우 공공기관은 제32조에 따라 등록 대상이 되는 개인정보파일에 대하여 개인정보 처리방침을 정한다.

1. 개인정보의 처리 목적
2. 개인정보의 처리 및 보유 기간
3. 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다)
4. 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다)
5. 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항
6. 제31조에 따른 개인정보 보호책임자의 성명 또는 개인정보 보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처
7. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항(해당하는 경우에만 정한다)
8. 그 밖에 개인정보의 처리에 관하여 대통령령으로 정한 사항

② 개인정보처리자가 개인정보 처리방침을 수립하거나 변경하는 경우에는 정보주체가 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.

Ⅳ.

요양기관 개인정보보호 상담사례

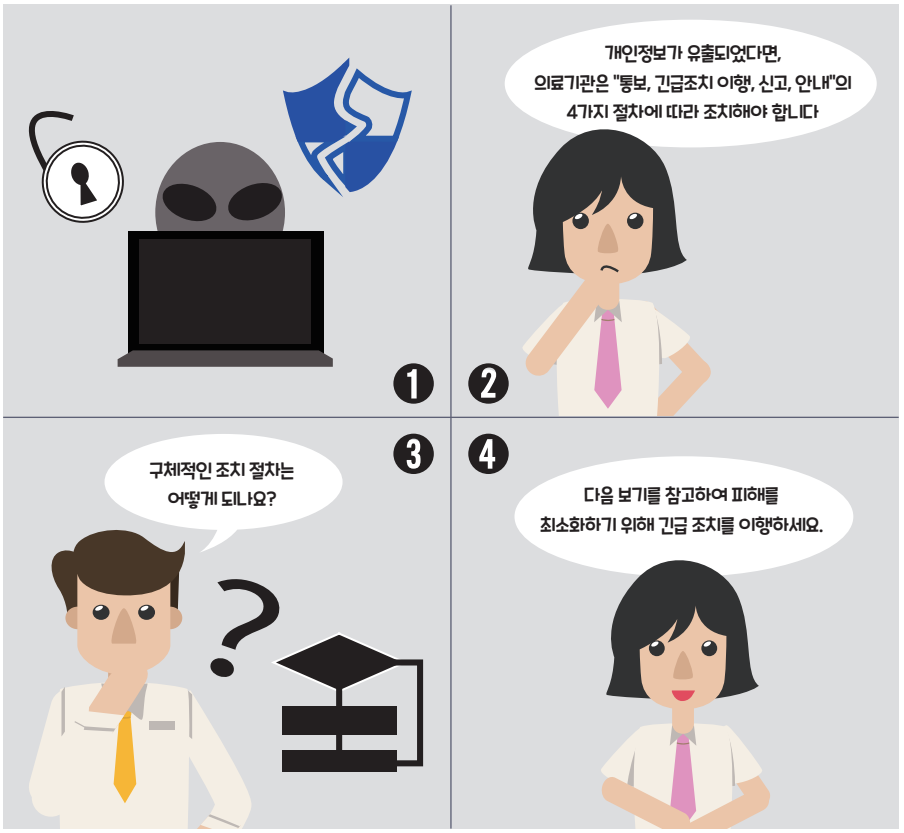
1. 공통사항

1.5 개인정보 유출방지

점검항목 **3.9.2**

Q6.

홈페이지를 운영하면서 해킹으로 인해 보유하고 있는 1,500명의 개인정보가 유출되었습니다. 이에 따라 관련 조치를 취하려고 하나, 정확한 조치 방법을 모르겠습니다. 어떠한 방식으로 진행해야 하는지 궁금합니다.



A.

개인정보가 유출되었다면 의료기관은 다음의 4가지 절차에 따라 조치를 취해야 합니다.
(「개인정보 보호법」 제34조 개인정보 유출 통지 등)

① 개인정보가 유출되었음을 알게 되었을 때로부터 지체 없이(5일 이내) 환자(정보주체)에게 유출 사실을 통보해야 합니다. 통보 내용은 다음과 같습니다.

1. 유출된 개인정보의 항목
2. 유출 시점과 그 경위
3. 피해 최소화를 위한 정보주체의 조치방법
4. 기관의 대응조치 및 피해구제 절차
5. 피해 신고 접수 담당부서 및 연락처

② 접속경로 차단, 취약점 점검·보완, 유출된 개인정보의 삭제 등 피해를 최소화하기 위해 필요한 긴급조치를 이행하여야 합니다.

③ 1천명 이상 개인정보가 유출된 경우 유출 통지 및 조치 결과를 지체 없이(5일 이내) 보호위원회 또는 한국인터넷진흥원(www.privacy.go.kr)에 신고해야 합니다.

④ 1천명 이상 개인정보가 유출된 경우에는 환자(정보주체)에게 개별통지와 함께 유출된 사실을 인터넷 홈페이지에 7일 이상 게재하여야 합니다.

* 홈페이지를 운영하지 않는 경우 서면 등의 방법으로 사업장 등의 보기 쉬운 장소에 7일 이상 게시

Ⅳ.

요양기관 개인정보보호 상담사례

2. 개인정보의 수집

2.1 개인정보의 수집

점검항목 **1.1.1**

Q7.

혼자서 운영하는 1인 약국입니다. 약국의 조제, 복약상담 등 업무 활용 목적으로 환자의 연락처가 필요합니다. 이 경우 환자 연락처를 수집해도 되나요? 된다면 동의는 어떻게 받는지요?

A.

「약사법」 제30조제1항 중 '환자의 인적사항'에는 연락처가 포함된 것으로, 약국의 조제와 복약지도 등 환자의 안전 확보를 위한 목적에 한하여 별도 동의 없이 수집이 가능합니다.

「개인정보 보호법」 제15조(개인정보의 수집·이용)제1항

개인정보처리자는 다음 각 호의 어느 하나에 해당되는 경우에는 개인정보를 수집할 수 있으며, 그 수집 목적의 범위에서 이용할 수 있다.

1. 정보주체의 동의를 받은 경우 2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
4. 정보주체화의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우
5. 정보주체 또는 그 법정대리인의 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
6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.

「약사법」 제30조(조제기록부)제1항

약사는 약국에서 의약품을 조제(제23조제3항 각 호외의 부분단서 및 각 호에 따라 처방전 없이 조제하는 경우를 포함한다)하면 환자의 인적사항, 조제 연월일, 처방 약품명과 일수 조제 내용 및 복약지도 내용, 그 밖에 보건복지부령으로 정하는 사항을 조제기록부(전자문서로 작성한 것을 포함한다)에 적어 5년 동안 보존하여야 한다.

점검항목 **1.1.1**

Q8.

우리 병원은 입원환자를 대상으로 노래자랑, 음악회 등 다양한 환자 프로그램을 운영하고 있습니다. 환자가족과 보호자가 환자의 생활모습을 확인할 수 있도록 행사 시 환자들의 활동모습을 사진으로 찍어 홈페이지에 게시하고, 병원 안내판에 사용하는데 개별적으로 환자의 동의를 받아야 하나요?

A.

개인정보 보호법 제2조 제1호는 '개인정보'를 살아있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보라고 정의하고 있습니다. 특정인을 식별할 수 있는 사진은 개인정보로서 보호대상이며 사진을 활용하기 위해서는 환자의 명시적 동의를 받아 사용하여야 할 것입니다.

「개인정보 보호법」 제15조(개인정보의 수집·이용)제1항

개인정보처리자는 다음 각 호의 어느 하나에 해당되는 경우에는 개인정보를 수집할 수 있으며, 그 수집 목적의 범위에서 이용할 수 있다.

1. 정보주체의 동의를 받은 경우 2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
4. 정보주체화의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우
5. 정보주체 또는 그 법정대리인의 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
6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.

점검항목 **1.2.3**

Q9.

OO 의원입니다. 의원 홈페이지를 개발 중입니다. 환자 편의를 위해, 홈페이지 회원가입 시 동의사항인 '개인정보 수집·이용, 제3자 제공, 마케팅 목적 처리'에 대하여 내용을 명시하고, 하나의 선택사항으로 포괄하여 동의를 받아도 되나요?

A.

의료기관에서 진료목적 외로 개인정보를 수집하기 위해서는 환자의 동의를 받아야 합니다. 동의를 받을 때에는 환자가 동의사항을 명확히 인지할 수 있도록 목적별로 구분하여 명시하고, 목적별로 각각의 동의를 받아야 합니다.

구분 동의가 필요한 경우

① 개인정보 수집·이용 동의 ② 마케팅 목적 처리 동의
③ 제3자 제공 동의 ④ 목적 외 이용·제공 동의
⑤ 법정대리인 동의 ⑥ 민감정보 처리 동의
⑦ 고유식별정보 처리 동의 ⑧ 국외 제3자 제공 동의

「개인정보 보호법」 제22조(동의를 받는 방법)제1항

개인정보처리자는 이 법에 따른 개인정보의 처리에 대하여 정보주체(제6항에 따른 법정대리인을 포함한다. 이하 이 조에서 같다)의 동의를 받을 때에는 각각의 동의 사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 각각 동의를 받아야 한다.

Q10.

산부인과를 운영 중인 원장입니다. 환자의 정확한 진료를 위해 건강, 성생활 등의 민감정보를 수집하고자 합니다. 이에 대해 환자에게 별도 동의를 받아야 하나요?

A.

진료목적으로만 민감정보를 수집·이용하는 경우는 의료법에 따라 환자 동의 없이 수집할 수 있습니다. 민감정보를 홍보 목적 등 진료와 관계없이 수집하는 경우에는,
① 민감정보의 수집/이용 목적 ②수집하려는 민감정보의 항목 ③ 민감정보의 보유 및 이용기간 ④ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우 그 불이익의 내용이 명확하게 기재되어 있어야 합니다. 또한, 환자가 14세 미만 아동인 경우에는 법정대리인의 동의도 받을 수 있도록, '개인정보 수집 동의서'를 갖추어야 합니다.
* 민감정보: 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보 등

「개인정보 보호법」 제23조(민감정보의 처리 제한)제1항

1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 민감정보의 처리를 요구하거나 허용하는 경우

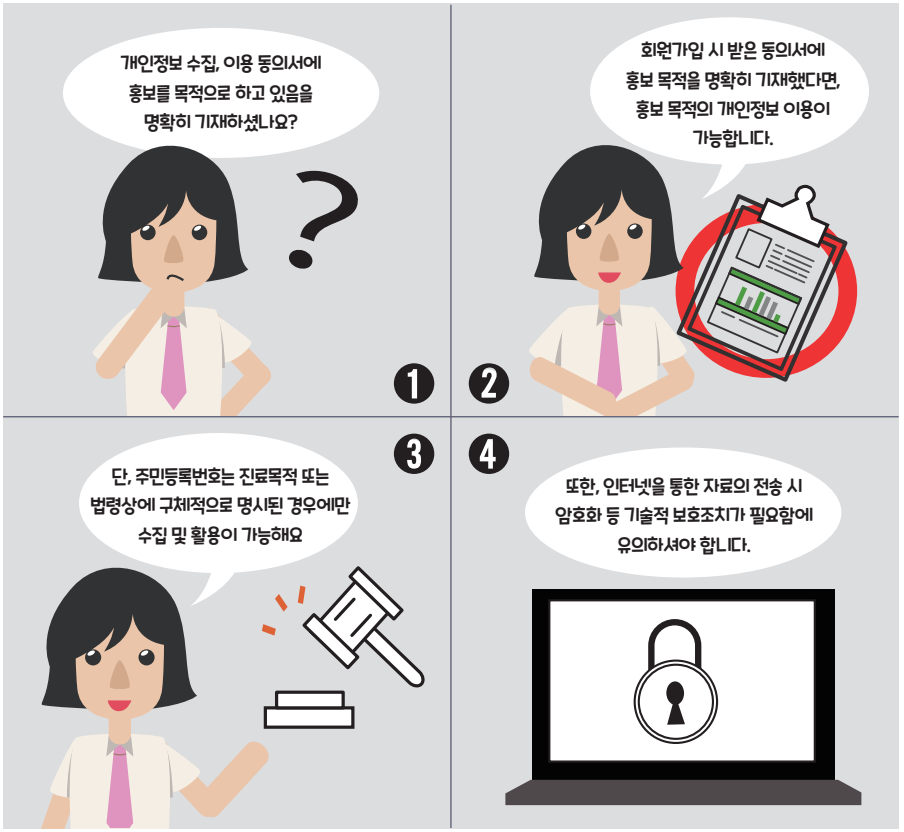
「의료법」 제22조(진료기록부 등)제1항

① 의료인은 각각 진료기록부, 조산기록부, 간호기록부, 그 밖의 진료에 관한 기록을 갖추어 두고 환자의 주된 증상, 진단 및 치료 내용 등 보건복지부령으로 정하는 의료행위에 관한 사항과 의견을 상세히 기록하고 서명하여야 한다.

점검항목 **2.1.1**

Q11.

우리 의원은 홈페이지를 운영하고 있습니다. 회원가입 시, 개인정보 수집·이용 동의서를 받고 고객의 이름, 주민등록번호 및 휴대폰번호 등을 입력토록 하고 있습니다. 이렇게 수집된 고객의 개인정보를 의원 홍보 목적으로 사용해도 될까요?



A.

회원가입 시 받은 개인정보 수집·이용 동의서에 홍보를 목적으로 하고 있음을 명확히 기재하여 해당 내용에 대한 회원들의 동의를 받았다면, 홍보목적의 개인정보 이용이 가능합니다.
단, 주민등록번호는 진료목적 또는 법령상에 구체적으로 명시된 경우에만 수집이 허용됨으로 비록 환자의 동의를 받았다 하더라도 수집할 수 없습니다.

「개인정보 보호법」 제24조의2(주민등록번호 처리의 제한)제1항

① 제24조제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다.

1. 법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
3. 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 보호위원회가 고시로 정하는 경우

Q12.

우리 치과병원에서는 주민등록번호 수집을 통해 환자를 식별하고 홍보 활동을 진행하고 있습니다. 최근 개인정보보호법을 확인해 보니 주민등록번호를 수집할 수 없다는 사실을 알게 되었습니다. 주민등록번호는 홍보 목적으로 수집할 수 없나요?

A.

2011년 「개인정보 보호법」이 시행된 이후, 개인의 주민등록번호는 법령상에 명시된 사항 이외에는 수집할 수 없습니다. 따라서 개인정보 수집·이용 동의서를 통해 개인의 동의를 받더라도 홍보목적으로는 개인의 주민등록번호는 수집할 수 없습니다.

「개인정보 보호법」 제24조의2(주민등록번호 처리의 제한)제1항

① 제24조제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다.

1. 법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
3. 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 보호위원회가 고시로 정하는 경우

Ⅳ.

요양기관 개인정보보호 상담사례

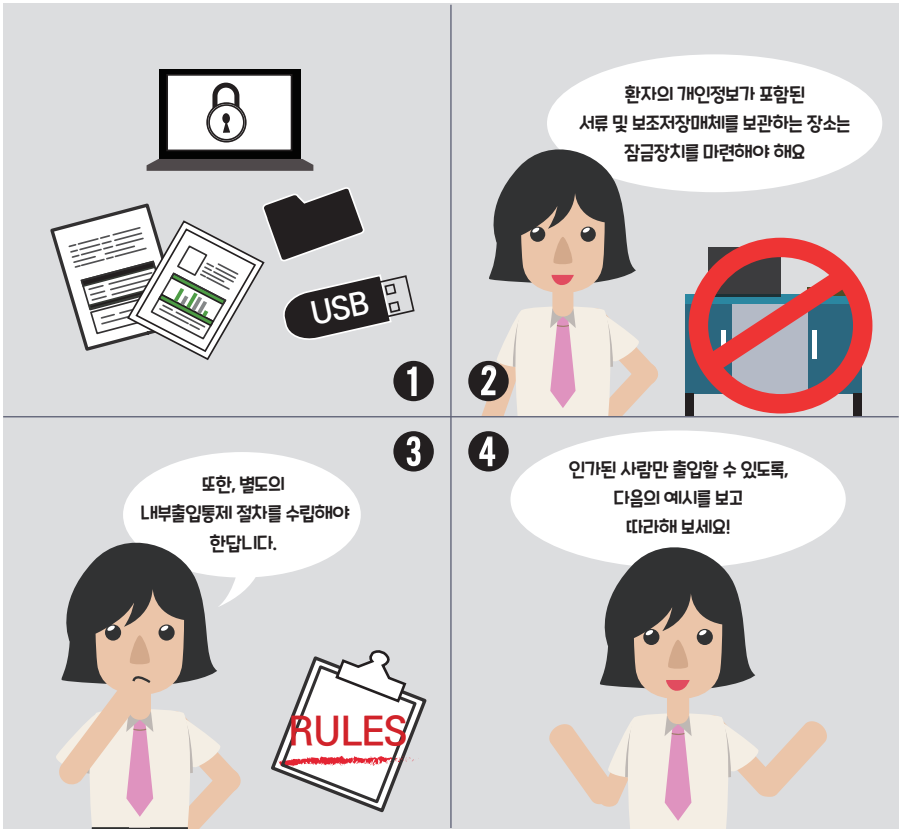
3. 개인정보의 보관

3.1 물리적 접근방지

점검항목 **3.6.1**

Q13.

전산실, 자료보관실 등 물리적 보관 장소에 대해 출입 통제절차를 수립하여 운영하라고 하는데, 저희 치과에는 전산실이 따로 없고, 진료기록부도 데스크 옆의 차트장에 잠금장치 설치 후 보관하고 있습니다. 이러한 경우 출입통제 절차를 수립하지 않아도 되나요?



A.

환자의 개인정보가 포함된 서류 및 보조저장매체(USB, 이동형 하드디스크 등)를 보관하는 장소(서랍, 캐비넷, 금고 등)에는 잠금장치를 마련하고, 별도의 내부출입통제 절차를 수립해야 합니다. 또한 환자의 개인정보를 보관하는 장소에는 가급적 인가된 사람만 출입할 수 있도록 안전한 조치를 해야 합니다.

☑ **통제구역 출입관리대장 예시자료는 [첨부] ② 참조**

「개인정보의 안전성 확보조치 기준」 제11조(물리적 안전조치)제1항 내지 제3항

① 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제절차를 수립·운영하여야 한다.

② 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.

③ 개인정보처리자는 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안 대책을 마련하여야 한다. 다만, 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있다.

Ⅳ.

요양기관 개인정보보호 상담사례

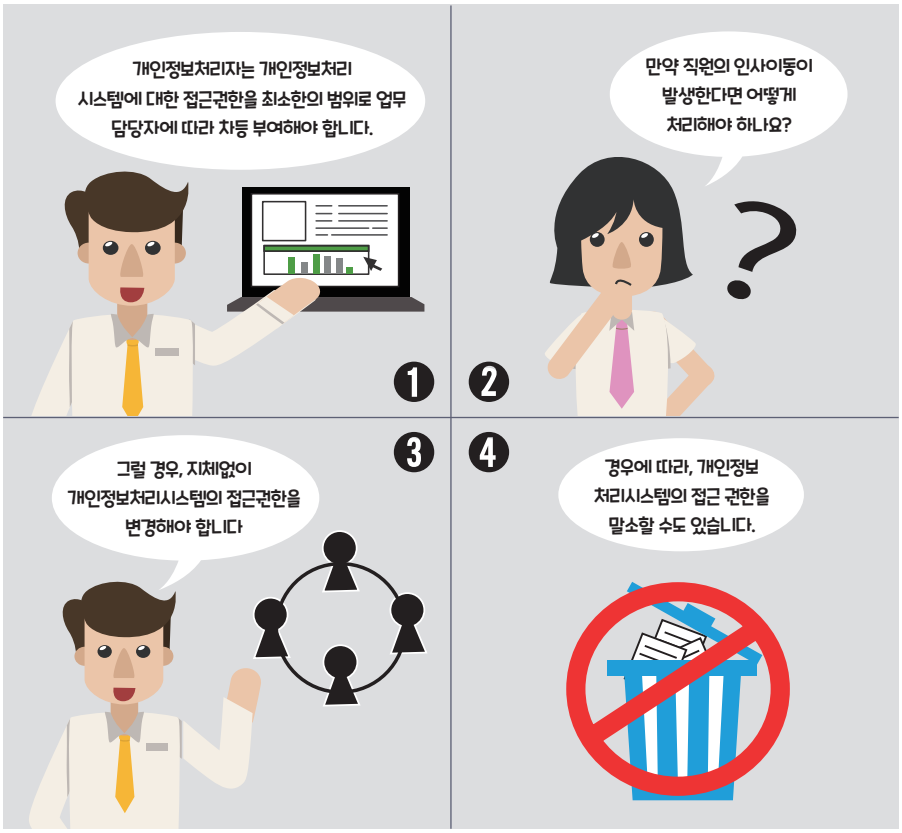
3. 개인정보의 보관

3.2 접근권한 관리 및 접근 통제

점검항목 **3.2.1**

Q14.

우리 의원에서는 직원의 휴가 및 부재 시를 대비해서 청구소프트웨어의 모든 기능들을 사용할 수 있도록 권한을 부여하였습니다. 직원마다 권한을 차등하여 부여해야 한다고 하는데 어떻게 관리해야 하나요?



A.

개인정보처리자는 환자의 개인정보처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여해야 합니다. 그리고 내부 직원이 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우에는 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소해야 할 의무가 있습니다.

「개인정보 보호법」 제29조(안전조치의무)

개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

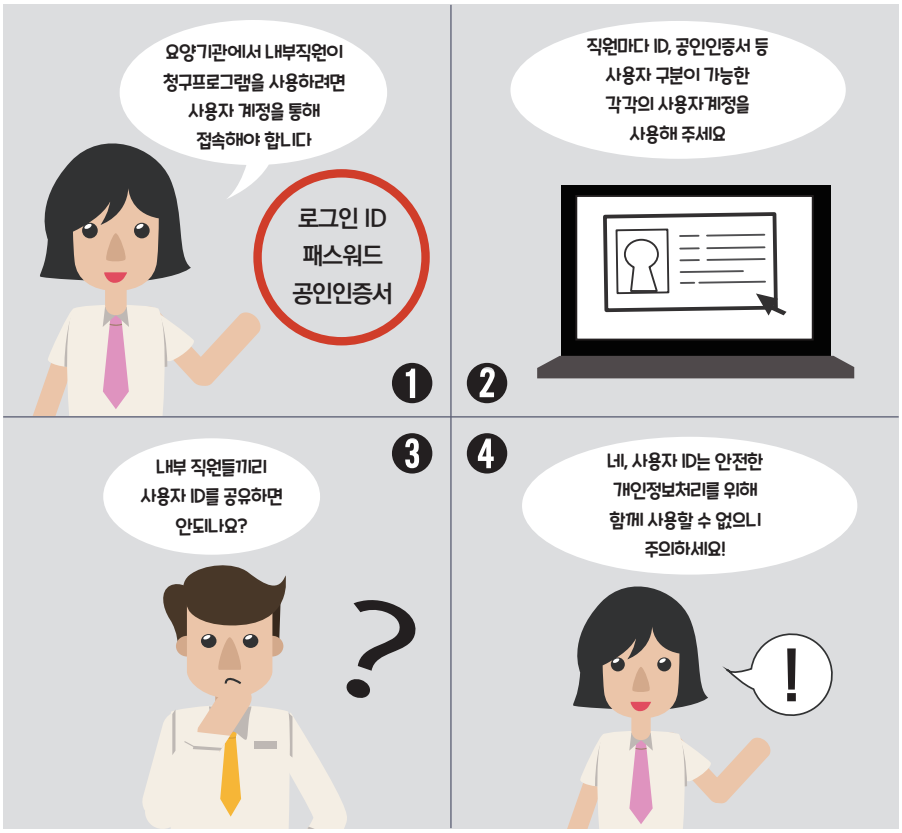
「개인정보의 안전성 확보조치 기준」 제5조(접근 권한의 관리)제1항

① 개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.

점검항목 **3.2.1**

Q15.

의원에서 청구프로그램을 사용하고 있으며, 로그인 시 ID, 패스워드 입력을 통해 접속하도록 구현되어 있습니다. 접속 기능이 불편하여 청구프로그램 업체에 로그인 기능 삭제를 요청하였으나, 청구프로그램에 들어가는 필수 기능이므로 삭제가 불가능하다는 의견을 받았습니다. 청구프로그램 접속 시 반드시 ID, 패스워드를 통해 접속하여야 하나요?



A.

요양기관에서 내부 직원이 개인정보처리시스템인 청구프로그램에 접속하기 위해서는 본인 인증 과정을 거쳐야 합니다. 인증방식으로는 계정(ID)을 부여받아 패스워드를 입력하거나 공인인증서 등을 통해 접속할 수 있습니다. 반드시 ID, 패스워드 방식으로만 접속하라는 것은 아니지만 이러한 인증 없이 바로 청구프로그램에 접속하는 것은 안 됩니다.

「개인정보 보호법」 제29조(안전조치의무)

개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

「개인정보의 안전성 확보조치 기준」 제5조(접근 권한의 관리)제4항

④ 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자 별로 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

점검항목 **3.2.1**

Q16.

약국에서 근무하는 직원은 3명입니다. 업무 편의성을 위해 1개의 사용자계정으로 환자 처방을 진행하고 있습니다. 「개인정보 보호법」상 문제는 없을까요?

A.

여러 직원이 하나의 ID를 공유하여 청구프로그램에 접속하는 것은 개인정보보호법 위반사항입니다. 따라서 청구프로그램을 사용하는 직원별로 사용자 계정을 만들어야 합니다(1인 1계정 원칙). 또한 청구프로그램 사용 권한을 각 직원이 담당하는 업무에 필요한 최소한의 범위로 부여해야 합니다.
예) 수납 담당직원의 ID로 상세 개인정보를 조회하거나 다운로드 할 수 없도록 권한을 부여

「개인정보 보호법」 제29조(안전조치의무)
개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

「개인정보의 안전성 확보조치 기준」 제5조(접근 권한의 관리)제1항, 제4항
① 개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.
④ 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자 별로 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

점검항목 **3.2.2**

Q17.

환자의 업무 처리를 위해 청구프로그램에 접속할 수 있는 접근권한을 내부 직원에게 부여하고자 합니다. 내부직원의 접근권한 부여·변경·말소 내역은 어떻게 관리하고 얼마 동안 보관해야 하나요?

A.

개인정보처리자는 접근권한 부여·변경·말소에 대한 내역을 전자적으로 기록하거나 수기로 작성한 관리대장 등에 기록하고 해당 기록을 최소 3년간 보관하여야 합니다. 또한 내부직원의 접근권한을 주기적으로 검토하여 접근권한의 과도한 부여 및 오·남용을 확인하고 조치하는 것이 필요합니다.

「개인정보 보호법」 제29조(안전조치의무)

개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

「개인정보의 안전성 확보조치 기준」 제5조(접근 통제)제1항 내지 제3항

① 개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.

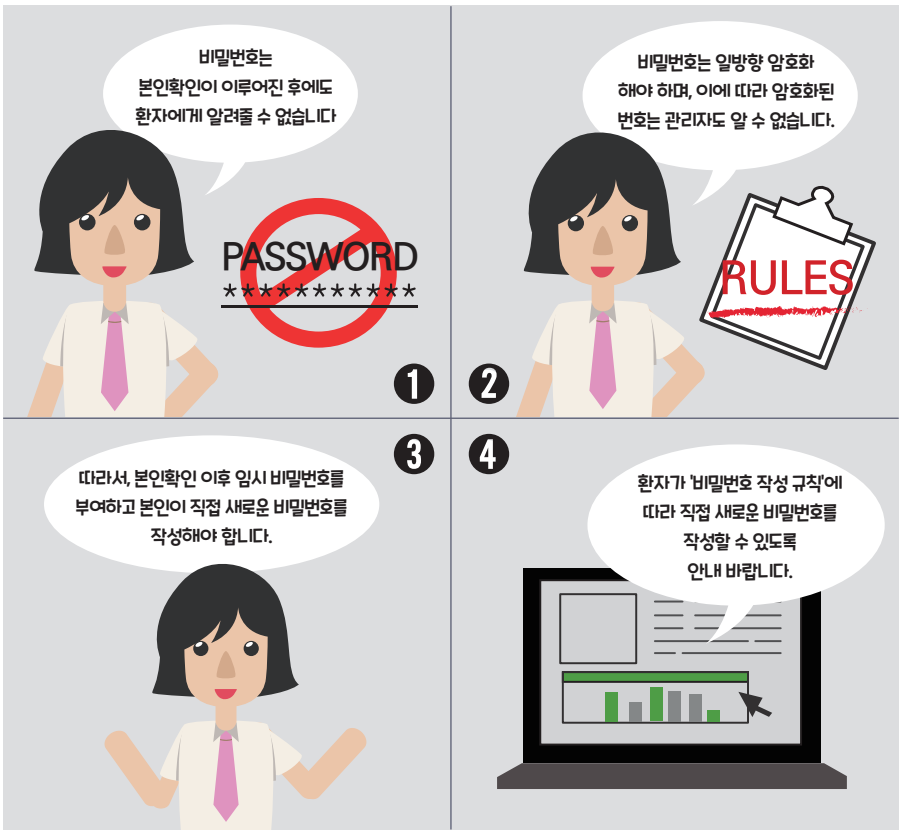
② 개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하여야 한다.

③ 개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.

점검항목 **3.2.3**

Q18.

홈페이지에 가입한 환자가 비밀번호를 알려달라고 요청했습니다. 본인 확인 후 비밀번호를 알려주어도 문제가 없나요?



A.

비밀번호는 일방향암호화(해독이 불가능한 방법) 적용에 따라 비록 관리자라 하더라도 알 수 없습니다. 따라서 본인확인 후에는 임시 비밀번호를 부여하고 '비밀번호 작성규칙*'에 따라 직접 새로운 비밀번호를 작성하도록 안내하시기 바랍니다. 아울러, 비밀번호를 관리자는 알 수 있다면 일방향암호화 미적용 상태로 개선이 필요한 사항입니다.

* '비밀번호 작성규칙' 중 최소길이는 영어 대·소문자, 숫자, 특수문자 등 3가지 조합 8자리, 2가지 조합 10자리를 부여해야 합니다.

「개인정보 보호법」 제29조(안전조치의무)

개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

「개인정보의 안전성 확보조치 기준」 제7조(개인정보의 암호화)제1항, 제2항

① 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

② 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향암호화하여 저장하여야 한다.

점검항목 **3.2.3**

Q19.

치과병원 청구프로그램 운영 직원입니다. 우리 치과병원에서는 내부 직원의 비밀번호 확인 요청 시 비밀번호를 초기화하여 직원이 직접 재설정 하도록 안내하고 있습니다. 하지만 일부 직원들이 비밀번호를 직접 알려달라고 하는데 알려줘도 문제가 없을까요?

A.

비밀번호는 직원에게 직접적으로 알려줄 수 없습니다. 비밀번호는 반드시 일방향암호화(해독이 불가능한 방법)해야 하며, 암호화 된 비밀번호는 관리자도 알 수 없어야 합니다. 따라서 내부 직원이 비밀번호 확인 요청 시 임시 비밀번호를 부여하고 '비밀번호 작성규칙'에 따라 내부직원이 직접 새로운 비밀번호를 설정 후 사용하도록 안내해야 합니다.

「개인정보 보호법」 제29조(안전조치의무)

개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

「개인정보의 안전성 확보조치 기준」 제5조(접근권한의 관리)제6항

⑥ 개인정보처리자는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다.

점검항목 **3.2.3**

Q20.

최근 다양한 개인정보 유출 기사를 통해 개인정보보호의 중요성을 인식하고 있습니다. 약국에서 사용하는 청구프로그램의 비밀번호를 지속적으로 변경하고자 합니다. 몇 개월마다 변경해야 할까요?

A.

개인정보를 저장하고 있는 청구프로그램의 비밀번호는 최소 6개월마다 변경하여야 합니다. 이와 같은 조치를 통해 해킹, 악성코드 등 개인정보 유출 위험으로부터 환자의 개인정보를 안전하게 보호할 수 있습니다.

「개인정보 보호법」 제29조(안전조치의무)

개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

*** 「개인정보 보호법」 해설서 및 보호위원회 '개인정보 오남용 피해예방 10계명'**

– 비밀번호에 유효기간을 설정하고 주기적으로 변경할 필요가 있다.

「요양급여비용 심사청구소프트웨어 검사 등에 관한 기준」(보건복지부 고시 제2018-141호, 2018.7.12.)

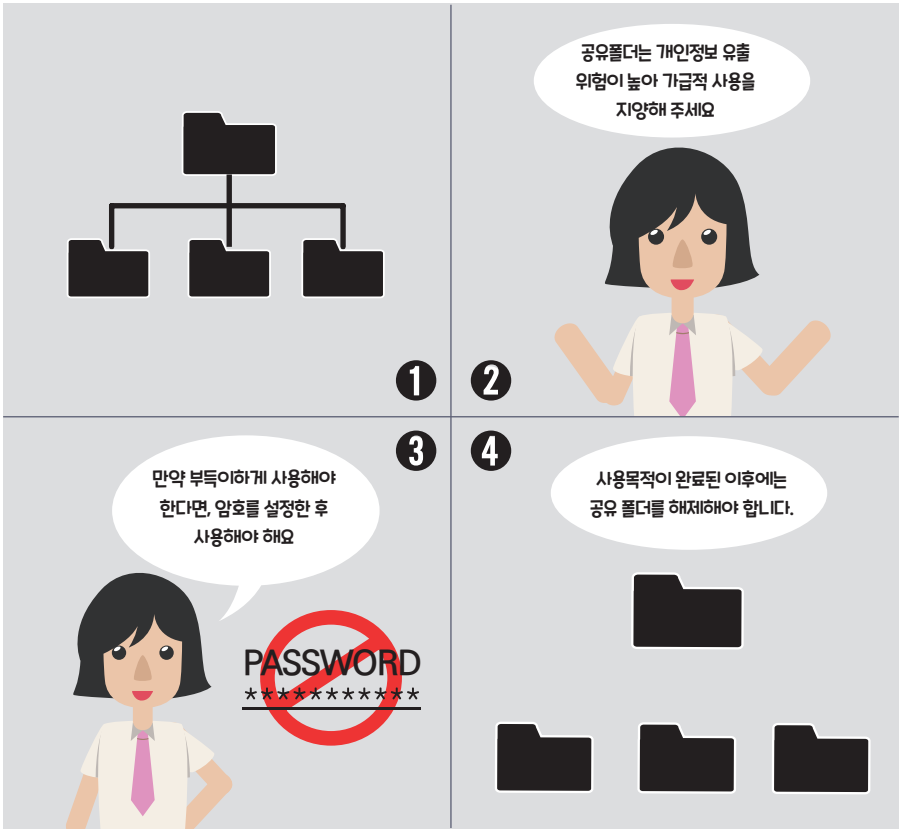
*** '청구소프트웨어 보안기능 검사 안내서'** 1. 접근 권한관리 및 접근 통제 1.6 비밀번호 사용 관리

– 비밀번호를 최소 6개월마다 변경하도록 작성규칙을 수립하여 적용하여야 한다.

점검항목 **3.2.6**

Q21.

우리 치과의원은 진료실이 3곳으로 분산되어 있습니다. 원장님의 진료 편의를 목적으로 PC에 공유폴더를 설정하여 환자의 개인정보를 확인하고 있습니다. 공유폴더 사용 시 주의사항에는 어떠한 것이 있나요?



A.

공유폴더는 개인정보 유출위험이 높기 때문에 가급적 사용을 지양하여 주시기 바랍니다. 그러나 업무목적 등 부득이한 사유로 공유폴더를 사용해야 한다면 공유폴더에 암호를 설정한 후 사용해야 합니다. 사용목적이 완료된 이후에는 공유폴더를 해제해야 합니다.

「개인정보 보호법」 제29조(안전조치의무)

개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

「개인정보의 안전성 확보조치 기준」 제6조(접근 통제)제3항

③ 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 하여야 한다.

점검항목 **3.2.8**

Q22.

청구프로그램 접속 시 비밀번호를 5회 연속으로 잘못 입력 하였더니 접속 ID가 일정 시간동안 비활성화 되었습니다. 한의원 내부 직원만 사용하는 프로그램으로 해당 기능은 너무 불필요한 기능인 것 같습니다. 청구프로그램업체에 해당 기능의 삭제를 요청해도 될까요?

A.

의료기관은 환자의 개인정보를 보유하고 있기 때문에, 내부 및 외부의 위험으로부터 환자의 개인정보를 안전하게 보호해야 합니다. 계정 접근제한 기능은 환자의 개인정보를 보호하기 위한 최소한의 기능입니다. 이러한 기능은 비인가자의 로그인 시도를 차단하는데 의미가 있으며, 잠금 해제 시에도 별도로 본인확인 절차를 마련하여 적용해야 합니다.

「개인정보 보호법」 제29조(안전조치의무)

개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

「개인정보의 안전성 확보조치 기준」 제5조(접근 통제)제6항

⑥ 개인정보처리자는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다.

점검항목 **3.2.9**

Q23.

의원에서 청구프로그램 사용 시 일정 시간(예: 5분)이 지나면 화면 접속이 차단되어 업무에 불편함이 있습니다. 이러한 기능은 반드시 필요한가요?

A.

개인정보취급자가 일정시간 이상 업무처리를 하지 않을 시 접속 차단을 하는 것은 환자의 개인정보를 지키기 위한 최소한의 기능입니다. 또한 화면이 차단된 이후 재접속 시에는 최초의 로그인과 동일한 방법으로 ID, 패스워드를 입력해야 합니다.

「개인정보 보호법」 제29조(안전조치의무)

개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

「개인정보의 안전성 확보조치 기준」 제6조(접근 통제)제5항

⑤ 개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하여야 한다.

Ⅳ.

요양기관 개인정보보호 상담사례

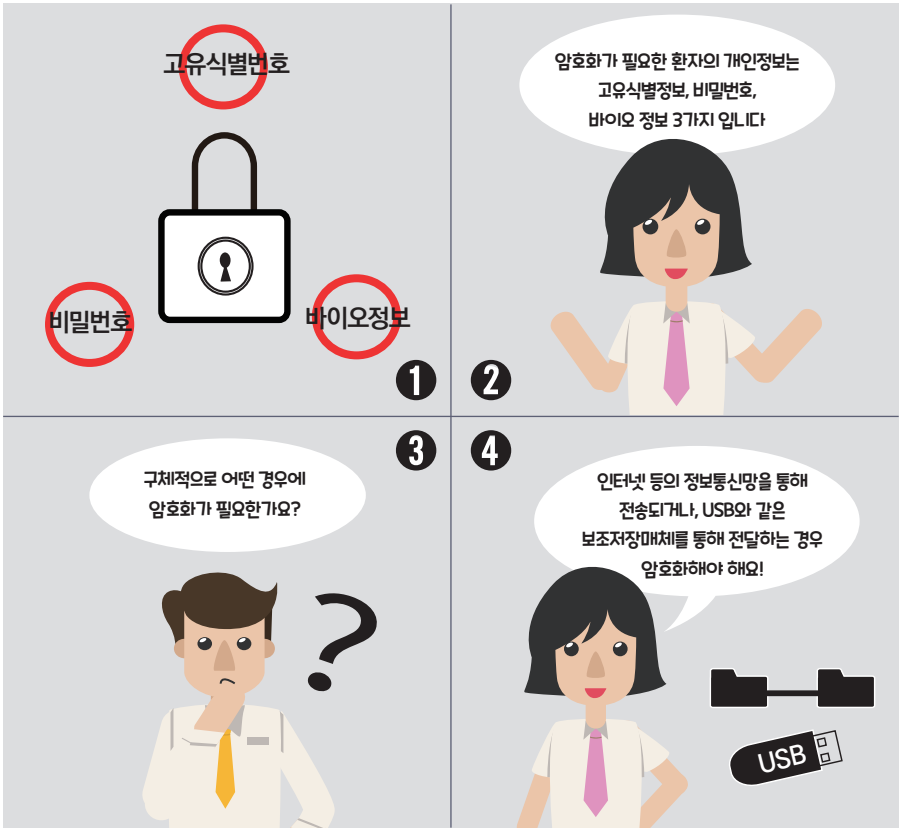
3. 개인정보의 보관

3.3 개인정보 암호화

점검항목 **3.3.1**

Q24.

의료기관에서 암호화를 해야 하는 환자의 개인정보에는 어떠한 것들이 있나요?



A.

암호화 대상인 환자(정보주체)의 개인정보는 고유식별정보, 비밀번호, 바이오정보입니다. 이와 같은 3가지 개인정보는 인터넷 등의 정보통신망을 통해 전송되거나 USB 등과 같은 보조저장매체를 통해 전달하는 경우 암호화해야 합니다.

「개인정보 보호법」 제29조(안전조치의무)

개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

「개인정보의 안전성 확보조치 기준」 제7조(개인정보의 암호화)제1항

① 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

점검항목 **3.3.4**

Q25.

치과병원에서 청구프로그램을 개발하는 직원입니다. 환자의 비밀번호 암호화 시 사용가능한 알고리즘에는 어떠한 것들이 있나요?

A.

비밀번호를 암호화하는 경우 안전한 암호 알고리즘으로 일방향 암호화하여 저장해야 합니다.
아래 표에서 제시하는 일방향 암호 알고리즘을 적용하시면 됩니다.

구분	공공기관	민간 부문(법인·단체·개인)
대칭키 암호 알고리즘	SEED. LEA, HIGHT, ARIA-128/192/256	ARIA-128/192/256, SEED, AES-128/192/256, Blowfish, Camella-128/192/256, MISTYI, KASUMI, 등
공개키 암호 알고리즘	RSAES-OAEP	RSA, RSAES-OAEP, RSAES-PKCSI 등
일방향 암호 알고리즘	SHA-224/256/384/512	SHA-224/256/384/512, Whirlpool 등

「개인정보 보호법」 제29조(안전조치의무)
개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

「개인정보의 안전성 확보조치 기준」 제7조(개인정보의 암호화)제2항, 제5항
② 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화 되지 아니하도록 일방향암호화하여 저장하여야 한다.
⑤ 개인정보처리자는 제1항, 제2항, 제3항, 또는 제4항에 따라 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

Ⅳ.

요양기관 개인정보보호 상담사례

3. 개인정보의 보관

3.4 접속기록 보관

점검항목 **3.4.1**

Q26.

우리 의원은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 6개월 이상 보관하고 있습니다. 개인정보 보호 조치를 잘하고 있는 것인가요?

A.

의원은 「의료법」에 따라 고유식별정보 및 민감정보를 처리하고 있습니다. 따라서 「개인정보의 안전성 확보조치 기준」 개정(2019.6.7.)에 따라 접속한 기록을 2년 이상 보관하여야 합니다. 개인정보처리시스템을 위탁·운영하는 경우에도 2년 이상 접속기록 보관하여야 합니다.

또한, 개인정보의 유출·변조·훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 하며, 개인정보를 다운로드 한 것이 발견되었을 경우에는 내부관리 계획으로 정하는 바에 따라 그 사유를 반드시 확인하여야 합니다.

「개인정보의 안전성 확보조치 기준」 제8조(접속기록의 보관 및 점검)

① 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하여야 한다. 다만, 5만명 이상의 정보주체에 관하여 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다.

② 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 특히 개인정보를 다운로드한 것이 발견되었을 경우에는 내부관리 계획으로 정하는 바에 따라 그 사유를 반드시 확인하여야 한다.

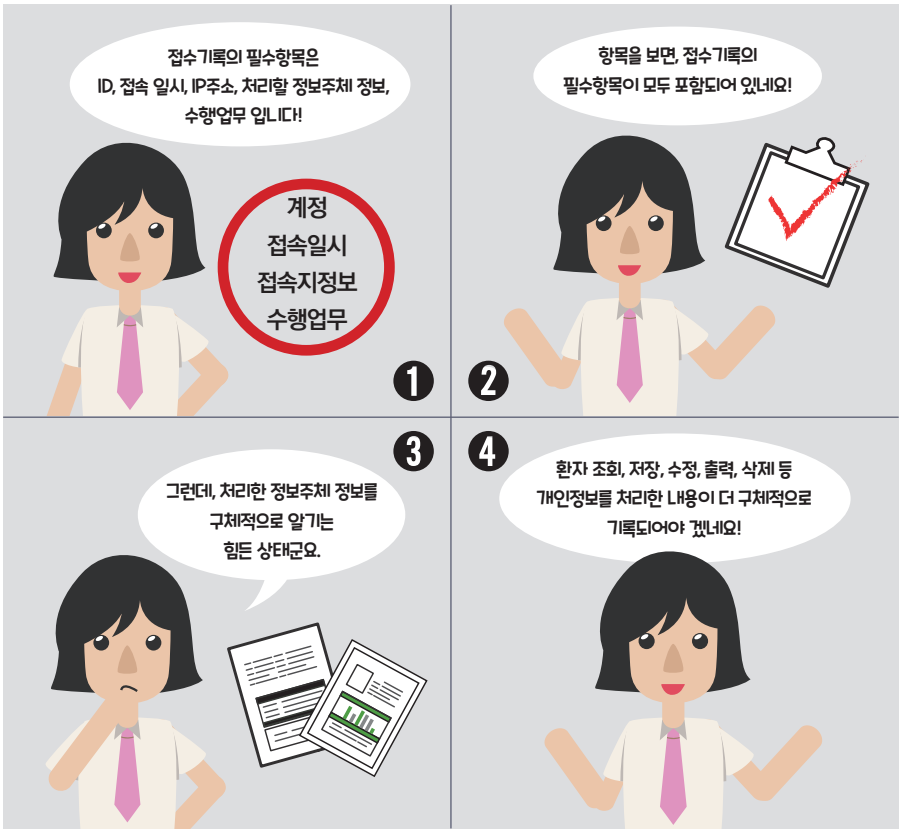
③ 개인정보처리자는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.

점검항목 **3.4.1**

Q27.

청구프로그램의 접속기록을 확인해 보니 아래와 같이 2년 이상 보관되고 있습니다. 잘 되고 있는 것인가요?

구분	접속자 ID	접속 일시	접속 IP	수행 업무
1	Admin	202X/01/01 09:00:00	192.168.0.1	Log in
2	Admin	202X/01/02 09:00:00	192.168.0.1	Log in
⋮	⋮	⋮	⋮	⋮



A.

접속기록의 필수항목(계정, 접속 일시, 접속지 정보, 수행 업무)에 더해 「개인정보의 안전성 확보조치 기준」에서는 처리한 정보주체 정보가 포함되어야 합니다. 환자 조회, 저장, 수정, 출력, 삭제 등 요양기관에서 환자의 개인정보를 처리한 내용이 더 구체적으로 기록되어야 합니다. 아울러, 고유식별정보 및 민감정보를 처리하는 요양기관의 접속기록 보관기간은 2년입니다.

「개인정보의 안전성 확보조치 기준」 제2조(정의)제19호

19. "접속기록"이란 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무내역에 대하여 개인정보취급자 등의 계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우 "접속"이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신이 가능한 상태를 말한다.

「개인정보의 안전성 확보조치 기준」 제8조(접속기록의 보관 및 점검)제1항

① 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하여야 한다. 다만, 5만명 이상의 정보주체에 관하여 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다.

Ⅳ.

요양기관 개인정보보호 상담사례

3. 개인정보의 보관

3.5 보안프로그램 설치운영

점검항목 **3.5.1**

Q28.

의료기관은 악성 프로그램 등을 방지·치료할 PC에 백신 프로그램 등을 설치하라고 하는데 무료 백신 프로그램을 설치해도 되나요?

A.

백신 프로그램의 유·무료 여부는 상관없으나 라이센스 정책(이용 약관, 사용권 계약서 등)을 점검해 보아야 합니다. 개인용으로는 무료로 이용가능하나 기업에서 이용할 경우 비용을 지불해야 하는 프로그램이 많이 있습니다. 이를 위반할 경우 「개인정보 보호법」이 아닌 「저작권법」에 의해 처벌을 받을 수도 있습니다.

[기업에서는 유료인 프로그램의 라이센스 정책 내용 예시]

제1조 소프트웨어 사용권

본 소프트웨어 제품에 대한 귀하의 권리는 사용기간 동안 사용할 수 있는 비독점적이고 양도 불가능한 권리를 말합니다. 귀하는 귀하가 비영리적이고 개인적인 용도로 사용하는 컴퓨터에 본 소프트웨어 제품의 무료 버전을 무상으로 설치해 비영리적이고 개인적인 목적으로 사용할 수 있습니다. 따라서 귀하는 본 소프트웨어 제품을 명리적인 목적이나 개인적인 것이 아닌 목적으로 사용할 수 없으며, 법인 등 단체에서 사용하는 컴퓨터 등 귀하가 개인적인 용도로 사용하지 아니하는 컴퓨터에는 본 소프트웨어 제품을 설치하거나 사용할 수 없습니다.

Tip. 심평원에서 제공하는 AOS 백신은 의료기관·약국에서 무료로 사용 가능합니다.

* 설치방법은 심평원 요양기관업무포털(biz.hira.or.kr) 내 'DUR자료실'을 참고하시면 됩니다.

Ⅳ.

요양기관 개인정보보호 상담사례

4. 개인정보의 이용·제공

4.1 개인정보의 이용

점검항목 **1.1.1**

Q29.

2개월 전, 개인사정으로 한의원을 폐업하였습니다. 최근 문제가 해결되어 한의원을 재개설하고자 합니다. 기존에 폐업했던 한의원에서 수집한 환자의 개인정보를 재개설한 한의원에서 진료목적으로 사용해도 괜찮을까요?

A.

동일한 대표자가 의원을 재개설할 경우 진료목적으로 수집한 환자의 개인정보는 진료목적으로 재이용할 수 있습니다. 하지만 홍보목적으로 환자의 개인정보를 이용하고 싶으시다면 개인정보 수집·이용 동의를 위한 필수항목(①개인정보 수집/이용 목적 ②수집하려는 개인정보의 항목 ③개인정보의 보유 및 이용기간 ④동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우 그 불이익의 내용)을 환자에게 알리고 동의를 받아야 합니다. 만일 대표자가 변경되어 재개설 할 경우 개인정보 양도에 해당되어 아래와 같이 개인정보 이전 사실을 환자에게 알려야 합니다.

「개인정보 보호법」 제27조(영업양도 등에 따른 개인정보의 이전 제한)제1항 환자에게 알려야할 사항
1. 개인정보를 이전하려는 사실
2. 개인정보를 이전받는 자의 성명(법인, 기관명), 주소, 전화번호 및 그 밖의 연락처
3. 정보주체가 개인정보의 이전을 원하지 아니하는 경우 조치할 수 있는 방법 및 절차

알리는 방법은 아래와 같습니다.

1. 서면, E-Mail, Fax, 전화, 문자전송 또는 이에 상당하는 방법
2. 개인정보를 이전하려는 의료기관의 과실 없이 서면 등에 따른 방법으로 통지사항을 정보주체에게 알릴 수 없는 경우에는 해당 사항을 인터넷 홈페이지에 30일 이상 게재하여야 합니다. 다만, 인터넷 홈페이지를 운영하지 않는 경우 기관 내 보기 쉬운 장소(접수대 등)에 30일 이상 게시하여야 합니다.

점검항목 **2.5.1**

Q30.

작년에 수탁업체 직원 및 내부 직원들에게 보안서약서를 작성하게 하였습니다. 보안서약서는 매년 갱신해야 하나요? 혹은 한 번만 받으면 되나요?

A.

보안서약서는 직원, 아르바이트 직원 등이 입사 시에 한 번 작성하는 것이 일반적이지만, 서약에 중요사항이 변경되었거나 의료기관 운영 정책에 따라 갱신하고 작성토록 할 수도 있습니다. 수탁업체의 경우 전담하는 담당자가 별도로 없거나 계속 바뀐다면 수탁업체 대표자의 보안서약서를 받거나 계약서에 해당내용을 추가하는 방법도 있습니다.

「개인정보 보호법」 제28조(개인정보취급자에 대한 감독)제1항

① 개인정보처리자는 개인정보를 처리함에 있어서 개인정보가 안전하게 관리될 수 있도록 임직원, 파견근로자, 시간제근로자 등 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 자에 대하여 적절한 관리·감독을 행하여야 한다.

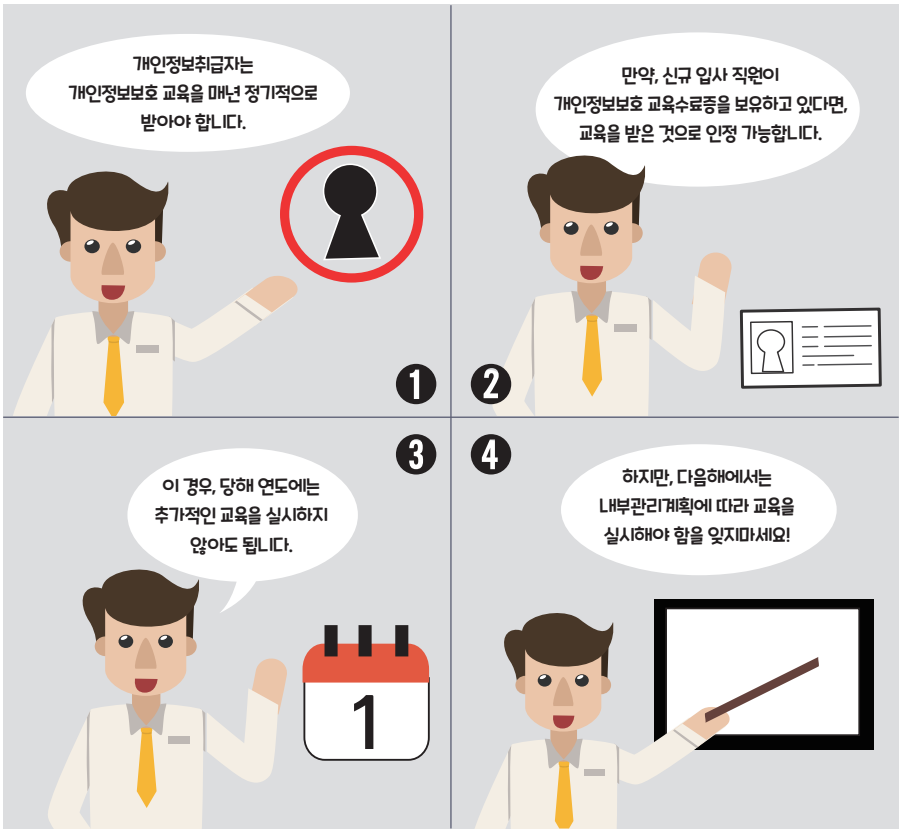
「표준 개인정보 보호지침」 제15조(개인정보취급자에 대한 감독)제3항

③ 개인정보처리자는 개인정보취급자에게 보안서약서를 제출하도록 하는 등 적절한 관리·감독을 해야 하며, 인사이동 등에 따라 개인정보취급자의 업무가 변경되는 경우에는 개인정보에 대한 접근권한을 변경 또는 말소해야 한다.

점검항목 **2.5.2**

Q31.

최근 입사한 직원은 이전 직장에서 개인정보보호 교육을 이수하였다고 합니다. 그렇다면 개인정보보호 책임자로서 직원에 대한 개인정보보호 교육을 따로 진행하지 않아도 될까요?



A.

개인정보취급자는 개인정보보호 교육을 매년 정기적으로 받아야 합니다. 신규 입사한 직원이 개인정보보호 교육을 이수하고 교육수료증을 보유하고 있다면, 개인정보보호 교육을 받은 것으로 인정할 수 있습니다. 따라서 당해 연도에는 추가적으로 교육을 실시하지 않으셔도 됩니다. 하지만 다음 해에는 내부관리계획 등에 따라 교육을 실시해야 합니다.

「개인정보 보호법」 제28조(개인정보취급자에 대한 감독)제2항
개인정보처리자는 개인정보의 적정한 취급을 보장하기 위하여 개인정보취급자에게 정기적으로 필요한 교육을 실시하여야 한다.

Ⅳ.

요양기관 개인정보보호 상담사례

4. 개인정보의 이용·제공

4.2 개인정보의 제공

점검항목 **1.3.1**

Q32.

보험회사에서 환자가 요구하는 보험금 지급과 관련하여 환자의 진료기록부 사본을 요구하는 경우가 종종 있습니다. 환자에게 별도 동의를 받아야 하나요?

A.

환자가 해당 보험회사 직원을 대리인으로 지정했음을 증빙하는 경우 「의료법」에 따라 해당 진료기록부 사본을 제공할 수 있습니다. 즉, 보험회사가 ① 보험회사 직원의 신분증 사본, ② 환자가 자필 서명한 동의서(만 14세 미만인 경우 환자의 법정대리인이 작성 및 가족관계증명서 등 증빙서류 첨부), ③ 환자가 자필 서명한 위임장 ④ 환자의 신분증 사본을 갖추어 요청하는 경우입니다.

단, **의료기관으로부터 청구를 받은 보험회사가 그 의료기관에 관계 진료기록의 열람을 청구하는 경우는 「자동차손해배상 보장법」에 따라 위 증빙서류를 환자의 확인 없이 제공할 수 있습니다.**

「개인정보 보호법」 제18조(개인정보의 목적 외 이용·제공 제한)제2항

② 제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다.

1. 정보주체로부터 별도의 동의를 받은 경우　　2. 다른 법률에 특별한 규정이 있는 경우

「의료법」 제21조(기록 열람 등)제3항제2호, 제9호

2. 환자가 지정하는 대리인이 환자 본인의 동의서와 대리권이 있음을 증명하는 서류를 첨부하는 등 보건복지부령으로 정하는 요건을 갖추어 요청한 경우
9. 「자동차손해배상 보장법」 제12조제2항 및 제14조에 따라 의료기관으로부터 자동차보험진료 수가를 청구 받은 보험회사 등이 그 의료기관에 대하여 관계 진료기록의 열람을 청구한 경우

점검항목 **2.4.1**

Q33.

치과의원에서 환자의 틀니 및 보철 치료를 위해 구강 모형(틀) 제작을 외부업체에 의뢰하고자 합니다. 개인정보보호 관련하여 계약서에 반드시 명시되어야 할 사항들이 있나요?

A.

환자의 구강 모형(틀)은 개인마다 달라 개인을 식별할 수 있는 개인정보라고 할 수 있습니다. 따라서 외부업체와 위탁업무 수행 목적 등 7개 항이 포함된 계약서를 작성해야 합니다.

☑ 표준 개인정보처리 위탁계약서 예시자료는 [첨부] ③ 참조

또한 위탁사실을 인터넷 홈페이지 또는 의료기관 내 환자들이 보기 쉬운 장소(안내판, 접수대 등)에 해당 외부업체의 명칭과 위탁 사실(위탁내용)을 공개해야 합니다.

「개인정보 보호법」 제26조(업무위탁에 따른 개인정보의 처리 제한)제1항, 제2항

① 개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서에 의하여야 한다.

1. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
2. 개인정보의 기술적·관리적 보호조치에 관한 사항
3. 그 밖에 개인정보의 안전한 관리를 위하여 대통령령으로 정한 사항

② 제1항에 따라 개인정보의 처리 업무를 위탁하는 개인정보처리자(이하 "위탁자"라 한다)는 위탁하는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자(이하 "수탁자"라 한다)를 정보주체가 언제든지 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.

점검항목 **2.4.1**

Q34.

한의원을 운영 중입니다. 타지에서 방문한 환자는 편의를 위해 한약 배송서비스를 택배로 진행하고 있습니다. 택배업체에 환자의 성명, 주소, 연락처 등 환자의 개인정보를 제공하는데 택배업체와 위탁계약을 진행해야 할까요?

A.

우편배달사업자나 인터넷서비스 제공자 등이 다른 사람의 개인정보를 단순히 전달 또는 전송하는 업무는 개인정보 이용에 해당되지 않습니다. 따라서 개인정보 처리 위탁계약서를 통해 계약하지 않으셔도 됩니다. 그러나 택배업체와 계약을 맺고 정기적으로 개인정보가 제공되는 배달 업무를 위탁하는 경우에는 개인정보 위탁 계약에 해당되므로 위탁계약서를 통해 택배업체와 계약을 맺으셔야 합니다.

☑ 표준 개인정보처리 위탁계약서 예시자료는 [첨부] ③ 참조

「개인정보 보호법」 제26조(업무위탁에 따른 개인정보의 처리 제한)제1항

① 개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서에 의하여야 한다.

1. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
2. 개인정보의 기술적·관리적 보호조치에 관한 사항
3. 그 밖에 개인정보의 안전한 관리를 위하여 대통령령으로 정한 사항

점검항목 **2.4.1**

Q35.

PC에서 문제가 발생하는 경우, PC 유지보수 업체 직원이 출장을 와서 PC를 고치면 출장 및 수리비를 지불하는 형식으로 진행합니다. 이러한 경우에도 PC안에 개인정보에 접근할 수 있기 때문에 개인정보 처리 위탁 계약서를 작성해야 하나요?

A.

계약기간 및 업체를 정해놓은 경우라면 개인정보 처리 위탁 계약서를 작성해야 하지만 그렇지 않은 경우에는 해당 업체 직원이 출장 방문 시 보안서약서 작성 등 간단한 교육을 실시하고 직원의 관리·감독 하에 PC 유지보수 업무를 할 수 있도록 하는 것이 바람직합니다.

☑ 표준 개인정보처리 위탁계약서 예시자료는 [첨부] ③ 참조

「개인정보 보호법」 제26조(업무위탁에 따른 개인정보의 처리 제한)제1항, 제4항

① 개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서에 의하여야 한다.

1. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
2. 개인정보의 기술적·관리적 보호조치에 관한 사항
3. 그 밖에 개인정보의 안전한 관리를 위하여 대통령령으로 정한 사항

④ 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.

Ⅳ.

요양기관 개인정보보호 상담사례

5. 개인정보의 파기

5.1 개인정보의 파기

점검항목 **1.5.1**

Q36.

진료기록부 보존기간은 10년으로 알고 있습니다. 하지만 치과의원의 경우 보철, 임플란트 등 지속적인 진료의 필요성으로 환자의 진료기록부를 10년 이상 보존해야 하는 경우가 많습니다. 이러한 경우 진료기록부 보존기간을 연장할 수 있을까요?

A.

「의료법」은 환자의 진료기록 보존기간을 10년으로 명시하고 있습니다. 또한, 계속적인 진료를 위해 진료기록 연장보관이 필요한 경우에는 1회에 한정하여 10년을 연장 보관할 수 있습니다.
다만, 보존 기간을 연장할 시에는 향후 증빙이 가능하도록 반드시 의료기관 내부 결재를 득하여 해당 서류를 보존하셔야 합니다.

법 근거	의료법(시행규칙 제15조)	약사법(법 29조, 30조)
기록물 (보존기간)	환자명부(5년), 진료기록부(10년), 처방전(2년, 건강보험 청구건 5년), 수술기록(10년), 검사소견기록(5년), 방사선 사진 및 그 소견서(5년), 간호기록부(5년), 조산기록부(5년), 진단서 등의 부본(3년)	처방전 (2년, 건강보험 청구건 3년), 조제기록부(5년)

「의료법 시행규칙」 제15조(진료기록부 등의 보존)제1항

① 의료인이나 의료기관 개설자는 법 제22조제2항에 따른 진료기록부 등을 다음 각 호에 정하는 기간 동안 보존하여야 한다. 다만, 계속적인 진료를 위하여 필요한 경우에는 1회에 한정하여 다음 각 호에 정하는 기간의 범위에서 그 기간을 연장하여 보존할 수 있다.

점검항목 **1.5.2**

Q37.

약국에서 보관중인 처방전 및 접수증 등 종이문서를 파기하고자 합니다. 손으로 찢거나 가위로 잘라서 휴지통에 버려도 괜찮을까요?

A.

환자의 개인정보가 담긴 접수증, 진료기록부 등을 파기할 때에는 복구 또는 재생이 불가능한 방법으로 파기해야 합니다. 가위나 손으로 찢어 쓰레기통에 버리는 것은 완벽히 복구 또는 재생이 불가능하다고 입증하기는 어려운 방법입니다. 파쇄기로 분쇄하거나 소각하는 방법 등으로 개인정보를 완전히 파기해야 합니다. 필요한 경우 외부 전문업체를 이용하여 파기하는 방법도 가능합니다.

개인정보보호법 제21조(개인정보의 파기)제1항, 제2항

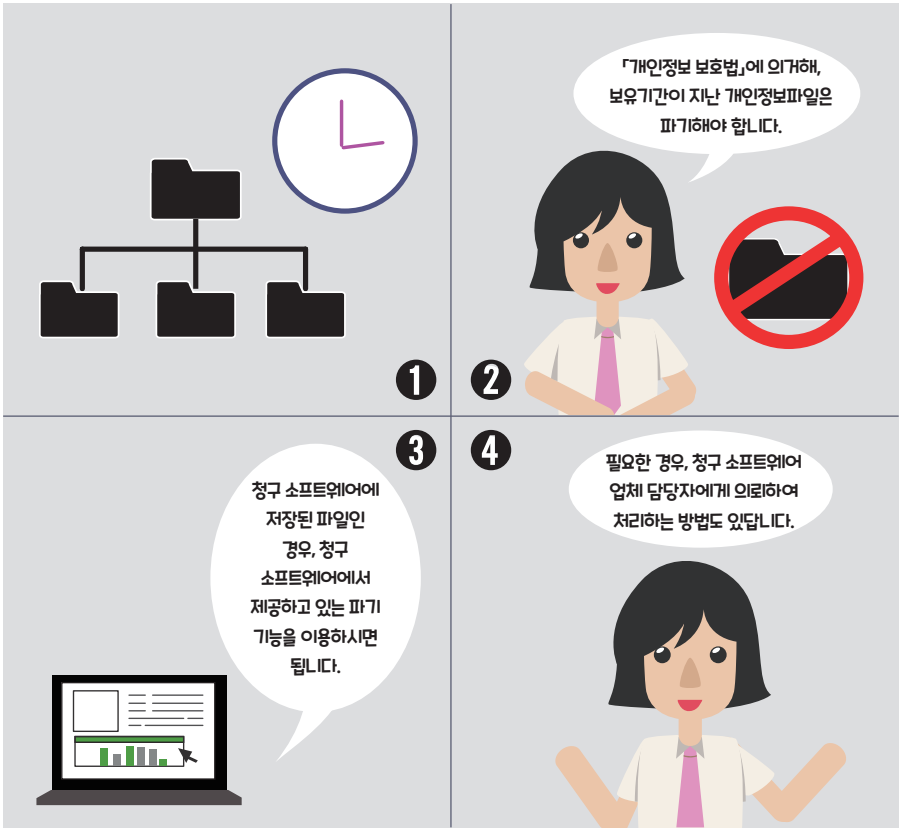
① 개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.

② 개인정보처리자가 제1항에 따라 개인정보를 파기할 때에는 복구 또는 재생되지 아니하도록 조치하여야 한다.

점검항목 **1.5.2**

Q38.

○○ 약국입니다. 한 달 후면 약국을 개설한지 3주년이 됩니다. 이에 따라, 그간 심평원에 심사·청구한 자료 중 PC에 남아 있는 청구파일 일부는 개인정보 보유기간 경과로 파기해야할 것 같습니다. 어떻게 파기해야 하나요?



A.

청구소프트웨어에 저장된 파일의 경우 청구소프트웨어에서 제공하고 있는 파기 기능을 사용하여 관리하시면 됩니다. **파기 시에는 복구 및 재생되지 않도록 개인정보를 완전 파기해야 합니다.** 필요한 경우 청구소프트웨어 업체 담당자에게 의뢰하여 처리하는 방법도 있습니다.

「표준 개인정보 보호지침」 제10조(개인정보의 파기방법 및 절차)제1항

① 개인정보처리자는 개인정보의 보유 기간이 경과하거나 개인정보의 처리 목적 달성, 해당 서비스의 폐지, 사업의 종료 등 그 개인정보가 필요하게 되었을 때에는 정당한 사유가 없는 한 그로부터 5일 이내에 그 개인정보를 파기하여야 한다.

「표준 개인정보 보호지침」 제11조(법령에 따른 개인정보의 보존)제1항, 제2항

① 개인정보처리자가 법 제21조제1항 단서에 따라 법령에 근거하여 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 물리적 또는 기술적 방법으로 분리하여서 저장·관리하여야 한다.

② 제1항에 따라 개인정보를 분리하여 저장·관리하는 경우에는 개인정보 처리방침 등을 통하여 법령에 근거하여 해당 개인정보 또는 개인정보파일을 저장·관리한다는 점을 정보주체가 알 수 있도록 하여야 한다.

점검항목 **1.5.2**

Q39.

약국에서 종이 처방전을 직접 파기하는 경우 증빙자료는 어떻게 준비해야 하나요?

A.

약국에서 직접 처방전을 파기하는 경우 복구 또는 재생되지 않도록 분쇄기로 분쇄하거나 소각하여 파기하며, 파기사실을 파기대장에 기록하시면 됩니다.

☑ 표준 개인정보처리 위탁계약서 예시자료는 [첨부] ④ 참조

「개인정보 보호법 시행령」 제16조(개인정보의 파기방법)제1항

① 개인정보처리자는 법 제21조에 따라 개인정보를 파기할 때에는 다음 각 호의 구분에 따른 방법으로 하여야 한다.

1. 전자적 파일 형태인 경우: 복원이 불가능한 방법으로 영구 삭제
2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우: 파쇄 또는 소각

「표준 개인정보 보호지침」 제10조(개인정보의 파기방법 및 절차)제1항, 제2항

① 개인정보처리자는 개인정보의 보유 기간이 경과하거나 개인정보의 처리 목적 달성, 해당 서비스의 폐지, 사업의 종료 등 그 개인정보가 불필요하게 되었을 때에는 정당한 사유가 없는 한 그로부터 5일 이내에 그 개인정보를 파기하여야 한다.

② 영 제16조제1항제1호의 '복원이 불가능한 방법'이란 현재의 기술수준에서 사회통념상 적정한 비용으로 파기한 개인정보의 복원이 불가능하도록 조치하는 방법을 말한다.

③ 개인정보처리자는 개인정보의 파기에 관한 사항을 기록·관리하여야 한다.

④ 개인정보 보호책임자는 개인정보 파기 시행 후 파기 결과를 확인하여야 한다.

Ⅳ.

요양기관 개인정보보호 상담사례

6. 영상정보처리기기(CCTV)

6.1 영상정보처리기기 설치·운영

점검항목 **2.3.2**

Q40.

접수실과 복도에 CCTV를 설치하고 있습니다. 설치 안내판을 부착해야 한다고 들었는데 CCTV 설치 장소마다 안내판을 설치해야 하나요?

A.

건물 내 여러 장소에 CCTV를 설치하는 경우 해당 건물 또는 장소 전체가 CCTV 설치 구역임을 알리는 안내판을 환자가 의료기관 진입 시 쉽게 확인할 수 있는 곳에 설치하면 됩니다. 안내판에는 ①CCTV 설치 목적 및 장소, ②촬영 범위 및 시간, ③관리책임자 성명 및 연락처, ④(CCTV 설치·운영을 위탁한 경우) 수탁자의 명칭 및 연락처를 기재해야 합니다.

☑ CCTV 설치 안내판 예시자료는 [첨부] ⑤ 참조

「개인정보 보호법」 제25조(영상정보처리기기의 설치·운영 제한)제4항

④ 제1항 각 호에 따라 영상정보처리기기를 설치·운영하는 자는 정보주체가 쉽게 인식할 수 있도록 다음 각 호의 사항이 포함된 안내판을 설치하는 등 필요한 조치를 하여야 한다.

1. 설치 목적 및 장소
2. 촬영 범위 및 시간
3. 관리책임자 성명 및 연락처
4. 그 밖에 대통령령으로 정하는 사항

「개인정보 보호법 시행령」 제24조(안내판의 설치 등)제1항

① 법 제25조제1항 각 호에 따라 영상정보처리기기를 설치·운영하는 자는 영상정보처리기기가 설치·운영되고 있음을 정보주체가 쉽게 알아볼 수 있도록 같은 조 제4항 각 호의 사항이 포함된 안내판을 설치하여야 한다. 다만, 건물 안에 여러 개의 영상정보처리기기를 설치하는 경우에는 출입구 등 잘 보이는 곳에 해당 시설 또는 장소 전체가 영상정보처리기기 설치지역임을 표시하는 안내판을 설치할 수 있다.

점검항목 **2.3.2**

Q41.

치과병원을 운영하고 있습니다. 환자와의 분쟁 발생, 도난 등에 대비하여 진료실에 CCTV를 설치하여 운영하고 있습니다. CCTV촬영 시 환자의 별도 동의를 받아야 하나요?

A.

공개된 장소(도로, 공원, 광장, 지하철역 등)에서는 범죄의 예방 및 수사를 목적으로 CCTV 설치가 가능합니다. 하지만 치과병원(의료기관)의 진료실, 수술실 등은 불특정 다수가 출입할 수 있는 공개된 장소가 아닙니다. 그러므로 CCTV를 설치하여 영상을 촬영하기 위해서는 진료실에 출입하는 환자의 별도 동의를 받은 후 촬영해야 합니다. 또한 환자가 촬영에 동의하지 않는다 하더라도 진료를 거부할 수 없으므로 주의하셔야 합니다.

「개인정보 보호법」 제25조(영상정보처리기기의 설치·운영 제한)제1항, 제2항

① 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 영상정보처리기기를 설치·운영하여서는 아니 된다.

1. 법령에서 구체적으로 허용하고 있는 경우
2. 범죄의 예방 및 수사를 위하여 필요한 경우
3. 시설안전 및 화재 예방을 위하여 필요한 경우

② 누구든지 불특정 다수가 이용하는 목욕실, 화장실, 발한실(發汗室), 탈의실 등 개인의 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있도록 영상정보처리기기를 설치·운영하여서는 아니 된다. 다만, 교도소, 정신보건 시설 등 법령에 근거하여 사람을 구금하거나 보호하는 시설로서 대통령령으로 정하는 시설에 대하여는 그러하지 아니하다.

점검항목 **2.3.2**

Q42.

CCTV 구입 및 유지비용이 만만치 않아 휴대폰 카메라나 캠코더를 활용하려고 합니다. CCTV를 대체해서 이러한 기기를 사용하려면 어떻게 해야 하나요?

A.

휴대폰 카메라, 개인 캠코더, CAM 등을 CCTV 용도로 활용할 경우에도 CCTV 안내판 설치 등 개인정보보호법상 의무를 다하여야 합니다. 또한 위 기기의 동영상 촬영 기능을 그대로 이용할 경우 소리까지 기록될 수 있으므로 녹음기능은 반드시 끄고 사용해야 합니다.

「개인정보 보호법」 제2조(정의)제7호

이 법에서 사용하는 용어의 뜻은 다음과 같다.

7. "영상정보처리기기"란 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 대통령령으로 정하는 장치를 말한다.

「개인정보 보호법」 제25조(영상정보처리기기의 설치·운영 제한)제5항

⑤ 영상정보처리기기운영자는 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비춰서는 아니 되며, 녹음기능은 사용할 수 없다.

점검항목 **2.3.2**

Q43.

약국 내부에 설치된 CCTV가 실시간 촬영만 되고 영상은 저장되지 않습니다. CCTV와 관련한 사항을 점검해야 하나요?

A.

촬영만 되는 CCTV라 하더라도 영상정보처리기기의 운영·관리 방침에 준하여 관리해야 합니다. 따라서 CCTV 설치 안내판, 영상정보처리기기 운영·관리방침 등을 수립하여 공개하시고, 영상이 저장되지 않기 때문에 열람, 보관 등의 사항은 별도로 제외하면 됩니다.

「개인정보 보호법 시행령」 제25조(영상정보처리기기의 운영·관리 방침)제1항

① 영상정보처리기기운영자는 법 제25조제7항에 따라 다음 각 호의 사항이 포함된 영상정보처리기기 운영·관리 방침을 마련하여야 한다.

1. 영상정보처리기기의 설치 근거 및 설치 목적
2. 설치 대수, 설치 위치 및 촬영 범위
3. 관리책임자, 담당 부서 및 영상정보에 대한 접근 권한이 있는 사람 (수탁자 포함)
4. 영상정보의 촬영시간, 보관기간, 보관 장소 및 처리방법
5. 영상정보처리기기 운영자의 영상정보 확인 방법 및 장소
6. 정보주체의 영상정보 열람 등 요구에 대한 조치
7. 영상정보 보호를 위한 기술적·관리적 및 물리적 조치
8. 그 밖에 영상정보처리기기의 설치·운영 및 관리에 필요한 사항

점검항목 **2.4.1**

Q44.

CCTV 업체가 상시적으로 위탁업무를 처리하지 않는 경우 보안서약서만 받아도 될 것 같은데 반드시 위·수탁계약서가 필요한가요?

A.

수탁자가 상시적으로 위탁업무를 처리하지 않는 경우에도 위·수탁 계약서를 체결해야 하며, 위탁업무 발생 시 보안서약서 등을 확보해 놓아야 합니다.

☑ 표준 개인정보처리 위탁계약서 예시자료는 [첨부] ③ 참조

「개인정보 보호법」 제26조(업무위탁에 따른 개인정보의 처리 제한)제1항

① 개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서에 의하여야 한다.

1. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
2. 개인정보의 기술적·관리적 보호조치에 관한 사항
3. 그 밖에 개인정보의 안전한 관리를 위하여 대통령령으로 정한 사항

[첨부]요양기관 구비 법정서식

❶ 개인정보 처리방침(예시)

【 개인정보 처리방침 】

OO 의원/약국(이하 "A"이라 함)은 귀하의 개인정보보호를 매우 중요시하며, 『개인정보 보호법』을 준수하고 있습니다. A는 개인정보 처리방침을 통하여 귀하께서 제공하시는 개인정보가 어떠한 용도와 방식으로 이용되고 있으며 개인정보보호를 위해 어떠한 조치가 취해지고 있는지 알려드립니다.

이 개인정보 처리방침의 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 공지의무

1. 수집하는 개인정보의 항목 및 수집방법

A는 환자의 진료와 관련하여 필요한 개인정보와 건강보험급여 청구에 필요한 최소한의 개인정보만을 수집합니다.

- 수집항목: 성명, 주민등록번호, 주소, 연락처, (관련내용 등)
- 수집방법: 「OO법」(의료법, 약사법)에 의해 개인정보가 포함된 문서명(처방전, 진료정보 등)을 접수(정보주체의 별도 동의 없이 수집 가능)

2. 개인정보의 수집 및 이용목적

수집하는 개인정보는 「의료법」, 「약사법」, 「국민건강보험법」에 따른 업무(처방전의 보관 진료정보의 보관 등), 건강보험급여의 청구에만 사용하며 이용 목적이 변경될 시에는 사전 동의를 구할 것입니다.

3. 개인정보의 보유 및 이용기간 및 파기절차 및 파기방법

「의료법」, 「약사법」, 「국민건강보험법」에서 정한 보유기간 동안 개인정보를 보유하며 그 이후는 지체 없이 파기합니다.

- 보유기간: 처방전 2년(요양급여비용을 청구한 처방전은 3년), 건강보험청구 관련 자료 5년 (법령기간)
  환자명부 5년, 진료기록부 10년, 처방전 2년, 수술기록 10년, 검사소견기록 5년,
  방사선 사진 및 그 소견서 5년, 간호기록부 5년, 조산기록부 5년, 진단서 등의 부본 3년
- 파기절차: 법정 보유기간 후 파기방법에 의하여 파기
- 파기방법: 전자적 파일형태로 저장된 개인정보는 기록을 재생할 수 없는 기술적 방법을 사용하여 삭제하고 종이에 출력된 처방전은 분쇄기로 분쇄하거나 소각하여 파기

4. 이용자 및 법정대리인의 권리와 그 행사방법

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

A에서 법에 따라 의무적으로 보관하고 있는 처방전, 건강보험청구 관련 자료는 이용자의 요청이 있더라도 법에서 정한 기간 동안은 변경, 삭제할 수 없습니다.

5. 개인정보의 제3자 제공

A는 건강보험심사평가원에 요양급여비용 청구를 위해 진료기록을 제출합니다.

※「국민건강보험법」에 의해 의무적으로 제출하는 사항이므로 별도의 제공 동의 불필요

6. 개인정보 처리의 위탁

개인정보를 정보시스템을 통해 관리하기 위해 다음의 회사에 개인정보를 위탁하고 있습니다.

- 청구프로그램(업무 및 기록의 전산관리): 프로그램명, 회사명(연락처) 기입
- 폐기: 업체명(연락처) 기입
- CCTV: 업체명(연락처) 기입

7. 개인정보 보호책임자

소속	성명	전화번호	메일
A	홍길동	00-000-0000	webmaster@oo.co.kr

8. 개인정보의 안전성 확보조치

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

또한 A는 이용자의 개인정보보호를 위한 관리적 대책으로서 이용자의 개인정보에 대한 접근 및 관리에 필요한 절차를 마련하고, 이용자의 개인정보를 처리하는 인원을 최소한으로 제한하고 개인정보를 처리하는 시스템의 사용자 비밀번호를 정기적으로 갱신하여 안전하게 관리합니다.

9. 정책 변경에 따른 공지의무

이 개인정보 처리방침은 202X년 X월 XX일에 제정되었으며 법령·정책 또는 보안기술의 변경에 따라 내용의 추가·삭제 및 수정이 있을 시에는 변경되는 개인정보 처리방침을 시행하기 최소 7일전 홈페이지 또는 접수창구에 변경이유 및 내용 등을 공지하도록 하겠습니다.

공고일자: 년 월 일
시행일자: 년 월 일

〈참고〉 제정일자/공고일자/시행일자: 2012년 3월 30일 이후 날짜로 기입
※ 본 서식은 요양기관의 업무현황에 맞게 수정하여 사용할 수 있음

❷ 통제구역 출입관리대장(예시)

출 입 관 리 대 장						
날짜	방문자		시간		방문목적	확인자
	회사명	성명	입실시간	퇴실시간		
2021.1.1.	요양기관	홍길동	10:00	18:00	A/S	홍길동

※ 위의 서식을 참고하여 요양기관의 환경에 맞게 수정 가능함

❸ 표준 개인정보처리위탁 계약서(예시)

※ 계약 체결 시, 관련 법 조항의 변경사항 유무 등 확인 필요

본 표준 개인정보처리위탁 계약서는 「개인정보 보호법」제26조제1항에 따라 위탁계약에 있어 개인정보 처리에 관하여 문서로 정하여야 하는 최소한의 사항을 표준적으로 제시한 것으로서, 위탁계약이나 위탁업무의 내용 등에 따라 세부적인 내용은 달라질 수 있습니다.
개인정보처리업무를 위탁하거나 위탁업무에 개인정보 처리가 포함된 경우에는 본 표준 개인정보처리위탁 계약서의 내용을 위탁계약서에 첨부하거나 반영하여 사용하실 수 있습니다.

표준 개인정보처리위탁 계약서

OOO(이하 "갑"이라 한다)과 △△△(이하 "을"이라 한다)는 "갑"의 개인정보 처리업무를 "을"에게 위탁함에 있어 다음과 같은 내용으로 본 업무위탁계약을 체결한다.

제1조 (목적) 이 계약은 "갑"이 개인정보처리업무를 "을"에게 위탁하고, "을"은 이를 승낙하여 "을"의 책임아래 성실하게 업무를 완성하도록 하는데 필요한 사항을 정함을 목적으로 한다.

제2조 (용어의 정의) 본 계약에서 별도로 정의되지 아니한 용어는「개인정보 보호법」, 같은 법 시행령 및 시행규칙,「개인정보의 안전성 확보조치 기준」(보호위원회 고시 제2020-2호) 및「표준 개인정보 보호지침」(보호위원회 고시 제2020-1호)에서 정의된 바에 따른다.

제3조 (위탁업무의 목적 및 범위) (예시 1) "을"은 계약이 정하는 바에 따라 개인정보처리시스템(청구 S/W)을 다음과 같은 개인정보 처리 업무를 수행한다.[1)]

1. 개인정보의 암호화 2. 프로그램의 유지보수

제4조 (재위탁 제한) ① "을"은 "갑"의 사전 승낙을 얻은 경우를 제외하고 "갑"과의 계약상의 권리와 의무의 전부 또는 일부를 제3자에게 양도하거나 재위탁할 수 없다.
② "을"이 다른 제3의 회사와 수탁계약을 할 경우에는 "을"은 해당 사실을 계약 체결 7일 이전에 "갑"에게 통보하고 협의하여야 한다.

제5조 (개인정보의 안전성 확보조치) "을"은「개인정보 보호법」제23조제2항 및 제24조제3항 및 제29조, 같은 법 시행령 제21조 및 제30조,「개인정보의 안전성 확보조치 기준」(보호위원회 고시 제2020-2호)에 따라 개인정보의 안전성 확보에 필요한 관리적·기술적 조치를 취하여야 한다.

제6조 (개인정보의 처리제한) ① "을"은 계약기간은 물론 계약 종료 후에도 위탁업무 수행 목적 범위를 넘어 개인정보를 이용하거나 이를 제3자에게 제공 또는 누설하여서는 안 된다.
② "을"은 계약이 해지되거나 또는 계약기간이 만료된 경우 위탁업무와 관련하여 보유하고 있는 개인정보를「개인정보 보호법」시행령 제16조 및「개인정보의 안전성 확보조치 기준」(보호위원회 고시 제2020-2호)에 따라 즉시 파기하거나 "갑"에게 반납하여야 한다.

1) 각호의 업무 예시: 고객만족도 조사 업무, 회원가입 및 운영 업무, 사은품 배송을 위한 이름, 주소, 연락처 처리 등

③ 제2항에 따라 “을”이 개인정보를 파기한 경우 지체없이 “갑”에게 그 결과를 통보하여야 한다.

제7조 (수탁자에 대한 관리·감독 등) ① 다음 각 호의 사항을 관리하도록 요구할 수 있으며, “을”은 특별한 사유가 없는 한 이에 응하여야 한다.

1. 개인정보의 처리 현황
2. 개인정보의 접근 또는 접속현황
3. 개인정보 접근 또는 접속 대상자
4. 목적외 이용·제공 및 재위탁 금지 준수여부
5. 암호화 등 안전성 확보조치 이행여부
6. 그 밖에 개인정보의 보호를 위하여 필요한 사항

② “갑”은 “을”에 대하여 제1항 각 호의 사항에 대한 실태를 점검하여 시정을 요구할 수 있으며, “을”은 특별한 사유가 없는 한 이행하여야 한다.

③ “갑”은 처리위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 1년에 ( )회 “을”을 교육할 수 있으며, “을”은 이에 응하여야 한다.[2)]

④ 제1항에 따른 교육의 시기와 방법 등에 대해서는 “갑”은 “을”과 협의하여 시행한다.

제8조 (손해배상) ① “을” 또는 “을”의 임직원 기타 “을”의 수탁자가 이 계약에 의하여 위탁 또는 재위탁받은 업무를 수행함에 있어 이 계약에 따른 의무를 위반하거나 “을” 또는 “을”의 임직원 기타 “을”의 수탁자의 귀책사유로 인하여 이 계약이 해지되어 “갑” 또는 개인정보주체 기타 제3자에게 손해가 발생한 경우 “을”은 그 손해를 배상하여야 한다.

② 제1항과 관련하여 개인정보주체 기타 제3자에게 발생한 손해에 대하여 “갑”이 전부 또는 일부를 배상한 때에는 “갑”은 이를 “을”에게 구상할 수 있다.

본 계약의 내용을 증명하기 위하여 계약서 2부를 작성하고, “갑”과 “을”이 서명 또는 날인한 후 각 1부씩 보관한다

20 . . .

갑	을
○○시 ○○구 ○○동 ○○번지	○○시 ○○구 ○○동 ○○번지
성 명: (인)	성 명: (인)

2) 「개인정보 안전성 확보조치 기준 고시」(보호위원회 고시 제2020-2호) 및 「개인정보 보호법」 제26조에 따라 위탁자는 수탁자에 대해서 교육을 의무적으로 시행하여야 한다. 이때 수탁자는 개인정보를 취급하는 소속 직원으로 본다.

❹ 개인정보 파기 관리대장(예시)

개인정보 파기 관리대장

번호	개인정보 파일명	자료의 종류	생성일	폐기일	폐기사유	처리담당자	처리부서장
1	환자 종이 청구 정보	종이처방전	2011.9.8.	2021.9.8.	보존기간 경과	○○○	홍길동
2	환자 조제 내역 정보	전산데이터	2011.3.12.	2021.3.12.	보존기간 경과	○○○	홍길동

❺ CCTV 설치 안내판(예시)

CCTV 설치 안내

- **설치목적**: 범죄예방 및 시설안전
- **설치장소**: 건물 출입문
- **촬영범위**: 50M 전방향
- **촬영시간**: 24시간
- **관리책임자**: OO과 홍길동 (02-OOO-OOOO)

(설치·운영을 위탁한 경우)

- 위탁관리자: OO업체 박길동 (02-OOO-OOOO)

건강보험심사평가원
HEALTH INSURANCE REVIEW & ASSESSMENT SERVICE

26465 강원도 원주시 혁신로 60(반곡동)
Tel. 1644-2000
www.hira.or.kr