2025년도

요양기관 개인정보 자율보호 표준가이드

2025. 5.

개인정보 보호 자율규제 전문기관

건강보험심사평가원

목 차

지표별 가이드

I. 개인정보의 처리

1.1.1 진료(조제, 복약지도 포함) 목적 외로 서면(오프라인) 및 홈페이지(온라인) 등을 통한 개인정보 수집 시 정보주체의 동의를 받고 있는가? 5

1.1.2 진료(조제, 복약지도 포함) 목적 외로 만 14세 미만 아동의 개인정보를 수집 · 처리 시, 법정대리인의 동의를 받았는가? 8

1.2.1 목적에 필요한 최소한의 개인정보만 수집하고 있는가? 10

1.2.2 최소한의 개인정보 수집 외에 선택정보에 대한 미동의를 이유로 재화 또는 부가 서비스 제공을 거부하고 있지 않은가? 11

1.2.3 개인정보 수집 시 목적에 따라 구분하여 동의를 받고 있는가? 12

1.3.1 개인정보를 수집 목적 외 이용하거나 제3자에게 제공하는 경우 정보주체에게 별도의 동의를 받고 있거나 법적 근거가 있는가? 13

1.4.1 개인정보의 보유기간 경과, 처리목적 달성 등 파기 시점이 도달한 때에 지체 없이 파기하고 있는가? 15

1.4.2 타 법령(전자상거래법, 형사소송법, 민사소송법 등)에 따라 개인정보를 파기하지 않고 보존하는 경우 별도로 분리하여 보관하고 있는가? 17

II. 개인정보의 처리 제한

2.1.1 진료(조제, 복약지도 포함) 목적 외로 민감정보를 수집할 경우, 별도 동의를 받고 있는가? 20

2.2.1 주민등록번호를 처리(수집·이용·보관 등)함에 있어 법령의 근거가 있는가? 21

2.2.2 여권번호, 운전면허번호, 외국인등록번호를 처리(수집·이용·보관 등)함에 있어 법령의 근거 또는 정보주체의 동의가 있는가? 23

2.3.1 고정형 또는 이동형 영상정보처리기기 운영·관리방침을 수립 및 공개하고 있는가? 25

2.3.2 고정형 영상정보처리기기를 설치한 장소에 정보주체가 해당 기기의 설치 사실을 인지할 수 있도록 필수기재 사항을 포함한 안내판을 설치하고 있는가? 26

2.3.3 고정형 또는 이동형(자율주행 자동차, 드론 등) 영상정보처리기기에 대한 이용 · 제공 · 열람 · 파기 내역을 기록하고 관리하고 있는가? 28

2.3.4 고정형 또는 이동형 영상정보처리기기의 안전성 확보조치를 하고 있는가? 30

2.3.5 이동형 영상정보처리기기로 촬영을 하는 경우 촬영 사실을 알리고 있는가? 32

2.4.1 업무 위탁 시 개인정보 처리 관련 필수사항 등을 계약서(문서)에 포함하였는가? 34

2.4.2 위탁에 관한 사실을 홈페이지 또는 사보, 접수실, 대기실 등에 공개하고 있는가? 35

2.4.3 수탁업체에 대한 관리 감독을 실시하고 있는가? 36

2.5.1 개인정보취급자에 대한 보안서약서를 징구하였는가? 37

2.5.2 개인정보취급자에 대한 정기적인 교육은 실시하고 있는가? 38

2.6.1 개인정보 처리방침을 알기 쉽게 작성하고 보기 쉬운 곳(홈페이지, 접수대, 대기실 등)에 공개하고 있는가? 39

2.7.1 개인정보 보호책임자를 지정하여 개인정보 보호 총괄 업무를 수행하고 있는가? 42

2.7.2 개인정보 유출 등 발생에 대비한 대응절차를 숙지하고 있는가? 44

2.8.1 개인정보 유출 등 발생 시 손해배상책임 이행이 보장될 수 있도록 보험 등에 가입하거나 준비금을 적립하고 있는가? 47

III. 개인정보의 안전한 관리

3.1.1 개인정보의 안전한 처리를 위한 내부 관리계획을 수립·시행 및 점검을 하고 있는가? 51

3.2.1 개인정보처리시스템에 (전자차트, 청구S/W 등) 대한 접근 권한을 업무수행에 필요한 최소한의 범위로 업무 담당자에게 차등 부여하고 있는가? 53

3.2.2 개인정보취급자 또는 개인정보취급자의 업무 변경 시, 지체 없이 개인정보처리시스템에 대한 접근 권한을 변경 또는 말소하고 있는가? 54

3.2.3 개인정보처리시스템(전자차트, 청구S/W 등) 접근 권한의 부여·변경·말소 내역 등을 최소 3년간 보관하고 있는가? 55

3.2.4 개인정보취급자별로 개인정보처리시스템에 대한 사용자계정(ID)을 발급하고 해당 사용자계정을 다른 개인정보취급자 등과 공유하고 있지는 않는가? 56

3.2.5 개인정보취급자 또는 정보주체의 비밀번호 등 인증수단을 안전하게 적용하고 관리하고 있는가? 57

3.2.6 개인정보취급자 또는 정보주체가 일정 횟수 이상 인증에 실패한 경우, 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 조치를 하고 있는가? 58

3.3.1 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하고 있는가? 59

3.3.2 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 접속한 IP주소 등을 분석하여 개인정보 유출시도를 탐지 및 대응하고 있는가? 60

3.3.3 외부에서 개인정보취급자가 정보통신망을 통해 개인정보처리시스템에 접속 시, 인증서, 보안토큰, 일회용비밀번호 등 안전한 인증수단을 적용하고 있는가? 62

3.3.4 개인정보가 인터넷 홈페이지, P2P, 공유설정 등으로 유출되지 않도록 개인정보처리시스템, 개인정보취급자 컴퓨터 등에 접근통제 조치를 하고 있는가? 63

3.3.5 홈페이지의 개인정보 노출 방지를 위한 보안 조치를 실시하고 있는가? 64

3.3.6 일정시간 이상 업무처리를 하지 않을 시 자동으로 시스템 접속이 차단되도록 하고 있는가? 65

3.3.7 업무용 모바일 기기의 분실・도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하고 있는가? 66

3.3.8 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근 권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등에 대하여, 인터넷망 차단 조치를 하고 있는가? 67

3.4.1 개인정보처리시스템에 고유식별정보, 비밀번호 및 생체인식정보를 저장하는 경우, 안전한 알고리즘으로 암호화 조치를 하고 있는가? 69

3.4.2 개인정보를 정보통신망을 통하여 인터넷망 구간으로 송・수신하는 경우 안전한 알고리즘에 의한 암호화 조치를 하고 있는가? 71

3.4.3 컴퓨터, 모바일 기기, 보조저장매체 등에 고유식별정보, 비밀번호 및 생체인식정보를 저장하는 경우, 안전한 알고리즘으로 암호화 조치를 하고 있는가? 72

3.4.4 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차 수립하였는가? 73

3.5.1 개인정보취급자가 개인정보처리시스템에 접속한 식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행한 업무내용 등이 포함된 접속기록을 2년 이상 보관·관리하고 있는가? 74

3.5.2 개인정보의 오·남용, 분실, 도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록, 다운로드가 확인된 경우 사유 확인 등을 월 1회 이상 점검하고 있는가? 76

3.6.1 악성 프로그램을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영 및 최신의 상태로 유지하고 있는가? 77

3.7.1 개인정보 등 중요자료가 보관된 물리적 장소에 대한 출입 통제 절차를 수립하여 운영하고 있는가? 78

3.7.2 개인정보가 포함된 종이 인쇄물, 개인정보가 복사된 외부 저장매체 등 개인정보의 출력・복사물을 안전하게 관리하기 위해 필요한 안전조치를 하였는가? 79

3.8.1 재해·재난 발생 시, 개인정보의 손실·훼손 등을 방지하기 위하여 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응 절차를 마련하고 있는가? 81

표준가이드 변경 이력

연번	일자	주요내용	비고
1	2015.	▪ 최초 작성	
2	2020. 2.	▪ (3.2.10) 업무용 모바일 기기 비밀번호 설정 ⇒ (3.2.3) 안전한 비밀번호 작성규칙 적용으로 통합 ▪ (3.8.2) 전담조직, 적정인력 운영 (3.8.4) 필요예산 반영 ⇒ (3.8.1) 개인정보 보호책임자 역할 정의로 통합 * (3.8.3) 개인정보 보호책임자 관리·감독 → (3.8.2) 변경 ▪ (3.2.7) 홈페이지 노출진단 서비스 내용 삭제 ▪ (3.4.1) 접속기록 2년 이상 보관, 기록항목 추가 등 * 「개인정보의 안전성 확보조치 기준」('19.6.7.) 개정사항 반영 ▪ 용어·서식 표준화, 기타 내용 현행화(파란색 표시)	(삭제) 3.2.10 3.8.2 3.8.4
3.	2020. 11.	▪ 「개인정보 보호법」 통합 및 개인정보보호위원회(이하 '보호위원회') 출범(8.5.) 등 변경사항 반영 ▪ 항목번호 1.1.3 → 1.1.2로 변경 ▪ 항목 증빙자료 명확화 및 인쇄물 제작에 따른 뒷표지 추가	(삭제) 1.1.3
4	2022. 11.	▪ 항목번호 1.5. → 1.4 로 변경(개인정보의 파기) ▪ 개인정보보호위원회 표준 개인정보 보호지침 반영 (별지 양식, 라벨링 등) ▪ 사전질문 변경(청구SW 점검 연계, 3.3.3 추가) ▪ 점검기준, 증빙자료, 근거규정 보완 및 지표설명 일반화	
5	2023. 4.	▪ (3.3.6) 암호 키 항목 추가 ▪ (3.6.2) 용어 변경	
6	2024. 1.	▪ 개정 개인정보 보호법(법률 제19234호) 반영 ▪ 개인정보 보호법 시행령 일부개정령(안) 반영 ▪ 개인정보의 안전성 확보조치 기준(고시 제2023-6호) 반영	
7	2024. 7.	▪ 표준 개인정보 보호지침(고시 제2024-1호) 반영 ▪ 항목번호 3.2.1 대상 확대(안전성 확보조치 기준) ▪ 항목번호 3.7.1, 3.7.2 → 3.7.1 통합 ▪ 항목번호 3.8.1, 3.8.2 → 3.8.1 통합	
8	2025. 5.	▪ 전면개정(개인정보보호위원회 「고유식별정보 안전조치 관리실태 점검」 관리항목 등 일괄 반영)	

지표별 가이드

사전 질문

필수 항목

Ⅰ. 개인정보의 처리

1.1. 개인정보의 수집·이용

1.2. 개인정보의 수집 제한

1.3. 개인정보의 제공

1.4. 개인정보 파기

개인정보 보호 자율점검 사전질문 항목

사 전 질 문 항 목	항목 번호	답변처리	
		예	아니오
1. 진료(조제, 복약지도 포함) 목적 외로 개인정보를 수집 및 이용(홍보용 SMS 발송 등) 하고 있습니까?	1.1.1 1.1.2 1.2.1 1.2.2 1.2.3 2.1.1 2.2.1 2.2.2	응답 필수	해당 없음
2. 영상정보처리기기를 설치, 운영하고 있습니까?	2.3.1 2.3.2 2.3.3 2.3.4 2.3.5	응답 필수	해당 없음
3. 개인정보를 수집하는(회원가입 등) 홈페이지를 보유 또는 운영하고 있습니까?	3.3.5 3.4.2	응답 필수	해당 없음
4. 청구 S/W를 제외하고 개인정보를 수집·이용·처리하는 시스템을 운영하고 있습니까?	3.2.5 3.2.6 3.3.1 3.3.2 3.3.8	응답 필수	해당 없음
5. 5만 명 이상 정보주체의 고유식별정보를 보유하고 있습니까?	3.1.1 3.2.3 3.3.3 3.3.6 3.4.3 3.5.1 3.5.2 3.6.1	증빙 필수	–

※ 사전질문에 해당되지 않는 문항은 모두 응답이 필요합니다. (양호/미흡)

개인정보 자율보호 표준가이드 필수 항목

항목번호	항 목
1.4.1	개인정보의 보유기간 경과, 처리목적 달성 등 파기 시점이 도달한 때에 지체 없이 파기하고 있는가?
2.5.1	개인정보취급자에 대한 보안서약서를 징구하였는가?
2.5.2	개인정보취급자에 대한 정기적인 교육은 실시하고 있는가?
2.6.1	개인정보 처리방침을 알기 쉽게 작성하고 보기 쉬운 곳(홈페이지, 접수대, 대기실 등)에 공개하고 있는가?
2.7.1	개인정보 보호책임자를 지정하여 개인정보 보호 총괄 업무를 수행하고 있는가?
2.7.2	개인정보 유출 등 발생에 대비한 대응절차를 숙지하고 있는가?
3.2.1	개인정보처리시스템(전자차트, 청구S/W 등)에 대한 접근 권한을 업무수행에 필요한 최소한의 범위로 업무 담당자에게 차등 부여하고 있는가?
3.6.1	악성 프로그램을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영 및 최신의 상태로 유지하고 있는가?

※ 모든 개인정보처리자가 준수해야하는 필수 항목으로 모두 응답(양호/미흡)이 필요하며 해당 항목의 점검 결과가 미흡한 경우 요양기관업무포털 안전신호등에 적색(자율점검 결과 미흡)으로 표시됩니다.

1.1.1	진료(조제, 복약지도 포함) 목적 외로 서면(오프라인) 및 홈페이지(온라인) 등을 통한 개인정보 수집 시 정보주체의 동의를 받고 있는가?
점검기준	☑ 정보주체(환자 등) 대상 필수항목 고지 및 동의 여부 확인 ☑ 동의 시 명시 항목과 실제 수집 항목 간 일치 여부 확인
증빙자료	☑ 개인정보수집동의서, 회원가입신청서 등 개인정보수집 양식
관련근거	「개인정보 보호법」 제15조(개인정보의 수집·이용) ①② 「개인정보 보호법」 제22조(동의를 받는 방법) ①②③⑤⑦ 「개인정보 보호법 시행령」 제17조(동의를 받는 방법) ①②③④ 「개인정보 처리 방법에 관한 고시」 제4조(서면 동의 시 중요한 내용의 표시 방법)
벌칙과태료	전체 매출액의 100분의 3이하의 과징금
세부설명	□ 개인정보처리자는 진료목적의 범위 외로 개인정보를 수집·이용하는 경우 정보주체 동의 등 적법한 방법으로 수집할 수 있으며, 그 수집 목적의 범위에서 이용 가능 ○ (예시) 진료목적의 범위 – 진료와 직접 관련된 자료 신청, 진단, 검사, 치료, 수납 등 업무 – 진료신청 문자 발송, 검사 결과 통보 등의 업무 – 진료와 연결된 예방접종(일반적 접종 안내 제외) – 병원 이전 또는 휴업에 관한 정보 ○ 개인정보처리자가 개인정보의 수집 및 수집 목적의 범위에서 이용이 가능한 경우 1. 정보주체의 동의를 받은 경우 2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우 3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우 4. 정보주체와 체결한 계약을 이행하거나 계약을 체결하는 과정에서 정보주체의 요청에 따른 조치를 이행하기 위하여 필요한 경우 5. 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. 7. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우

	□ 정보주체에게 개인정보 수집 동의를 받는 경우에는 개인정보 수집매체의 특성을 반영하여 적절한 방법으로 정보주체의 동의를 받아야 함 ○ 개인정보 처리에 대한 동의를 받는 방법 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 제1호부터 제5호까지의 규정에 따른 방식으로 동의 내용을 알리고 동의의 의사표시를 확인하는 방법 □ 정보주체에게 개인정보 수집 동의를 받는 경우에는 4가지의 법정 고지사항에 대해 명확하게 고지하고 동의를 받아야 함 ○ 개인정보의 수집·이용 동의 시 고지사항 1. 개인정보의 수집·이용 목적 2. 수집하려는 개인정보의 항목 3. 개인정보의 보유 및 이용기간 4. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우 그 불이익의 내용 □ 정보주체의 동의가 적법하기 위해서는 정보주체의 자유로운 의사에 따른 동의 여부 결정, 동의 내용의 구체성 및 명확성 등 적법 요건을 모두 충족하여야 함 ○ 정보주체의 동의를 받을 때 충족해야 하는 조건 1. 정보주체가 자유로운 의사에 따라 동의 여부를 결정할 수 있을 것 2. 동의를 받으려는 내용이 구체적이고 명확할 것 3. 그 내용을 쉽게 읽고 이해할 수 있는 문구를 사용할 것 4. 동의 여부를 명확하게 표시할 수 있는 방법을 정보주체에게 제공할 것

	□ 개인정보 처리에 대한 동의를 서면(전자문서 포함)으로 받을 때에는 다음과 같이 중요한 내용을 명확히 표시하여 알아보기 쉽게 하여야 함 ○ 명확히 표시하여야 하는 중요한 내용 – 개인정보의 수집·이용 목적 중 재화나 서비스의 홍보 또는 판매 권유 등을 위하여 해당 개인정보를 이용하여 정보주체에게 연락할 수 있다는 사실 – 처리하려는 개인정보 항목 중 민감정보, 여권번호, 운전면허번호, 외국인등록번호 – 개인정보의 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용 기간) – 개인정보를 제공받는 자 및 개인정보를 제공받는 자의 개인정보 이용 목적 ○ 중요한 내용의 표시 방법 – 글씨의 크기, 색깔, 굵기 또는 밑줄 등을 통하여 그 내용이 명확히 표시되도록 할 것 – 동의 사항이 많아 중요한 내용이 명확히 구분되기 어려운 경우에는 중요한 내용이 쉽게 확인될 수 있도록 그 밖의 내용과 별도로 구분하여 표시할 것 * 종이 인쇄물, 컴퓨터 표시화면 등 서면 동의를 요구하는 매체의 특성과 정보주체의 이용환경 등을 고려하여 정보주체가 쉽게 알아볼 수 있도록 표시
주요 확인사항	□ 개인정보를 수집하는 경우 정보주체 동의, 법령상 의무준수, 계약 체결·이행 등 관련 법률에 따른 적법 요건을 명확히 식별하고 이에 따라 개인정보를 적법하게 수집하였는가? □ 정보주체에게 개인정보 수집 동의를 받는 경우에는 개인정보 수집매체의 특성을 반영하여 적절한 방법으로 정보주체의 동의를 받아야 하며, 해당 정보가 필요한 시점에 수집하였는가? □ 정보주체에게 개인정보 수집 동의를 받는 경우에는 법정 고지사항에 대해 명확하게 고지하고 동의를 받아야 하며, 법령에서 정한 중요 내용에 대해 명확히 표시하여 정보주체가 이를 알아보기 쉽게 하였는가?

1.1.2	진료(조제, 복약지도 포함) 목적 외로 만 14세 미만 아동의 개인정보를 수집·처리 시, 법정대리인의 동의를 받았는가?
점검기준	☑ 진료(조제, 복약지도 포함) 목적 외 14세 미만 아동의 개인정보를 수집·처리 시, 법정대리인의 동의 여부 확인
증빙자료	☑ 개인정보수집동의서, 회원가입신청서 등 개인정보수집 양식
관련근거	「개인정보 보호법」 제22조의2(아동의 개인정보 보호) ①②③④ 「개인정보 보호법 시행령」 제17조의2(아동의 개인정보 보호) ① 「표준 개인정보 보호지침」 제13조(법정대리인의 동의) ①
벌칙과태료	5년 이하의 징역 또는 5천만 원 이하 벌금 전체 매출액의 100분의 3이하의 과징금
세부설명	□ 법정대리인의 동의를 받기 위하여 필요한 최소한의 정보(성명·연락처에 관한 정보)만을 수집하여야 하며, 법정대리인이 자격요건을 갖추고 있는지 확인하는 절차와 방법을 마련하여야 함 ○ 법정대리인 동의를 받기 위하여 필요한 최소한의 정보(법정대리인의 성명·연락처에 관한 정보)는 법정대리인의 동의 없이 아동으로부터 직접 수집 가능 ○ 다만, 법정대리인의 성명·연락처를 수집할 때에는 해당 아동에게 자신의 신분과 연락처와 함께, 법정대리인의 이름과 연락처를 수집하고자 하는 이유를 명확히 설명해야 함 ○ 아동으로부터 수집한 법정대리인의 개인정보는 동의를 얻기 위한 용도로만 활용 □ 진료(조제, 복약지도 포함) 목적 외로 14세 미만 아동에 대하여 개인정보를 수집·이용·제공 등 동의를 받는 경우 법정대리인에게 필요한 사항에 대하여 고지하고 동의를 받아야하며 증빙자료를 통해 확인이 필요함. ○ 만 14세 미만 아동의 개인정보를 처리할 필요가 없는 경우에는 적절한 연령 확인 절차를 통해 만 14세 미만 아동의 개인정보를 수집하지 않도록 조치 ○ 만 14세 미만 아동의 개인정보를 처리할 필요가 있는 경우에는 별도의 수집 동의 양식과 법정대리인 확인 절차를 마련하여 법정대리인의 동의를 받을 수 있도록 조치

	○ 법정대리인이 동의했는지를 확인하는 방법 1. 동의 내용을 게재한 인터넷 사이트에 법정대리인이 동의 여부를 표시하도록 하고 개인정보처리자가 그 동의 표시를 확인했음을 법정대리인의 휴대전화 문자메시지로 알리는 방법 2. 동의 내용을 게재한 인터넷 사이트에 법정대리인이 동의 여부를 표시하도록 하고 법정대리인의 신용카드·직불카드 등의 카드정보를 제공받는 방법 3. 동의 내용을 게재한 인터넷 사이트에 법정대리인이 동의 여부를 표시하도록 하고 법정대리인의 휴대전화 본인인증 등을 통하여 본인 여부를 확인하는 방법 4. 동의 내용이 적힌 서면을 법정대리인에게 직접 발급하거나 우편 또는 팩스를 통하여 전달하고, 법정대리인이 동의 내용에 대하여 서명날인 후 제출하도록 하는 방법 5. 동의 내용이 적힌 전자우편을 발송하고 법정대리인으로부터 동의의 의사표시가 적힌 전자우편을 전송받는 방법 6. 전화를 통하여 동의 내용을 법정대리인에게 알리고 동의를 받거나 인터넷 주소 등 동의 내용을 확인할 수 있는 방법을 안내하고 재차 전화 통화를 통하여 동의를 받는 방법 7. 그 밖에 제1호부터 제6호까지의 규정에 준하는 방법으로서 법정대리인에게 동의 내용을 알리고 동의의 의사표시를 확인하는 방법 □ 만 14세 미만의 아동에게 개인정보 처리와 관련한 사항 등의 고지 시 이해하기 쉬운 양식과 명확하고 알기 쉬운 언어로 표현하여야 함. ○ 아동이 이해하기 쉬운 언어, 그림, 동영상 등 아동 친화적인 방식으로 정보를 투명하게 전달 ○ 연령대별 아동의 역량과 이용행태 등을 고려 □ 법정대리인의 동의를 얻기 위해서는 아동이 제공한 정보가 진정한 법정대리인의 정보인지와 법정대리인의 미성년자 여부 확인, 아동과의 나이 차이 확인 등 진위 여부를 확인하여야 함 □ 법정대리인의 동의 거부가 있거나, 동의 의사가 확인되지 않는 경우 수집일로부터 5일 이내에 파기해야 함
주요 확인사항	□ 만 14세 미만 아동의 개인정보에 대해 수집·이용·제공 등의 동의를 받는 경우 법정대리인에게 필요한 사항에 대하여 고지하고 동의를 받고 있는가?

1.2.1	목적에 필요한 최소한의 개인정보만 수집하고 있는가?
점검기준	☑ 목적 달성을 위한 최소한의 개인정보(필수정보) 수집 여부 확인 ☑ 환자(정보주체)에게 수집되는 정보 중 선택적인 개인정보(필수정보 외)가 포함되어 있는 경우, 미동의 고지 여부 확인
증빙자료	☑ 개인정보수집동의서, 회원가입신청서 등 개인정보수집 양식
관련근거	「개인정보 보호법」 제16조(개인정보의 수집 제한) ① 「표준 개인정보 보호지침」 제4조(개인정보 보호 원칙) ①
벌칙과태료	3천만 원 이하 과태료
세부설명	□ 개인정보를 수집하는 경우 법률 근거, 법령상 의무준수, 계약의 체결·이행 등 수집 목적에 필요한 범위 내에서 최소한의 개인정보(필수정보)만 수집하여야 함 ○ 서면(오프라인) 또는 홈페이지(온라인) 등에서 추가적인 서비스 제공 등을 위한 선택적 개인정보를 수집하는 경우에도 최소한의 정보만 수집 ○ 최소한의 개인정보에 대한 입증책임은 개인정보처리자가 부담하므로 필수로 수집하는 정보에 대하여 서비스 제공 등에 필요한 최소한의 개인정보임을 입증할 수 있어야 함(이때 최소한의 개인정보란 해당 서비스의 본질적 기능을 위하여 반드시 필요한 정보를 말함)
주요 확인사항	□ 개인정보를 수집하는 경우 그 목적에 필요한 범위에서 최소한의 정보만을 수집하고 있는가?

1.2.2	최소한의 개인정보 수집 외에 선택정보에 대한 미동의를 이유로 재화 또는 부가서비스 제공을 거부하고 있지 않는가?
점검기준	☑ 선택정보 미동의 시 회원가입 등 기본적인 서비스 제공 여부 확인
증빙자료	☑ 개인정보수집동의서, 회원가입신청서 등 개인정보수집 양식
관련근거	「개인정보 보호법」 제16조(개인정보의 수집 제한) ②③
벌칙과태료	3천만 원 이하 과태료
세부설명	□ 최소한의 정보 외의 개인정보(선택정보) 수집 시 환자(정보주체)에게 동의하지 않을 수 있음을 구체적으로 알리고 수집하여야 함 ○ 선택정보 수집에 동의하지 않아도 기본적인 서비스 제공(회원가입 등)이 가능해야 함. 단, 환자(정보주체)가 선택정보에 대한 동의를 거부할 경우 재화 또는 부가서비스의 이용이 제한됨을 알리는 것은 가능함 ○ 회원가입 과정에서 선택정보에 대하여 동의를 하지 않거나 입력을 하지 않더라도 회원가입 등 필수적인 서비스는 이용이 가능하도록 구현 ※ 홈페이지 회원가입을 통한 정보를 수집하고자 하는 경우(예시) - 동의 필요(필수정보): 성명, 전화번호 - 동의거부 가능(선택정보): 성별, 나이
주요 확인사항	□ 정보주체의 동의를 받아 개인정보를 수집하는 경우 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 않을 수 있다는 사실을 구체적으로 알리고 있는가? □ 정보주체가 수집 목적에 필요한 최소한의 정보 이외의 개인정보 수집에 동의하지 않는다는 이유로 서비스 또는 재화의 제공을 거부하지 않도록 하고 있는가?

1.2.3	개인정보 수집 시 목적에 따라 구분하여 동의를 받고 있는가?
점검기준	☑ 목적에 따른 항목별 구분 동의 여부 확인
증빙자료	☑ 개인정보수집동의서, 회원가입신청서 등 개인정보수집 양식
관련근거	「개인정보 보호법」 제22조(동의를 받는 방법) ① 「표준 개인정보 보호지침」 제12조(동의를 받는 방법 등) ①②③
벌칙과태료	1천만 원 이하 과태료
세부설명	□ 개인정보의 처리에 대하여 환자(정보주체)의 동의를 받을 때에는 각각의 동의 사항을 구분하여 환자(정보주체)가 이를 명확하게 인지 할 수 있도록 알리고, 동의를 받아야 함 ○ 다음 각 호의 경우에는 동의사항을 구분하여 **각각의 동의**를 받아야 함 1. 개인정보 수집·이용(제15조제1항제1호: 개인정보의 수집・이용) 2. 개인정보의 제공(제17조제1항제1호: 개인정보의 제공) 3. 목적 외 이용·제공(제18조제2항제1호: 개인정보의 목적 외 이용・제공 제한) 4. 개인정보를 제공 받은 자의 이용・제공(제19조제1호: 개인정보를 제공받은 자의 이용・제공 제한) 5. 민감정보 처리(제23조제1항제1호: 민감정보의 처리 제한) 6. 고유식별정보 처리(제24조제1항제1호: 고유식별정보의 처리 제한) 7. 재화나 서비스를 홍보하거나 판매를 권유하기 위하여 개인정보의 처리에 대한 동의를 받으려는 경우 8. 그 밖에 정보주체를 보호하기 위하여 동의 사항을 구분하여 동의를 받아야 할 필요가 있는 경우로서 대통령령으로 정하는 경우 ※ 다른 개인정보의 처리에 대한 동의와 **별도로 동의**를 받아야 하는 경우 3. 목적 외 이용·제공 4. 개인정보를 제공 받은 자의 이용・제공 5. 민감정보 처리 6. 고유식별정보 처리
주요 확인사항	□ 정보주체의 동의를 받아 개인정보를 수집하는 경우 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 않을 수 있다는 사실을 구체적으로 알리고 있는가?

1.3.1	개인정보를 수집 목적 외 이용하거나 제3자에게 제공하는 경우 정보주체에게 별도의 동의를 받고 있거나 법적 근거가 있는가?
점검기준	☑ 법령(「의료법」, 「약사법」 등)에 근거한 경우 해당 법령 준수여부 확인 ☑ 법령에 근거하지 않은 제3자 제공의 경우, 필수 고지항목(5개)을 환자(정보주체)에게 고지하고 동의를 받았는지 여부 확인
증빙자료	☑ 목적 외 이용 및 제3자 개인정보 제공 동의서(필수고지내용 포함)
관련근거	「개인정보 보호법」 제17조(개인정보의 제공) ①② 「개인정보 보호법」 제18조(개인정보의 목적 외 이용·제공 제한) ①②③
벌칙과태료	5년 이하 징역 또는 5천만 원 이하 벌금 전체 매출액의 100분의 3 이하의 과징금
세부설명	□ 개인정보를 수집 목적 또는 개인정보처리자로부터 제공받은 목적의 범위를 초과하여 이용하거나 제공하는 경우 정보주체에게 별도의 동의를 받거나 법적 근거가 있는 경우로 제한하여야 함 ○ 개인정보를 목적 외의 용도로 이용·제공 가능한 경우(단, 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때는 제외) – 정보주체로부터 별도의 동의를 받은 경우 – 다른 법률에 특별한 규정이 있는 경우 – 명백히 정보주체 또는 제3자의 급박한 생명·신체·재산의 이익을 위하여 필요하다고 인정되는 경우 – 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우 □ 다른 법률에 특별한 규정이 있는 경우(예시) – 「의료법」 제21조(기록 열람 등)에 의해 건강보험 급여비용 청구를 위한 개인정보 제공은 환자의 동의 없이 가능함 □ 법령의 근거 없이 개인정보 수집 목적 외 이용 또는 제3자에게 제공하는 경우, 다른 개인정보의 처리에 대한 동의와 구분하여 필수 고지항목을 고지하고 목적 외 이용·제공에 대한 각각의 동의를 받아야 함 ○ 목적 외 이용의 경우 고지사항 1. 개인정보의 이용목적 2. 이용하는 개인정보의 항목 3. 개인정보의 보유 및 이용기간 4. 동의거부권이 있다는 사실 및 동의거부에 따른 불이익에 관한 사항

	○ 제3자 제공의 경우 고지사항 1. 개인정보를 제공받는 자의 성명(법인 또는 단체인 경우에는 그 명칭) 2. 제공받는 자의 이용목적 3. 제공하는 개인정보의 항목 4. 제공받는 자의 개인정보 보유 및 이용 기간 5. 동의거부권이 있다는 사실 및 동의거부에 따른 불이익 □ 정보주체의 동의를 미리 받아 둔 경우, 그 동의의 범위 내에서 개인정보 제3자 제공이 가능하나, 기존에 받은 동의의 범위를 넘어서 제3자 제공을 하는 경우에는 사유 발생 시점에 동의를 받아야 하며, 당초 동의와 구분되는 별도의 동의를 받아야 함 □ 다른 개인정보처리자로부터 개인정보를 제공받은 자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 개인정보를 제공받은 목적 외의 용도로 이용하거나 이를 제3자에게 제공하여서는 아니 됨 ○ 정보주체로부터 별도의 동의를 받은 경우 ○ 다른 법률에 특별한 규정이 있는 경우 □ 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우 제공받는 자에게 이용목적·방법 등을 제한하거나 안전성 확보를 위해 필요한 조치를 마련하도록 요청하여야 함 ○ 개인정보를 제공받는 자에게 이용 목적, 이용 방법, 이용 기간, 이용 형태 등을 제한 ○ 개인정보의 안전성 확보를 위하여 필요한 구체적인 조치를 마련하도록 문서(전자문서 포함)로 요청
주요 확인사항	□ 개인정보는 최초 수집 시 정보주체로부터 동의를 받은 목적 또는 법령에 근거한 범위 내에서만 이용·제공하고 있는가? □ 개인정보처리자로부터 개인정보를 제공받은 경우 제공받은 목적의 범위 내에서만 이용·제공하고 있는가?

<table>
<tr><td>1.4.1</td><td colspan="3">개인정보의 보유기간 경과, 처리목적 달성 등 파기 시점이 도달한 때에 지체 없이 파기하고 있는가?</td></tr>
<tr><td>점검기준</td><td colspan="3">☑ 법령에 규정된 보존기간이 지난 진료정보 및 기타 목적으로 수집한 개인정보에 대하여 목적 달성 이후 파기 여부 확인
☑ 개인정보의 파기 시 복원 불가능한 방법으로 파기 여부 확인
☑ 파쇄기 등 파기도구 설치 및 사용 여부</td></tr>
<tr><td>증빙자료</td><td colspan="3">☑ 개인정보 파기 관리대장</td></tr>
<tr><td>관련근거</td><td colspan="3">「개인정보 보호법」 제21조(개인정보의 파기) ①②③
「개인정보 보호법 시행령」 제16조(개인정보의 파기방법) ①
「개인정보의 안전성 확보조치 기준」 제13조(개인정보의 파기) ①②③
「표준 개인정보 보호지침」 제10조(개인정보의 파기방법 및 절차) ②</td></tr>
<tr><td>벌칙과태료</td><td>3천만 원 이하의 과태료</td><td>고유식별정보 안전조치 관리실태 점검 항목</td><td>3</td></tr>
<tr><td>세부설명</td><td colspan="3">□ 진료정보의 경우 「의료법」, 「약사법」 등 법령에 규정된 보존기한을 준수하여야 함
○ 단, 계속적인 진료를 위하여 필요한 경우에는 1회에 한정하여 동일 기간 만큼 연장 가능함(「의료법 시행규칙」 제15조)
<table>
<tr><th>구분</th><th>의료법(시행규칙 제15조)</th><th>약사법(제29조, 30조)</th></tr>
<tr><td>기록물
(보존기간)</td><td>환자명부(5년), 진료기록부(10년), 처방전(2년, 건강보험 청구건 (3년), 수술기록(10년), 검사소견기록(5년), 방사선 사진 및 그 소견서(5년), 간호기록부(5년), 조산기록부(5년), 진단서 등의 부본(3년)</td><td>처방전(2년,
건강보험청구건 (3년)
조제기록부(5년)</td></tr>
</table>
* 건강보험법 제96조의4(서류의 보존) 참고
□ 진료(조제, 복약지도 포함) 목적 외로 수집한 개인정보는 보유기간의 경과 및 처리목적 달성 시 지체 없이(5일 이내) 파기하여야 함
○ 단, 5명 미만의 상시근로자 가 있는 의료기관이 개인정보 파기를 독립적으로 수행하기 어려운 경우에는 협회의 중앙회 또는 지부에서 공동으로 파기할 수 있음(의료기관 개인정보 보호 가이드라인)
□ 개인정보(파일)의 당초 수집목적이 달성되었거나, 보유기간이 경과하여 파기하는 경우 복구·재생되지 않도록 안전한 방법으로 파기하여야 함
○ 완전파괴(소각·파쇄 등)</td></tr>
</table>

○ 전용 소자장비(자기장을 이용해 저장장치의 데이터를 삭제하는 장비)를 이용하여 삭제

○ 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

□ 개인정보의 일부만을 파기하는 경우 위의 방법으로 파기하는 것이 어려울 때에는 다음의 조치 이행

○ 전자적 파일: 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독

○ 기록물, 인쇄물, 서면, 그 밖의 기록매체: 해당 부분을 마스킹, 구멍 뚫기 등

□ 정보 파기에 대한 기록을 남기고 관리하여야 함

○ 개인정보 파기의 시행 및 파기 결과의 확인은 개인정보 보호책임자의 책임 하에 수행되어야 하며, 파기에 관한 사항을 기록·관리

○ 개인정보 파기에 대한 기록은 파기 관리대장에 기록하거나 파기 내용을 담은 사진 등을 기록물로 보관

※ 개인정보파일 파기 대장(예시)

번호	개인정보파일명	자료의 종류	생성일	폐기일	폐기사유	처리담당자	처리부서장
1	환자종이청구정보						
2	환자조제내역정보						

□ 업무 수행 상 보존 필요성은 없으나, 임시적으로 생성한 파일이나 출력자료는 사용 후 즉시 파기하여야 함

○ 불필요한 출력자료 생산은 지양하고 환자의 정보가 담긴 문서(접수증, 진료기록부 사본, 처방전 등)는 대기실 및 접수대 등 공용 공간에 방치되지 않도록 관리해야 함

○ 업무용 PC에 보관 중인 임시파일(개인정보가 포함된 문서 및 사진 등)은 목적 달성 후 즉시 파기해야 함

– 별도 저장이 필요한 경우 반드시 암호화(비밀번호 설정)하여 저장

– 주기적으로 임시파일 존재여부 점검 및 삭제

주요 확인사항

□ 개인정보의 보유기간 및 파기와 관련된 내부 정책을 수립하고 있는가?

□ 개인정보의 처리목적이 달성되거나 보유기간이 경과한 경우 지체 없이 해당 개인정보를 파기하고 있는가?

□ 개인정보를 파기할 때에는 복구·재생되지 않도록 안전한 방법으로 파기하고 있는가?

□ 개인정보 파기에 대한 기록을 남기고 관리하고 있는가?

1.4.2	타 법령(전자상거래법, 형사소송법, 민사소송법 등)에 따라 개인정보를 파기하지 않고 보존하는 경우 별도로 분리하여 보관하고 있는가?
점검기준	☑ 타 법령에 따라 보존하는 개인정보가 존재하는 경우 별도분리 보관 여부 확인
증빙자료	☑ 타 법령의 근거에 따라 별도 분리 보관하는 개인정보가 있는 경우, 개인정보처리시스템 내 분리 저장된 화면캡처 또는 물리적 보관사진 등
관련근거	「개인정보 보호법」 제21조(개인정보의 파기) ①③
벌칙과태료	1천만 원 이하 과태료
세부설명	□ 개인정보의 보유기간 경과 또는 처리목적 달성 후에도 관련 법령 등에 따라 파기하지 않고 보존하는 경우 관련 법령에 따른 최소한의 기간으로 한정하여 최소한의 정보만을 보존하도록 관리 ○ 개인정보의 항목을 보유목적에 맞는 최소한의 항목으로 제한 ○ 관련 법령에 따른 최소기간으로 보유기간 설정 □ 개인정보의 보유기간 경과 또는 처리목적 달성 후에도 「전자상거래법」, 「형사소송법」, 「민사소송법」 등에 따라 파기하지 않고 보존하는 경우 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여 저장·관리 ○ 서면: 물리적 장소 분리 ○ 전자파일: 별도의 DB, Table, 파일 등으로 분리 □ 접근권한은 해당업무 담당자 등 필수직원으로 엄격히 제한 ○ 법령에 따라 분리 보관한다는 의미는 소송, 민원 등 특정한 상황이 아니면 접근할 필요가 없다는 것을 의미 □ 법원·경찰 등에서 법률에 의해서 보존요청이 올 경우 요청기간에 따라 보존하여야함
주요 확인사항	□ 개인정보의 보유기간 경과 또는 처리목적 달성 후에도 관련 법령 등에 따라 파기하지 않고 보존하는 경우 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여 저장·관리하고 있는가?

지표별 가이드

Ⅱ. 개인정보의 처리 제한

2.1. 민감정보의 처리제한

2.2. 고유식별정보의 처리제한

2.3. 영상정보처리기기 설치운영 제한

2.4. 업무위탁에 따른 개인정보의 처리제한

2.5. 개인정보 취급자 감독

2.6. 개인정보 처리방침의 수립 및 공개

2.7. 개인정보 보호책임자 지정 및 유출방지

2.8. 손해배상책임 보험가입

2.1.1	진료(조제, 복약지도 포함) 목적 외로 민감정보를 수집할 경우, 별도 동의를 받고 있는가?
점검기준	☑ 목적 외 민감정보 수집 시 별도 동의를 받는지 여부 확인
증빙자료	☑ 개인정보수집동의서, 민감정보 수집 동의서 등 민감정보 수집 양식 ☑ 개인정보 처리방침
관련근거	「개인정보 보호법」 제23조(민감정보의 처리 제한) ① 「개인정보 보호법 시행령」 제18조(민감정보의 범위) 1234
벌칙과태료	5년 이하 징역 또는 5천만 원 이하 벌금 전체 매출액의 100분의 3 이하의 과징금
세부설명	□ 의료기관은 법령에 따라 진료(조제, 복약지도 포함) 목적을 위하여 민감정보를 환자(정보주체)의 별도 동의 없이 수집하고 이용할 수 있음 ○ 민감정보: 사상・신념, 노동조합・정당의 가입・탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 유전정보, 범죄경력정보, 생체인식정보, 인종이나 민족에 관한 정보 □ 진료(조제, 복약지도 포함) 목적 외 또는 법령에 근거하지 않고 민감정보를 처리하고자 하는 경우 환자(정보주체)에게 아래 사항을 고지하고 별도의 동의를 받아야 함 ○ 민감정보 수집·이용 시 고지사항 – 민감정보의 수집·이용 목적 – 수집하려는 민감정보의 항목 – 민감정보의 보유 및 이용기간 – 동의거부권 및 동의 거부에 따른 불이익 안내
주요 확인사항	□ 민감정보는 정보주체로부터 별도의 동의를 받거나 관련 법령에 근거가 있는 경우에만 처리하고 있는가? □ 재화 또는 서비스를 제공하는 과정에서 공개되는 정보에 정보주체의 민감정보가 포함됨으로써 사생활 침해의 위험성이 있다고 판단하는 때에는 재화 또는 서비스의 제공 전에 민감정보의 공개 가능성 및 비공개를 선택하는 방법을 정보주체가 알아보기 쉽게 알리고 있는가?

<table>
<tr><td>2.2.1</td><td colspan="3">주민등록번호를 처리(수집·이용·보관 등)함에 있어 법령의 근거가 있는가?</td></tr>
<tr><td>점검기준</td><td colspan="3">☑ 관련법령에 의거한 주민등록번호 처리(수집·이용·보관 등) 여부 확인</td></tr>
<tr><td>증빙자료</td><td colspan="3">☑ 「의료법」, 「약사법」 등 법령에 의거한 주민등록번호를 수집 및 처리하는 경우 별도의 증빙자료 없이 점검결과 ‘양호’ 선택</td></tr>
<tr><td>관련근거</td><td colspan="3">「개인정보 보호법」 제24조의2(주민등록번호 처리의 제한) ①
「개인정보보호법 시행령」 제19조(고유식별정보의 범위) 1234</td></tr>
<tr><td>벌칙과태료</td><td>5천만 원 이하 벌금
전체 매출액의 100분의 3 이하의 과징금</td><td>고유식별정보 안전조치 관리실태 점검 항목</td><td>1</td></tr>
<tr><td>세부설명</td><td colspan="3">□ 진료(조제, 복약지도 포함) 목적의 고유식별정보 처리는 법령에 의해 환자(정보주체)의 별도 동의 없이 처리 가능함
□ 주민등록번호는 법적 근거가 있는 경우를 제외하고는 수집·이용 등 처리할 수 없으며, 주민등록번호의 처리가 허용된 경우라 하더라도 인터넷 홈페이지 등에서 수집 시 대체수단을 제공하여야 함
(“주민등록번호 수집 법정주의“에 따라 동의에 근거한 수집은 불가함)
주민등록번호 대체수단 예시: 아이핀, 휴대전화, 신용카드, 인증서 등
* 법률, 대통령령, 국회규칙, 대법원규칙, 헌법재판소규칙, 중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우

※ 법률에 특별한 규정이 있는 경우(예시)
<table>
<tr><th>개인정보파일</th><th>수집항목</th><th>법률근거</th></tr>
<tr><td>진료신청서</td><td>성명, 주민등록번호, 진료과목, 전화번호, 환자등록번호 등</td><td>「의료법」 제22조</td></tr>
<tr><td>선택진료신청서</td><td>성명, 주소, 전화번호, 주민등록번호, 진료 지원항목 등</td><td>「의료법」 제46조</td></tr>
<tr><td>진료기록부</td><td>진료를 받은 사람의 주소, 성명, 연락처, 주민등록번호 등 인적사항
주된 증상, 병력 및 가족력,
진단결과 또는 진단명, 진료경과,
치료내용(주사·투약 등), 진료일시</td><td rowspan="2">「의료법」 제22조, 같은 법 시행규칙 제14조</td></tr>
<tr><td>조산기록부</td><td>조산을 받은 자의 주소, 성명, 연락처, 주민등록번호 등 인적사항</td></tr>
<tr><td>환자명부</td><td>주소, 성명, 주민등록번호, 전화번호</td><td>「의료법」 제22조, 같은 법 시행규칙 제15조</td></tr>
<tr><td>처방전</td><td>환자의 성명, 주민등록번호 의료기관의 명칭과 전화번호 및</td><td>「의료법」 제18조, 같은</td></tr>
</table></td></tr>
</table>

개인정보파일	수집항목	법률근거
	팩스번호, 질병분류기호, 의료인의 성명·면허종류 및 번호, 처방의약품의 명칭·분량·용법 및 용량, 처방전 발급 연월일 및 사용기간 등	법 시행규칙 제12조
수술기록	환자의 성명, 수술명, 수술기록 등, 수술의사의 성명 등	「의료법」 제22조, 같은 법 시행규칙 제15조
검사내용 및 검사소견서	성명, 주민등록번호, 의사면허번호, 소견인 성명, 질병 검사 소견 등	
방사선사진 및 소견서	성명, 주민등록번호, 의사면허번호, 소견인 성명, 방사선사진에 대한 검사 소견 등	
진단서	환자의 성명, 주민등록번호 및 주소	「의료법」 제17조, 같은 법 시행규칙 제9조
사망진단서 (시체검안서)	사망자의 성명, 성별, 주민등록번호, 실제생년월일, 직업, 주소, 발병일시, 사망일시, 사망장소, 사망의 원인, 사망의 종류, 외인 사사항(사고종류, 사고발생일시, 사고발생장소)	「의료법」 제17조, 같은 법 시행규칙 제10조
환자 진료기록의 열람 및 사본 교부	환자 본인 – 성명, 연락처, 생년월일, 주소 신청인 - 성명, 연락처, 생년월일, 주소, 환자와의 관계, 위임장 ㉠ 수임인의 성명, 연락처, 생년월일(외국인등록번호), 주소, 위임인과의 관계 ㉡ 위임인의 성명, 전화번호, 생년월일(외국인등록번호), 주소	「의료법」 제21조, 같은 법 시행규칙 제13조의3
요양급여 의뢰서	건강보험증번호, 가입자·세대주·환자의 성명 및 주민등록번호, 주소, 전화번호, 상병명, 상병분류기호, 진료기간, 진료구분, 환자상태 및 진료소견	「국민건강보험법」 제41조, 「국민건강보험 요양급여의 기준에 관한 규칙」 제2조
자원봉사자 정보	이름, 주소, 연락처, 이메일, 학력사항, 자원봉사 활동내역 주민등록번호	「자원봉사활동 기본법」 11조, 같은 법 시행령 제16조
진료비 수납	신용카드번호, 진료비, 신용카드사 등	「전자금융거래법」

주요 확인사항	□ 주민등록번호는 명확한 법적 근거가 있는 경우에만 처리하고 있는가? □ 주민등록번호의 수집 근거가 되는 법조항을 구체적으로 식별하고 있는가?

<table>
<tr><td>2.2.2</td><td colspan="3">여권번호, 운전면허번호, 외국인등록번호를 처리(수집·이용·보관 등)함에 있어 법령의 근거 또는 정보주체의 동의가 있는가?</td></tr>
<tr><td>점검기준</td><td colspan="3">☑ 고유식별정보(여권번호, 운전면허번호, 외국인등록번호)를 정보주체의 동의 또는 근거 법령에 따라 처리하는지 확인</td></tr>
<tr><td>증빙자료</td><td colspan="3">☑ 「의료법」, 「약사법」 등 법령에 의거한 고유식별정보 수집 및 처리만 하는 경우 별도의 증빙자료 없이 점검결과 ‘양호’ 선택</td></tr>
<tr><td>관련근거</td><td colspan="3">개인정보보호법 제24조(고유식별정보의 처리 제한) ①
개인정보보호법 시행령 제19조(고유식별정보의 범위) 1234</td></tr>
<tr><td>벌칙·과태료</td><td>5년 이하 징역 또는 5천만 원 이하 벌금
전체 매출액의 100분의 3 이하의 과징금</td><td>고유식별정보 안전조치
관리실태 점검 항목</td><td>2</td></tr>
<tr><td>세부설명</td><td colspan="3">□ 고유식별정보: 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호와 같은 특정 개인을 유일하게 식별할 수 있는 정보
○ 단, 주민등록번호의 경우 동의에 근거한 수집은 불가 함

□ 진료(조제, 복약지도 포함) 목적의 고유식별정보 처리는 법령에 의해 환자(정보주체)의 별도 동의 없이 처리 가능함

□ 진료(조제, 복약지도 포함) 목적 외 또는 법령에 근거하지 않고 고유식별정보를 처리할 경우 환자(정보주체)에게 별도의 동의를 받아야 함

□ 정보주체의 별도 동의를 받아 고유식별정보(여권번호, 운전면허번호, 외국인등록번호)를 처리하는 경우 필수항목을 포함하여 동의를 받아야 함
○ 제15조제2항(정보주체에게 고지하여야 할 4개 항목) 또는 제17조제2항(정보주체에게 고지하여야 할 5개 항목)의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받아야 함
※ 법률에 특별한 규정이 있는 경우(예시)
<table>
<tr><th>개인정보파일</th><th>법률근거</th></tr>
<tr><td>진료 신청서</td><td>의료법 제22조</td></tr>
<tr><td>선택진료 신청서</td><td>의료법 제46조, 선택진료에 관한 규칙 제2조</td></tr>
<tr><td>진료기록부</td><td rowspan="3">의료법 제22조, 같은 법 시행규칙 제14조</td></tr>
<tr><td>조산기록부</td></tr>
<tr><td>간호기록부</td></tr>
<tr><td>환자명부</td><td>의료법 제22조, 같은 법 시행규칙 제15조</td></tr>
<tr><td>처방전</td><td>의료법 제18조, 같은 법 시행규칙 제12조</td></tr>
<tr><td>수술기록</td><td>의료법 제22조, 같은 법 시행규칙 제15조</td></tr>
</table></td></tr>
</table>

개인정보파일	법률근거
검사소견서	
방사선사진.소견서	
진단서	의료법 제17조, 같은 법 시행규칙 제9조
사망진단서 (사체검안서)	의료법 제17조, 같은 법 시행규칙 제10조
출생증명서	의료법 제17조, 같은 법 시행규칙 제11조
사산.사태증명서	
환자 진료기록의 열람 및 사본 교부	「의료법」 제21조, 같은 법 시행규칙 제13조의3
요양급여 의뢰서	국민건강보험법 제41조, 국민건강보험 요양급여의 기준에 관한 규칙 제2조
자원봉사자 정보	「자원봉사활동기본법」 11조, 같은 법 시행령 제16조
진료비 수납	「전자금융거래법」
감염병환자, 감염병의사환자, 병원체보유자 신고의무	감염병의 예방 및 관리에 관한 법률 제11조, 같은 법 시행규칙 제6조, 성매개감염병 및 후천성면역결핍증 건강진단규칙 제7조
응급환자이송의무	응급의료에 관한 법률 제11조, 같은 법 시행규칙 제4조
감염인 진단.검안사실 신고의무	후천성면역결핍증예방법 제5조
특정수혈부작용 신고의무	혈액관리법 제10조, 같은 법 시행규칙 제13조
뇌사추정자신고의무	장기 등 이식에 관한 법률 제17조, 같은 법 시행규칙 제11조
질병자 또는 질병의심 대상자 발견 보고, 신고, 통지 등 의무	보건의료기본법 제5조
실지명의	금융실명거래 및 비밀보장에 관한 법률 시행령 제3조
성년후견등에 관한 기록사항	후견등기에 관한 법률 제25조제1항
조제정보 및 요양급여 청구 정보	「약사법」 제30조제1항, 국민건강보험법」 제96조의4 및 같은 법 시행규칙 제58조

(출처) 의료기관 개인정보보호가이드라인, 개인정보 보호 법령 및 지침·고시 해설서(2020.12)

주요 확인사항	□ 고유식별정보(주민등록번호 제외) 또는 민감정보를 수집·이용하는 경우에는 해당 정보주체 (환자, 의료인, 직원)의 동의를 별도로 받거나 법령에 구체적인 수집·이용 근거가 있는가?

2.3.1	고정형 또는 이동형 영상정보처리기기 운영·관리방침을 수립 및 공개하고 있는가?
점검기준	☑ 영상정보처리기기 운영·관리방침 수립·공개 여부 확인
증빙자료	☑ 영상정보처리기기운영 · 관리 방침 (필수 기재사항 ①~⑧ 포함 수립)
관련근거	「개인정보 보호법」 제25조(고정형 영상정보처리기기의 설치운영 제한) ⑦ 「개인정보 보호법」 제25조의2(이동형 영상정보처리기기의 설치운영 제한) ④ 「개인정보 보호법 시행령」 제25조(영상정보처리기기의 운영관리 방침) ①② 「표준 개인정보 보호지침」 제36조(영상정보처리기기 운영·관리 지침) ①②
벌칙과태료	–
세부설명	□ 고정형 영상정보처리기기운영자의 경우 고정형 영상정보처리기기 운영·관리 방침을 마련하고, 이동형 영상정보처리기기운영자의 경우 이동형 영상정보처리기기 운영·관리 방침을 마련하고, 이를 공개하여야 함 □ 영상정보처리기기 운영·관리 방침에 포함하여야 할 사항 1. 영상정보처리기기의 설치 근거 및 설치 목적 2. 영상정보처리기기의 설치 대수, 설치 위치 및 촬영 범위 3. 관리책임자, 담당 부서 및 영상정보에 대한 접근 권한이 있는 사람 4. 영상정보의 촬영시간, 보관기간, 보관장소 및 처리방법 5. 영상정보처리기기운영자의 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 □ 영상정보처리기기 운영·관리 방침 공개 방법 ○ 영상정보처리기기 운영·관리 방침은 개인정보 처리방침과 동일하게 인터넷 홈페이지 또는 보기 쉬운 장소(접수대 등)에 게시하여야 함 ○ 개인정보 처리방침에 포함하여 수립·공개 가능 ※ 참고: 영상정보처리기기 운영·관리 방침은 운영책임기관에서 수립하여 관리(위탁 운영하는 경우에는 위탁자가 운영·관리 방침을 수립·관리)
주요 확인사항	□ 영상정보처리기기 및 영상정보의 안전한 관리를 위한 영상정보처리기기 운영·관리 방침을 마련하여 시행하고 있는가?

2.3.2	고정형 영상정보처리기기를 설치한 장소에 정보주체가 해당 기기의 설치 사실을 인지할 수 있도록 필수기재 사항을 포함한 안내판을 설치하고 있는가?
점검기준	☑ 안내판 설치(필수 기재사항 ①~④ 포함) 여부 확인
증빙자료	☑ 안내판 설치 장소 및 내용
관련근거	「개인정보 보호법」 제25조(고정형 영상정보처리기기의 설치운영 제한) ④ 「개인정보 보호법 시행령」 제24조(안내판의 설치 등) ①②③ 「표준 개인정보 보호지침」 제39조(안내판의 설치) ①②③
벌칙과태료	3천만 원 이하 과태료
세부설명	□ 공개된 장소에서 고정형 영상정보처리기기를 설치·운영하여서는 아니됨 ○ 예외조건(법적 허용요건) – 법령에서 구체적으로 허용하고 있는 경우 – 범죄의 예방 및 수사를 위하여 필요한 경우 – 시설의 안전 및 관리, 화재 예방을 위하여 정당한 권한을 가진 자가 설치・운영하는 경우 – 촬영된 영상정보를 저장하지 아니하는 경우로서 다음 중 어느 하나에 해당하는 경우로서 촬영된 영상을 별도로 저장하지 아니하는 경우 · 출입자 수 등 통계값 산출을 위해 필요한 경우 · 성별, 연령대 등 통계적 특성값을 도출하기 위해 필요한 경우 · 그 밖에 위의 2가지에 준하는 경우로서 개인정보 보호위원회의 심의·의결을 거친 경우 □ 고정형 영상정보처리기기를 설치·운영하는 경우 환자(정보주체)가 쉽게 인지할 수 있도록 안내판을 설치하여야 함 ○ 안내판에 필수기재 하여야 할 사항 1. 설치 목적 및 장소 2. 촬영 범위 및 시간 3. 관리책임자의 연락처 4. 위탁받은 자의 명칭 및 연락처(설치·운영 위탁 시)

	○ 안내판 설치 시 고려하여야 할 사항 – 정보주체가 쉽게 알아볼 수 있는 위치에 설치 – 건물 안에 여러개의 고정형 영상정보처리기기를 설치하는 경우에는 출입구 등 잘 보이는 곳에 해당 시설 또는 장소 전체가 고정형 영상정보처리기기 설치지역임을 표시하는 안내판 설치 가능 □ 요양기관의 진료실, 처치실, 수술실, 입원실 등의 공간에 고정형 영상정보처리기기를 설치하여 개인영상 등을 수집하고자 하는 경우에는 정보주체의 **별도 수집·이용 동의를** 받아야 함 ○ 정신보건법에 의한 수용시설을 갖춘 정신의료기관, 정신질환자사회복귀시설, 정신요양시설은 제외
주요 확인사항	□ 공개된 장소에 고정형 영상정보처리기기를 설치·운영할 경우 법적 허용요건에 해당하는지를 검토하고 있는가? □ 고정형 영상정보처리기기 설치·운영 시 정보주체가 쉽게 인식할 수 있도록 안내판 설치 등 필요한 조치를 하고 있는가?

2.3.3	**고정형 또는 이동형(자율주행 자동차, 드론 등) 영상정보처리기기에 대한 이용 · 제공 · 열람 · 파기 내역을 기록하고 관리하고 있는가?**
점검기준	☑ 개인영상정보 관리대장 작성·관리 여부 확인
증빙자료	☑ 개인영상정보 관리대장
관련근거	「개인정보 보호법」 제21조(개인정보의 파기) ① 「표준 개인정보 보호지침」 제42조(이용·제3자 제공·파기의 기록 및 관리) ① 「표준 개인정보 보호지침」 제44조(정보주체의 열람등 요구) ② 「표준 개인정보 보호지침」 제45조(개인영상정보 관리대장) ⑤
벌칙과태료	–
세부설명	□ 고정형 또는 이동형 영상정보처리기기 운영자는 개인영상정보를 수집 목적 이외로 이용하거나 제3자에게 제공하는 경우, 파기하는 경우, 열람 요청이 있는 경우에는 아래 사항을 기록하고 관리하여야 함 ○ 개인영상정보의 목적 외 이용·제3자 제공 시 기록사항 1. 개인영상정보 파일의 명칭 2. 이용하거나 제공받은 자(공공기관 또는 개인)의 명칭 3. 이용 또는 제공의 목적 4. 법령상 이용 또는 제공 근거가 있는 경우 그 근거 5. 이용 또는 제공의 기간이 정해져 있는 경우에는 그 기간 6. 이용 또는 제공의 형태 7. 이용 또는 제공한 개인영상정보의 업무처리 담당자 8. 제공한 이후 파기 여부 등 그 결과와 처리 일자 9. 안전성 확보를 위하여 필요한 조치를 요청한 경우 그 내용 및 결과 * 단, 8 ~ 9호는 공공의료기관에 한하여 적용됨(민간분야는 적용제외) ○ 정보주체의 열람 등 요구 시 1. 개인영상정보 열람 등을 요구한 정보주체의 성명 및 연락처 2. 정보주체가 열람 등을 요구한 개인영상정보 파일의 명칭 및 내용 3. 개인영상정보 열람 등의 목적 4. 개인영상정보 열람 등을 거부한 경우 그 거부의 구체적 사유 5. 정보주체에게 개인영상정보 사본을 제공한 경우 해당 영상정보의 내용과 제공한 사유 6. 개인영상정보 열람 등의 업무처리 담당자 * 표준지침 별지 서식 제3호 개인영상정보 관리대장 활용 가능

	○ 파기하는 경우 1. 파기하는 개인영상정보 파일의 명칭 2. 개인영상 정보 파기일시(사전에 파기 시기 등을 정한 자동삭제의 경우에는 파기 주기 및 자동삭제 여부에 대한 확인 시기 기록) 3. 개인영상정보 파기 담당자 * 영상정보의 보관기간은 개인영상정보 수집 후 30일 이내로 파기하는 것을 권장함 □ 영상정보의 보관 기간을 정하여 보관 기간 만료 시 지체 없이 파기하여야 함 ○ 영상정보의 보유 목적 달성을 위한 최소한의 기간으로 보관 기간 결정 ○ 다만, 영상정보의 보관 기간과 관련하여 다른 법령에 특별한 규정이 있는 경우에는 해당 규정에 따라 보관 ○ 영상정보처리기기운영자가 그 사정에 따라 보유 목적 달성을 위한 최소한의 기간을 산정하기 곤란한 때에는 보관 기간을 개인영상정보 **수집 후 30일 이내**로 함(표준 개인정보 보호지침 제41조제2항)
주요 확인사항	□ 영상정보의 보관 기간을 정하고 있으며, 보관 기간 만료 시 지체 없이 파기하고 있는가?

2.3.4	고정형 또는 이동형 영상정보처리기기의 안전성 확보조치를 하고 있는가?
점검기준	☑ 개인영상정보의 보관시설 마련 또는 잠금장치 설치 여부 확인 ☑ 개인영상정보에 대한 접근통제 여부 확인
증빙자료	☑ 고정형 또는 이동형 영상정보처리기기 녹화장비(DVR) 등 물리적 시건장치 사진 또는 접속계정(ID) 관리화면 캡처
관련근거	「개인정보 보호법」 제25조(고정형 영상정보처리기기의 설치운영 제한) ⑥ 「개인정보 보호법」 제25조의2(이동형 영상정보처리기기의 설치운영 제한) ④ 「개인정보 보호법」 제29조(안전조치의무) 「표준 개인정보 보호지침」 제47조(개인영상정보의 안전성 확보를 위한 조치) 개인정보보호위원회 「영상정보처리기기 설치운영 가이드라인」
벌칙과태료	3천만 원 이하의 과태료
세부설명	□ 고정형 영상정보처리기기 운영자 또는 이동형 영상정보처리기기 운영자는 개인영상정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 개인영상정보의 안전성 확보에 필요한 조치를 하여야 함 ○ 개인영상정보의 안전한 처리를 위한 내부 관리계획의 수립·시행 – 개인영상정보 관리책임자 지정 – 개인영상정보 관리책임자 및 취급자의 역할 및 책임에 관한 사항 – 안전성 확보조치에 관한 사항 – 개인영상정보취급자 교육 – 그 밖에 개인영상정보의 안전성 확보에 필요한 조치에 관한 사항 ○ 개인영상정보에 대한 접근 통제 및 접근 권한의 제한 조치 ○ 개인영상정보를 안전하게 저장·전송할 수 있는 기술의 적용 – 안전한 저장·전송 방법(예시): 네트워크 카메라의 경우 안전한 전송을 위한 암호화 조치, 개인영상정보파일에 대한 비밀번호 설정 등 ○ 처리기록의 보관 및 위조·변조 방지를 위한 조치 (개인영상정보의 생성 일시 및 열람할 경우에 열람 목적·열람자·열람 일시 등 기록·관리 조치 등) ○ 개인영상정보의 안전한 물리적 보관을 위한 보관시설 마련 또는 잠금장치 설치 ※ 1만명 미만의 정보주체의 개인정보를 처리하는 소상공인·개인·단체는 안전성 확보조치 의무 중 내부관리계획 수립 생략 가능

	□ 고정형 영상정보처리기기 운영자는 고정형 영상정보처리기기에 의하여 수집·처리되는 개인영상정보의 접근권한을 관리책임자 등 지정된 최소한의 인원으로 제한하여야 함 □ 고정형 영상정보처리기기에 접근 권한이 없는 자가 고정형 영상정보처리기기를 함부로 조작하거나 모니터링 할 경우 관련 법령에 따라 처벌받을 수 있다는 사실의 안내판을 모니터링 화면 옆이나 고정형 영상정보처리기기 관리 본체에 부착하여 접근 권한 없는 자의 임의적 접근 및 조작 등을 방지하여야 함 □ 고정형 영상정보처리기기 운영자는 고정형 영상정보처리기기의 설치·운영으로 인하여 정보주체의 개인영상정보의 침해가 우려되는 경우에는 자체 점검 등을 통해 개인영상정보의 침해방지를 위해 적극 노력하여야 함
주요 확인사항	□ 개인영상정보의 안전한 처리를 위한 내부 관리계획을 수립하여 시행하고 있는가? □ 개인영상정보의 안전한 물리적 보관을 위한 별도 보관시설 마련 또는 잠금장치 설치하였는가? □ 개인영상정보에 대한 접근 통제 및 접근 권한 제한을 하고 있는가? (영상정보처리기기 운영자는 영상정보처리기기에 의하여 수집·처리되는 영상정보로의 접근권한을 관리책임자 등 지정된 최소한의 인원으로 제한)

2.3.5	이동형 영상정보처리기기로 촬영을 하는 경우 촬영 사실을 알리고 있는가?
점검기준	☑ 촬영 사실 표시 여부
증빙자료	☑ 촬영시 불빛, 소리, 안내판 등
관련근거	「개인정보 보호법」 제25조의2(이동형 영상정보처리기기의 설치운영 제한) ③ 「개인정보 보호법 시행령」 제27조의2(이동형 영상정보처리기기 촬영 사실 표시 등)
벌칙과태료	–
세부설명	□ 이동형 영상정보처리기기란 사람이 신체에 착용 또는 휴대하거나 이동 가능한 물체에 부착 또는 거치(据置)하여 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 대통령령으로 정하는 장치를 말함 ○ 착용형 장치: 안경 또는 시계 등 사람의 신체 또는 의복에 착용하여 영상 등을 촬영하거나 촬영한 영상정보를 수집·저장 또는 전송하는 장치 ○ 휴대형 장치: 이동통신단말장치 또는 디지털 카메라 등 사람이 휴대하면서 영상 등을 촬영하거나 촬영한 영상정보를 수집·저장 또는 전송하는 장치 ○ 부착·거치형 장치: 차량이나 드론 등 이동 가능한 물체에 부착 또는 거치(据置)하여 영상 등을 촬영하거나 촬영한 영상정보를 수집·저장 또는 전송하는 장치 □ 업무를 목적으로 이동형 영상정보처리기기를 운영하려는 요양기관은 공개된 장소에서 이동형 영상정보처리기기로 사람 또는 그 사람과 관련된 사물의 영상을 촬영하여서는 아니 됨 ○ 예외조건 – 제15조제1항 개인정보 수집·이용 조건 어느 하나에 해당하는 경우 – 촬영 사실을 명확히 고지하였으나 정보주체가 촬영 거부 의사를 밝히지 아니한 경우(정보주체의 권리를 부당하게 침해할 우려가 없고 합리적인 범위를 초과하지 않는 경우로 한정) – 그 밖에 제1호 및 제2호에 준하는 경우로서 대통령령으로 정하는 경우 – 인명의 구조·구급 등을 위하여 필요한 경우 및 그 밖에 제1호 및 제2호에 준하는 경우로서 대통령령으로 정하는 경우

	□ 이동형 영상정보처리기기로 사람 또는 그 사람과 관련된 사물의 영상을 촬영하는 경우에는 불빛, 소리, 안내판, 서면, 안내방송 등 대통령령으로 정하는 바에 따라 촬영 사실을 표시하고 알려야 함 ○ 이외 '영상정보처리기기 운영·관리방침', '영상정보의 이용 · 제공 · 열람 · 파기', '분실·도난·유출·변조 또는 훼손 등에 대한 안전성 확보 조치'는 고정형 영상정보처리기기의 규정을 준용
주요 확인사항	□ 이동형 영상정보처리기기로 사람 또는 그 사람과 관련된 사물의 영상(개인정보에 해당하는 경우로 한정)을 촬영하는 경우 불빛, 소리, 안내판, 안내서면, 안내방송 또는 그 밖에 이에 준하는 수단이나 방법으로 정보주체가 촬영 사실을 쉽게 알 수 있도록 표시하고 알리고 있는가 ?

2.4.1	업무 위탁 시 개인정보 처리 관련 필수사항 등을 계약서(문서)에 포함하였는가?
점검기준	☑ 위탁사업자별 계약서에 필수사항(7개) 포함 여부 확인
증빙자료	☑ 위탁사업자별 계약서(필수사항이 포함된 위·수탁 계약서, 협약서, 특약서 등) – 개인정보 처리방침(개인정보 처리업무 위탁 관련 공개 내역) – 개인정보 수집 양식 – 개인정보 처리위탁 계약서 – 재화 또는 서비스 홍보·판매 권유 업무 위탁 관련 정보주체 통지 내역
관련근거	「개인정보 보호법」 제26조(업무위탁에 따른 개인정보의 처리제한) ① 「개인정보 보호법 시행령」 제28조(개인정보의 처리 업무 위탁 시 조치) ①
벌칙·과태료	1천만 원 이하의 과태료
세부설명	□ 개인정보 처리 위탁 시 문서(계약서) 필수 기재사항 ① 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항 ② 개인정보의 기술적·관리적 보호조치에 관한 사항 ③ 위탁하는 업무의 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 수탁자가 준수해야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항 ※ (예시) 개인정보 위탁업무 – 진료신청서 처리사무, 진료비 수납사무, 연말정산 사무, 각종 증명서 발급 사무 등 개인정보 처리업무 위탁 – 전자차트 및 청구S/W 등의 유지보수, 혈액검사, CCTV 운영, 홈페이지 운영, 처방전 보관/폐기 등
주요 확인사항	□ 개인정보 처리업무를 제3자에게 위탁(재위탁 포함)하는 경우 문서(계약서)에 의한 위탁을 하고 있는가? □ 개인정보 처리 위탁 시 문서(계약서) 필수 기재사항이 포함 되어 있는가?

2.4.2	위탁에 관한 사실을 홈페이지 또는 사보, 접수실, 대기실 등에 공개하고 있는가?
점검기준	☑ 위탁에 관한 사실 공개(필수사항 포함) 여부 확인
증빙자료	☑ 위탁에 관한 사실을 공개한 증빙자료(개인정보 처리방침, 위탁계약서 등)
관련근거	「개인정보 보호법」 제26조(업무위탁에 따른 개인정보의 처리제한) ②③ 「개인정보 보호법 시행령」 제28조(개인정보의 처리 업무 위탁 시 조치) ②③④⑤
벌칙과태료	1천만 원 이하의 과태료
세부설명	□ 요양기관(개인정보처리자)은 위탁하는 업무의 내용과 수탁자를 정보주체가 언제든지 쉽게 확인 할 수 있도록 지속적으로 공개해야함 ○ 공개 필수사항: 수탁기관명, 위탁업무내용 ※ '수탁자'는 개인정보 처리 업무를 위탁받아 처리하는 자로부터 위탁받은 업무를 다시 위탁받은 제3자(재수탁자)를 포함 ○ 공개 방법 - 홈페이지(운영하는 기관만 해당) 내 위탁내역 게시 - 요양기관 내 공용장소(접수실, 대기실 등)에 게재 □ 개인정보 처리방침 내 '위탁에 관한 사실' 항목에 포함하여 작성 후 공개 가능함 □ 진료를 목적으로 타 요양기관 또는 검사기관에 개인정보 처리를 위탁하는 경우 환자(정보주체)의 동의를 받을 필요는 없으나, 별도 '개인정보 처리 위탁 계약서'를 작성하여 보관 필요
주요 확인사항	□ 개인정보 처리업무를 제3자에게 위탁(재위탁 포함)하는 경우 인터넷 홈페이지 등에 위탁하는 업무의 내용과 수탁자를 현행화하여 공개하고 있는가? □ 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 서면, 전자우편, 문자전송 등의 방법으로 위탁하는 업무의 내용과 수탁자를 정보주체에게 알리고 있는가?

2.4.3	수탁업체에 대한 관리 감독을 실시하고 있는가?
점검기준	☑ 수탁업체에 대한 개인정보 보호 교육 실시 여부 ☑ 수탁업체 대상 개인정보 처리 업무에 대한 점검·확인 여부
증빙자료	☑ 수탁업체 개인정보 보호 실태 점검표, 개인정보 보호 교육 결과 등
관련근거	「개인정보 보호법」 제26조(업무위탁에 따른 개인정보의 처리제한) ④
벌칙과태료	–
세부설명	□ 수탁업체 교육 ○ 환자(정보주체)의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 수탁자를 교육하여야 함 – 단, 수탁업체를 대상으로 교육이 현실적으로 어려운 경우 수탁업체의 자체 개인정보 보호 교육 실시 증빙서류를 받아 보관하는 것으로 대체할 수 있음 □ 수탁업체 관리·감독 ○ 수탁자(위탁받는 업체)의 개인정보 처리현황 및 실태, 목적 외 이용·제공 여부, 재위탁 여부, 안전성 확보조치 여부 등을 정기적으로 관리·감독하고 그 결과를 '수탁업체 개인정보 보호 실태 점검표'를 이용하여 기록·보관하여야 함 – 수탁업체를 대상으로 직접 관리·감독이 어려운 경우 수탁업체 자체적으로 개인정보의 안전성 확보조치 등에 대한 점검 등을 실시하여 그 결과를 '수탁업체 개인정보 보호 실태 점검표'를 제출 받아 보관하는 것으로 대체할 수 있음 □ 수탁자가 상시적으로 위탁업무를 처리하지 않는 경우, 계약서에 자체 교육 및 감독에 관한 사항을 명시하고 위탁업무 발생 시 보안서약서, 확인서 등 증빙자료를 확보하여야 함
주요 확인사항	□ 개인정보 처리업무를 위탁받은 수탁자가 관련 업무를 제3자에게 재위탁하는 경우 위탁자의 동의를 받도록 하고 있는가? □ 계약서에 자체 교육 및 감독에 관한 사항을 명시하였는가? □ 위탁업무 발생 시 보안서약서, 확인서 등 증빙자료 확보하였는가? □ 수탁업체 개인정보 보호 실태 점검표를 확인하였는가? □ 수탁업체 개인정보 보호 교육 결과 등을 확인 하였는가?

2.5.1	개인정보취급자에 대한 보안서약서를 징구하였는가?
점검기준	☑ 보안서약서 제출 여부 확인
증빙자료	☑ 개인정보취급자 목록 및 보안서약서(임직원, 외부인력) ☑ 비밀유지 서약서(퇴직자)
관련근거	「개인정보 보호법」 제28조(개인정보취급자에 대한 감독) ① 「표준 개인정보 보호지침」 제15조(개인정보취급자에 대한 감독) ①②③
벌칙과태료	–
세부설명	□ 정보자산을 취급하거나 접근권한이 부여된 임직원·임시직원·외부자 등이 내부 정책 및 관련 법규, 비밀유지 의무 등 준수사항을 명확히 인지할 수 있도록 업무 특성에 따른 정보보호 서약을 받아야 함 ○ 신규 인력 채용 시 정보보호 및 개인정보 보호 책임이 명시된 정보보호 및 개인정보 보호 서약서 징구 ○ 임시직원, 외주용역직원 등 외부자에게 정보자산에 대한 접근권한을 부여할 경우 정보보호 및 개인정보 보호에 대한 책임, 비밀유지 의무 등이 명시된 서약서 징구 ○ 임직원 퇴직 시 별도의 비밀유지에 관련한 서약서 징구 ○ 정보보호, 개인정보 보호 및 비밀유지 서약서는 안전하게 보관하고 필요시 쉽게 찾아볼 수 있도록 관리 필요
주요 확인사항	□ 신규 인력 채용 시 정보보호 및 개인정보보호 책임이 명시된 정보보호 및 개인정보보호 서약서를 받고 있는가? □ 임시직원, 외주용역직원 등 외부자에게 정보자산에 대한 접근권한을 부여할 경우 정보보호 및 개인정보보호에 대한 책임, 비밀유지 의무 등이 명시된 서약서를 받고 있는가? □ 임직원 퇴직 시 별도의 비밀유지에 관련한 서약서를 받고 있는가? □ 정보보호, 개인정보보호 및 비밀유지 서약서는 안전하게 보관하고 필요시 쉽게 찾아볼 수 있도록 관리하고 있는가?

2.5.2	개인정보취급자에 대한 정기적인 교육은 실시하고 있는가?
점검기준	☑ 내부관리계획 또는 연간 개인정보 보호 교육계획에 따른 교육 실시 여부 확인 (연 1회 이상 교육 실시)
증빙자료	☑ 개인정보 보호 교육 결과(교육 수료증, 교육 참석 서명록 등)
관련근거	「개인정보 보호법」 제28조(개인정보 취급자에 대한 감독) ② 「개인정보의 안전성 확보조치 기준」 제4조(내부관리계획의 수립·시행 및 점검) ②
벌칙과태료	–
세부설명	□ 개인정보취급자(직원 등)을 대상으로 매년 정기적으로 개인정보 보호 교육을 실시하여야 함 ○ 교육내용 및 방법은 요양기관 자체 내부관리계획(3.1.1 항목)에 따라 시행 – 교육대상: 개인정보 및 관련설비(서버, PC, CCTV등)에 직·간접적으로 접근하는 내부직원 및 외주용역업체 직원 등 모든 인력 포함 – 교육내용: 개인정보 수집 및 처리 방법 등 – 교육방법: 기관의 환경을 고려하여 집합교육, 인터넷 교육, 외부교육과정 참석, 전문 강사초빙 등 다양한 방법 활용
주요 확인사항	□ 임직원 채용 및 외부자 신규 계약 시 업무 시작 전에 개인정보보호 교육을 시행하고 있는가? □ 교육시행에 대한 기록을 남기고 교육 효과와 적정성을 평가하여 다음 교육 계획에 반영하고 있는가? □ 최소 연 1회 이상 교육을 수행하고 있는가? (특히, 개인정보취급자의 경우 법적 요구사항에 따라 연 1회 이상 개인정보보호 교육 필요)

2.6.1	개인정보 처리방침을 알기 쉽게 작성하고 보기 쉬운 곳(홈페이지, 접수대, 대기실 등)에 공개하고 있는가?
점검기준	☑ 필수항목을 포함한 개인정보 처리방침 수립 여부 ☑ 개인정보 처리방침 공개 여부
증빙자료	☑ 개인정보 처리방침 ☑ 개인정보 처리방침 공개 사실을 확인할 수 있는 자료(공지사항 게시판 등)
관련근거	「개인정보 보호법」 제30조(개인정보 처리방침의 수립 및 공개) ①② 제30조의2(개인정보 처리방침의 평가 및 개선권고) ① 3 「개인정보 보호법 시행령」 제31조(개인정보 처리방침의 내용 및 공개방법 등) ①②③
벌칙과태료	1천만 원 이하의 과태료
세부설명	□ 개인정보 처리방침 작성 기본 원칙 ○ 법령 부합성 – 개인정보처리자는 법 제30조 제1항 각 호 및 영 제31조 제1항 각 호의 사항 중 해당되는 내용을 모두 작성하여야 하며, 작성된 내용은 개인정보 보호 법령에 부합하여야 함 ○ 투명성 및 정확성 – 개인정보처리자는 정보주체의 알 권리 보장을 위해 자신의 개인정보 처리 현황을 정확하게 반영하여 개인정보 처리방침을 작성하고, 이를 투명하게 공개하여야 함 – 개인정보처리자는 개인정보 처리방침에 공개한 내용이 실제 개인정보 처리 현황과 일치할 수 있도록 하는 등의 정확성과 투명성, 최신성을 유지할 수 있도록 수립 및 관리하여야 함 ○ 명확성 및 가독성 – 개인정보처리자는 법 제30조 제1항 각 호 및 영 제31조 제1항 각 호의 사항을 정보주체가 쉽게 알 수 있도록 구분하여 작성해야 하며, 가급적 각각 별도의 항목으로 명시적으로 구분하여 작성할 것을 권고함 – 개인정보처리자는 개인정보 처리방침에 개인정보 처리 현황을 구체적으로 작성하여야 하며, 모호하고 불명확한 표현을 사용하는 것은 지양됨 – 개인정보 처리방침은 알기 쉬운 용어로 구체적이고 명확하게 표현되어야 하며(표준지침 제18조 제1항), 정보주체가 쉽게 이해할 수 있도록 가급적 평어체를 사용하고, 전문용어(법률용어 등)는 쉬운 표현으로 부연 설명을 제공하는 것을 권장함

	– 특히 개인정보 보호법의 적용을 받는 해외사업자의 경우 국내이용자가 이해할 수 있도록 쉽고 명확한 한글로 정보를 제공하여야 함 ○ 접근성 – 개인정보 처리방침은 정보주체 누구나 쉽게 확인할 수 있는 방법으로 공개되어야 함 – 개인정보 처리방침 상 정보주체 권리행사 방법은 개인정보를 수집하는 방법과 동일한 수준이거나 보다 쉬운 절차로 설계하고 구체적이고 상세하게 안내하여야 함 □ 개인정보 처리방침 기재사항 ① 제목 ② 개인정보의 처리 목적 ③ 처리하는 개인정보의 항목 ④ 14세 미만 아동의 개인정보 처리에 관한 사항(권장, 해당 시) ⑤ 개인정보의 처리 및 보유 기간 ⑥ 개인정보의 파기 절차 및 방법에 관한 사항 ⑦ 개인정보의 제3자 제공에 관한 사항(해당 시) ⑧ 추가적인 이용·제공이 지속적으로 발생 시 판단 기준(해당 시) ⑨ 개인정보 처리업무의 위탁에 관한 사항(해당 시) ⑩ 개인정보의 국외 수집 및 이전에 관한 사항(해당 시) ⑪ 개인정보의 안전성 확보조치에 관한 사항 ⑫ 민감정보의 공개 가능성 및 비공개를 선택하는 방법(해당 시) ⑬ 가명정보 처리에 관한 사항(해당 시) ⑭ 개인정보 자동 수집 장치의 설치·운영 및 그 거부에 관한 사항(해당 시) ⑮ 개인정보 자동 수집 장치를 통해 제3자가 행태정보를 수집하도록 허용하는 경우 그 수집·이용 및 거부에 관한 사항(권장, 해당 시) ⑯ 정보주체와 법정대리인의 권리·의무 및 행사방법에 관한 사항 ⑰ 자동화된 결정에 관한 사항(해당 시) ⑱ 개인정보 보호책임자의 성명또는 개인정보 업무 담당부서 및 고충사항을 처리하는 부서에 관한 사항 ⑲ 국내대리인 지정에 관한 사항(해당 시) ⑳ 정보주체의 권익침해에 대한 구제방법(권장) ㉑ 고정형 영상정보처리기기 운영·관리에 관한 사항(해당 시) ㉒ 이동형 영상정보처리기기 운영·관리에 관한 사항(해당 시)

㉓ 개인정보처리자가 개인정보 처리 기준 및 보호조치 등에 관하여 자율적으로 개인정보 처리방침에 포함하여 정한 사항

㉔ 개인정보 처리방침의 변경에 관한 사항

* 개인정보 포털(www.privacy.go.kr)의 '개인정보 처리방침 작성지침' 참조

□ 개인정보 처리방침은 환자(정보주체)가 언제든지 쉽게 확인할 수 있도록 홈페이지 게시 또는 기관 내 공용공간(대기실 등)에 비치 등을 통하여 공개하여야 함

○ 개인정보 처리방침 변경 시 변경내용 및 시행시기 등을 현행화하여야 함

□ 주요 개인정보 처리 표시(라벨링)는 중요한 처리 사항을 정보주체가 직관적으로 파악할 수 있도록 기호 등을 활용하여 표시하여야 함

※ 주요 개인정보 처리 표시(라벨링 예시)

주요 확인사항	□ 개인정보 처리방침을 법령에서 요구하는 내용을 모두 포함하여 알기 쉬운 용어로 구체적이고 명확하게 작성하였는가? □ 개인정보 처리방침을 정보주체가 쉽게 확인할 수 있도록 인터넷 홈페이지 등에 지속적으로 현행화하여 공개하고 있는가? □ 개인정보 처리방침이 변경되는 경우 사유 및 변경 내용을 지체 없이 공지하고 정보주체가 언제든지 변경된 사항을 쉽게 알아 볼 수 있도록 조치하고 있는가?

2.7.1	개인정보 보호책임자를 지정하여 개인정보 보호 총괄 업무를 수행하고 있는가?
점검기준	☑ 개인정보 보호책임자 지정 시 자격요건 준수 여부 확인 ☑ 개인정보 보호책임자의 교육이수, 관리 · 감독 활동 수행 여부 확인
증빙자료	☑ 개인정보 보호책임자 지정 및 역할 확인이 가능한 문서 – 내부관리계획, 업무 분장표, 직제표, 개인정보 처리방침 등 ☑ 개인정보 보호책임자 교육이수 증빙자료 ☑ 관리 · 감독 및 제도개선 활동 실적
관련근거	「개인정보 보호법」 제31조(개인정보 보호책임자의 지정) ①②③ 「개인정보 보호법 시행령」 제32조(개인정보 보호책임자의 업무 및 지정요건 등) ①③④ 「개인정보의 안전성 확보조치 기준」 제4조(내부관리계획의 수립·시행) ①
벌칙·과태료	1천만 원 이하의 과태료
세부설명	□ 개인정보처리자는 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 지정하여야 함 ○ 다만, 종업원 수, 매출액 등이 대통령령으로 정하는 기준*에 해당하는 개인정보처리자의 경우에는 지정하지 아니할 수 있음, 이 경우에는 사업주 또는 대표자가 개인정보 보호책임자가 됨 * 「소상공인기본법」 제2조제1항에 따른 소상공인 – 의원: 종업원 수 5인 미만 및 평균매출액 등 10억원 이하 – 약국(도소매업): 종업원 수 5인 미만 및 평균매출액 등 50억원 이하 (관련근거: 알기 쉽게 풀어 쓴 중소기업 범위해설, 2022, 중소벤처기업부) □ 개인정보 보호책임자의 자격 ○ 정보주체의 개인정보 보호업무를 위해 조직된 부서의 장 또는 개인정보 보호에 관한 소양이 있는 사람 ○ 사업주 또는 대표자, 임원(임원이 없는 경우에는 개인정보 처리 관련 업무를 담당하는 부서의 장) ○ 「의료법」 제3조의4에 따른 상급종합병원인 경우 개인정보보호 경력, 정보보호 경력, 정보기술 경력을 합하여 총 4년 이상 보유하고, 그 중 개인정보보호 경력을 최소 2년 이상 보유해야 함

	□ 개인정보 보호책임자의 권한 ○ 개인정보의 처리 현황, 처리 체계 등에 대하여 수시로 조사하거나 관계 당사자로부터 보고를 받을 수 있음 ○ 개인정보 보호책임자는 업무를 수행함에 있어서 정당한 이유 없이 불이익을 주거나 받아서는 안되며, 업무를 독립적으로 수행할 수 있도록 보장 받아야 한다. □ 개인정보 보호책임자의 주요업무 및 역할 ○ 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 오·남용 방지를 위한 내부통제시스템 구축 ○ 개인정보 보호 교육 계획의 수립 및 시행 ○ 개인정보파일의 보호 및 관리·감독 ○ 개인정보 처리방침의 수립·변경 및 시행 ○ 개인정보 처리와 관련된 인적·물적 자원 및 정보의 관리 ○ 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기 등 ○ 그 밖에 개인정보보호 관련 법령에서 명시하는 사항 □ 개인정보 보호책임자를 지정·변경한 경우 ○ 개인정보 보호책임자의 지정 및 변경 사실, 성명과 부서의 명칭, 전화번호 등 연락처를 개인정보 처리방침 등에 공개하여야 함. ○ 개인정보 보호책임자를 공개하는 경우 개인정보 보호와 관련한 고충처리 및 상담을 실제로 처리할 수 있는 연락처를 공개하여야 하며, 이 경우 개인정보 보호 업무 담당자의 성명, 부서의 명칭, 전화번호 등 연락처를 함께 공개할 수 있음.
주요 확인사항	□ 최고경영자는 개인정보보호 처리에 관한 업무를 총괄하여 책임질 최고책임자를 공식적으로 지정하고 있는가? □ 개인정보 보호책임자는 예산, 인력 등 자원을 할당할 수 있는 임원으로 지정하고 있으며, 관련 법령에 따른 자격요건을 충족하고 있는가?

2.7.2	개인정보 유출 등 발생에 대비한 대응절차를 숙지하고 있는가?
점검기준	☑ 개인정보 유출사고를 예방하고 사고 발생 시 신속하고 효과적으로 대응하기 위한 체계와 절차를 마련하고 있는지 여부 확인
증빙자료	☑ 개인정보 침해 및 유출 등을 대비한 대응 지침·절차·매뉴얼 ☑ 침해사고 대응 조직도 및 비상연락망
관련근거	「개인정보 보호법」 제34조(개인정보 유출통지 등) ①②③④ 「개인정보 보호법 시행령」 제39조(개인정보 유출 통지의 방법 및 절차) ①②③ 「개인정보 보호법 시행령」 제40조(개인정보 유출 신고의 범위 및 기관) ①②③ 「표준 개인정보 보호지침」 제26조(유출 등의 통지시기 및 항목) ①②③ 「표준 개인정보 보호지침」 제28조(유출 등의 신고) ①②③④
벌칙·과태료	3천만 원 이하의 과태료
세부설명	□ 개인정보가 유출 등 발생 시 정보주체에게 다음 내용을 통지 * (통지 규모) 단 1명의 정보주체에 관한 개인정보라도 유출 등이 된 경우 해당 ○ 유출 등이 된 개인정보의 항목 ○ 유출 등이 된 시점과 그 경위 ○ 유출 등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보 ○ 개인정보처리자의 대응조치 및 피해 구제절차 ○ 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처 – 72시간 이내 정보주체에게 통지, 다만 정당한 사유가 있는 경우에는 자신의 인터넷 홈페이지에 30일 이상 게시하는 것으로 통지를 갈음 □ 다음과 같은 상황이 발생한 경우에는 72시간 이내 개인정보 보호위원회 또는 전문기관(한국인터넷진흥원)에 신고하여야 함 ○ 1천명 이상의 정보주체에 관한 개인정보가 유출된 경우 ○ 민감정보, 고유식별정보가 유출등이 된 경우 ○ 외부로부터의 불법적인 접근에 의해 개인정보가 유출된 경우 ○ 다만, 유출등이 된 개인정보의 확산 및 추가 유출등을 방지하기 위하여 접속경로의 차단, 취약점 점검・보완, 유출등이 된 개인정보의 회수・삭제 등 긴급한 조치가 필요한 경우, 천재지변이나 그 밖에 부득이한 사유로 인하여 72시간 이내에 통지하기 곤란한 경우에는 해당 사유가 해소된 후 지체 없이 정보주체에게 알릴 수 있음.

□ 개인정보 유출 등 발생 시 대응 및 신고절차

단계	주요 내용
사고인지 및 긴급조치	▪ 개인정보 유출사고 신고 접수 및 사고인지 – 유출사고 발생이 의심되는 경우, 지체 없이 개인정보 보호 담당자에게 신고 ▪ 개인정보 보호 담당자는 사고 내용 등에 대해 개인정보 보호 책임자에게 보고 ▪ 개인정보 유출 신고 등 사고 신속 대응팀 구성 ▪ 피해 최소화를 위한 긴급조치 수행 – 유출된 개인정보 비공개 또는 삭제 조치 – 유출 접속 경로 차단, 취약점 점검 및 보완 등 긴급조치, 재발장지 조치 등
↓	
정보주체 유출통지	▪ 1건이라도 개인정보 유출 시, 정보주체에게 개인정보 유출사실 통지 (72시간 이내) – 유출된 개인정보의 항목, 유출된 시점과 그 경위, 피해 구제절차 등
↓	
개인정보 유출신고	▪ 1천명 이상의 정보주체에 관한 개인정보 유출 시 ▪ 민감정보 또는 고유식별정보 유출 시 ▪ 개인정보처리시스템 또는 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대한 외부로부터의 불법적인 접근에 의해 개인정보가 유출 등이 된 경우 ▪ 개인정보보호위원회 또는 한국인터넷진흥원에 유출신고(72시간 이내)
↓	
사고분석	▪ 사고 원인 분석, 유출 규모 확인, 사고 원인에 대한 조치
↓	
민원대응	▪ 민원대응을 위한 별도의 온/오프라인 창구 개설 및 운영 – 피해자 구제방안, 수사 진행상황 등에 대한 답변 방향 결정 및 응대 – 2차 비해 방지를 위한 조치방법 안내 및 피해구제 절차 안내
↓	
유출사고 결과보고	▪ 개인정보 유출 등 사고 결과보고서 작성 및 보고
↓	
개선 및 이행점검	▪ 개인정보 유출 등 사고 사례 전파 교육 및 개선(재발방지)

	□ 진료정보 침해사고의 통지 ○ 의료인 또는 의료기관 개설자는 전자의무기록에 대한 전자적 침해행위로 진료정보가 유출되거나 의료기관의 업무가 교란·마비되는 등 대통령령으로 정하는 사고(이하 "진료정보 침해사고"라 한다)가 발생한 때에는 보건복지부장관에게 즉시 그 사실을 통지하여야 함(「의료법」 제23조의3) ※ 통지 방법 예시 – 홈페이지에 '개인정보 유출 등 안내', '사과문' 등의 제목을 사용하고, 법에서 정한 통지 내용을 모두 포함하여 30일 이상 게시(홈페이지를 운영하지 아니하는 경우, 사업장 등의 보기 쉬운 장소에 30일 이상 게시) – 대규모 유출 등으로 72시간 이내 전체 통지가 기술적으로 불가능한 경우에는 홈페이지 팝업창 등을 통해 방문하는 이용자가 모두 알 수 있도록 현재까지 파악된 유출 등 사실을 게시를 하고 나서 추가적으로 해당 정보주체에게 개별적으로 통지 – 유출 등 통지를 할 때에는 정보주체가 실제 확인 가능하도록 이용 빈도가 높은 방법을 우선 활용하여 통지하는 것이 바람직하며, 휴대전화번호를 보유하고 있는 경우에는 전화통화 및 문자 등을 활용하고 곤란한 경우에는 이메일, 팩스, 우편 등의 방법을 활용
주요 확인사항	□ 침해사고 및 개인정보 유출사고를 예방하고 사고 발생 시 신속하고 효과적으로 대응하기 위한 체계와 절차를 마련하고 있는가? □ 침해사고 및 개인정보 유출의 징후 또는 발생을 인지한 경우 정의된 침해사고 대응절차에 따라 신속하게 대응 및 보고가 이루어지고 있는가? □ 개인정보 침해사고 발생 시 관련 법령에 따라 정보주체 통지 및 관계기관 신고 절차를 이행하고 있는가? □ 침해사고가 종결된 후 사고의 원인을 분석하여 그 결과를 보고하고 관련 조직 및 인력과 공유하고 있는가?

2.8.1	**개인정보 유출 등 발생 시 손해배상책임 이행이 보장될 수 있도록 보험 등에 가입하거나 준비금을 적립하고 있는가?**
점검기준	☑ 개인정보 유출 등 발생으로 소송 등에 대비하여 손해 배상책임 이행이 보장될 수 있도록 보험 등에 가입하거나 준비금을 적립하고 있는지 여부 * (대상) 전년도 매출액 10억원 이상, 저장관리하는 정보주체 수 일일평균 1만명 이상 요양기관
증빙자료	☑ 개인정보 손해배상 책임보장 입증 자료 (개인정보보호배상책임보험, 사이버종합배상보험 약정서 등) ☑ 준비금, 임의적립금을 확인 할 수 있는 자료
관련근거	「개인정보 보호법」 제39조(손해배상책임) ①③ 「개인정보 보호법」 제39조의2(법정손해배상의 청구) ①②③ 「개인정보 보호법」 제39조의7(손해배상의 보장) ①② 「개인정보 보호법 시행령」 제48조의7(손해배상책임의 이행을 위한 보험 등 가입 대상자의 범위 및 기준 등) ①②③④
벌칙·과태료	3천만 원 이하의 과태료
세부설명	□ 「개인정보 보호법」에서는 민간·공공 분야 개인정보처리자의 손해배상책임 이행을 보장하도록 보험 또는 공제(이하 '보험 등'이라 함)에 가입하거나 준비금을 적립하도록 의무화 ○ 「개인정보 보호법 시행령」에서는 법에서 위임한 의무대상 사업자의 범위, 가입금액 기준 등 마련 □ 적용대상 ○ 다음 각 호의 요건을 모두 갖춘 개인정보처리자 – 직전 사업연도의 매출액이 10억원 이상일 것 – 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 정보주체 수가 일일평균 1만명 이상일 것 □ 연 매출 10억원 이상 되면서 동시에 저장·관리되고 있는 정보주체 수가 1만명 이상인 모든 약국, 의원·병원은 유사 시, 정보주체에 대한 손해배상책임 이행을 보장하도록 보험 또는 공제에 가입하거나 준비금을 적립하여야 함 □ 면제대상(소상공인) 「소상공인기본법」 제2조 제1항에 따른 소상공인으로 아래의 요건을 갖춘 자에게 개인정보 저장·관리업무를 위탁한 경우 의무 면제

	1. 「소상공인기본법」 제2조 제1항에 따른 소상공인으로부터 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 개인정보의 저장·관리 업무를 위탁 받은 자 2. 1호에 따라 위탁받은 업무에 대하여 「개인정보보호법」 제39조 및 제39조의2에 따른 손해배상책임의 이행을 보장하는 보험 또는 공제에 가입하거나 준비금을 적립하는 등 필요한 조치를 한 자 □ 준비금 적립 방법 ○ 임의적립금(자본계정)으로 적립하고 주주총회 결의 등을 통해 해당 임의적립금이 「개인정보 보호법」 제39조의7의 의무 이행을 위한 것임을 명확히 하여야 함 ▪ 준비금: 회사가 순자산액으로부터 자본액을 공제한 금액(잉여금) 중 일부를 장래 생길지도 모르는 필요에 대비하기 위하여 회사에 적립해 두는 금액 ▪ 임의적립금: 법률이 아닌 정관/주주총회의 결의에 의하여 이익을 유보한 것으로, 그 이용 목적과 방법은 회사에서 자유롭게 정할 수 있음 □ 다른 법률에 따른 의무보험 등과의 관계 ○ 다른 법률에 따라 손해배상책임의 이행을 보장하는 보험 등에 가입 하거나 준비금을 적립한 개인정보처리자는 「개인정보 보호법」에 따른 보험 등 가입 또는 준비금 적립 등의 조치를 아니할 수 있음(개인정보보호법 제39조, 제39조의2 및 제39조의7에서 정한 개인정보보호 손해배상책임 범위를 충족하여야 함)
주요 확인사항	□ 개인정보 보호법에 따라 개인정보 손해배상책임 보장제도 적용 대상이 이를 인지하고 보험 가입이나 준비금 적립을 하였는가? □ 이용자 수 및 매출액에 따른 최저가입금액 기준을 준수하였는가?

지표별 가이드

Ⅲ. 개인정보의 안전한 관리

3.1. 내부관리 계획수립·시행

3.2. 접근권한 관리

3.3. 접근통제

3.4. 개인정보 암호화

3.5. 접속기록 보관

3.6. 보안프로그램 설치운영

3.7. 물리적 접근방지

3.8. 재해·재난 대비 안전조치

<table>
<tr><td>3.1.1</td><td colspan="3">개인정보의 안전한 처리를 위한 내부 관리계획을 수립·시행 및 점검을 하고 있는가?</td></tr>
<tr><td>점검기준</td><td colspan="3">☑ 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 필수사항(16개)을 포함하는 내부 관리계획을 수립·시행하는지 여부 확인
* 1만명 미만의 정보주체에 관하여 개인정보를 처리하는 소상공인 · 개인 · 단체의 경우는 내부 관리계획 수립 생략 가능</td></tr>
<tr><td>증빙자료</td><td colspan="3">☑ (필수제출) 승인된 내부관리계획서(필수 반영 사항 포함)</td></tr>
<tr><td>관련근거</td><td colspan="3">「개인정보 보호법」 제29조(안전조치 의무)
「개인정보의 안전성 확보조치 기준」 제4조(내부 관리 계획의 수립시행 및 점검) ①</td></tr>
<tr><td>벌칙·과태료</td><td>3천만 원 이하의 과태료</td><td>고유식별정보 안전조치 관리실태 점검 항목(증빙필수)</td><td>4</td></tr>
<tr><td>세부설명</td><td colspan="3">□ 내부 관리계획 수립·시행 및 점검
○ 개인정보의 안전한 처리를 위해 개인정보 보호책임자의 의무와 책임, 개인정보 처리단계별 기술적·관리적 안전조치, 개인정보 교육, 개인정보 침해대응 및 피해구제 등과 같은 개인정보보호 의무를 위한 내부 관리계획서 수립·시행
○ 내부 관리계획의 문서 제목은 가급적 “내부 관리계획”이라는 용어를 사용하는 것이 바람직하나, 개인정보처리자의 내부 방침에 따라 다른 용어를(개인정보 보호지침 등) 사용 가능
○ 내부 관리계획은 전사적인 계획 내에서 개인정보가 관리될 수 있도록 최고경영층으로부터 내부결재 등의 승인을 받아 모든 임직원 및 관련자에게 알림으로써 이를 준수할 수 있도록 하여야 함
○ 개인정보 보호책임자는 연 1회 이상 내부 관리계획의 이행 실태를 점검 관리하여야 함
○ 개인정보처리자는 내부 관리계획의 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부 관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 함</td></tr>
</table>

	□ 내부 관리계획 필수 사항 1. 개인정보 보호 조직의 구성 및 운영에 관한 사항 2. 개인정보 보호책임자의 자격요건 및 지정에 관한 사항 3. 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항 4. 개인정보취급자에 대한 관리·감독 및 교육에 관한 사항 5. 접근 권한의 관리에 관한 사항 6. 접근통제에 관한 사항 7. 개인정보의 암호화 조치에 관한 사항 8. 접속기록 보관 및 점검에 관한 사항 9. 악성프로그램 등 방지에 관한 사항 10. 개인정보의 유출, 도난 방지 등을 위한 취약점 점검에 관한 사항 11. 물리적 안전조치에 관한 사항 12. 개인정보 유출사고 대응 계획 수립·시행에 관한 사항 13. 위험 분석 및 관리에 관한 사항 14. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항 15. 개인정보 내부 관리계획의 수립, 변경 및 승인에 관한 사항 16. 그 밖에 개인정보 보호를 위하여 필요한 사항
주요 확인사항	□ 개인정보의 안전한 처리를 위해 개인정보 보호책임자의 의무와 책임, 개인정보 처리단계별 기술적 · 관리적 안전조치, 개인정보 교육, 개인정보 침해대응 및 피해구제 등과 같은 개인정보보호 의무를 위한 내부 관리계획서에 필수 사항을 수립 및 시행 여부를 확인하는가? □ 내부 관리계획은 전사적인 계획 내에서 개인정보가 관리될 수 있도록 최고경영층으로부터 내부결재 등의 승인을 받았는가? 아울러, 모든 임직원 및 관련자에게 알렸는가? □ 개인정보 보호책임자는 연 1회 이상 내부 관리계획의 이행 실태를 점검 관리를 하는가?

3.2.1	**개인정보처리시스템에 (전자차트, 청구S/W 등) 대한 접근 권한을 업무수행에 필요한 최소한의 범위로 업무 담당자에게 차등 부여하고 있는가?**		
점검기준	☑ 개인정보처리시스템에 대한 접근 권한을 업무수행에 필요한 최소한의 범위로 업무 담당자에게 차등 부여하고 있는지 확인		
증빙자료	☑ 접속계정(ID) 등록 현황 및 부여된 권한내역 자료(사용자ID관리대장) 또는 화면 캡처		
관련근거	「개인정보 보호법」 제29조(안전조치 의무) 「개인정보의 안전성 확보조치 기준」 제5조(접근 권한의 관리) ①		
벌칙과태료	3천만 원 이하의 과태료	고유식별정보 안전조치 관리실태 점검 항목	5
세부설명	□ 개인정보처리시스템에 대한 접근 권한은 개인정보취급자에게만 업무 수행에 필요한 최소한의 범위로 차등 부여 □ 개인정보처리시스템에 접근 가능한 개인정보취급자를 식별 ○ 식별된 개인정보취급자의 접근 권한, 개인정보 다운로드 권한이 업무 목적에 적합한 최소한의 범위로 부여되어 있는지 접근 권한 관리 테이블, 접근 권한 관리 대장 등을 확인 ※ 개인정보처리시스템에 기능이 없다면 수기문서로 관리 사용자 권한관리 부서명 권한상태 ○ 반려포함 ○ 반려제외 조회 결과 번호 부서 사용자 계정 업무 접근권한 변경일시 변경사유 처리자 1 원무과 김 장 k 3 환자관리 환자정보(입력, 조회, 수정, 삭제) 2021-08-10 10:00 입사 병원장 2 A병동 김 정 ka 3 환자관리 환자정보(입력, 조회, 수정, 삭제) 2021-12-22 15:45 부서변경 병원장 3 원무과 이 리 k 5 환자관리 환자정보(입력, 조회, 수정) 2022-05-06 16:50 입사 병원장 4 B병동 최 장 ch 6 환자관리 환자정보(입력, 조회) 2023-09-10 09:25 부서변경 병원장 5 원무과 박 원 pa 9 환자관리 환자정보(입력) 2024-03-15 14:06 입사 병원장 6 C병동 정 원 ju 9 환자관리 환자정보(입력) 2024-08-22 09:30 입사 병원장		
주요 확인사항	□ 개인정보처리시스템에 대한 접근 권한이 업무 목적에 적합한 최소한의 범위로 부여되었는가?		

3.2.2	**개인정보취급자 또는 개인정보취급자의 업무 변경 시, 지체없이 개인정보처리 시스템에 대한 접근 권한을 변경 또는 말소하고 있는가?**		
점검기준	☑ 개인정보취급자 또는 개인정보취급자의 업무 변경 시, 개인정보처리시스템의 접근 권한을 지체없이 변경 또는 말소하는지 확인		
증빙자료	☑ 개인정보처리시스템 내 접근권한 관리 테이블 ☑ 접근권한 관리대장 / 퇴직 및 인사이동 점검표		
관련근거	「개인정보 보호법」 제29조(안전조치 의무) 「개인정보의 안전성 확보조치 기준」 제5조(접근 권한의 관리) ②		
벌칙·과태료	3천만 원 이하의 과태료	고유식별정보 안전조치 관리실태 점검 항목	6
세부설명	□ 정보시스템과 개인정보 및 중요정보에 대한 비인가 접근을 통제하기 위하여 다음 사항을 고려하여 공식적인 사용자 계정 및 접근권한 등록·변경·삭제·해지 절차를 수립·이행하여야 함. ○ 사용자 및 개인정보취급자별로 고유한 사용자 계정 발급 및 공유 금지 ○ 사용자 및 개인정보취급자에 대한 계정 발급 및 접근권한 부여·변경 시 승인 절차 등을 통한 적절성 검토 ○ 전보, 퇴직 등 인사이동 발생 시 지체 없이 접근권한 변경 또는 말소 (계정 삭제 또는 비활성화 포함) ○ 정보시스템 설치 후 제조사 또는 판매사의 기본 계정, 시험 계정 등은 제거하거나 추측하기 어려운 계정으로 변경 ○ 사용자 계정 및 접근권한의 등록·변경·삭제·해지 관련 기록의 유지·관리		
주요 확인사항	□ 개인정보 내부 관리계획에 접근 권한의 변경・말소에 관한 사항을 반영하여 수립・시행하고 있는가? □ 조직 내의 임직원의 전보 또는 퇴직, 휴직 등 인사이동 발생 시 해당 인력의 계정을 지체없이 변경 또는 말소하고 있는가?		

3.2.3	**개인정보처리시스템(전자차트, 청구S/W 등) 접근 권한의 부여·변경·말소 내역 등을 최소 3년간 보관하고 있는가?**		
점검기준	☑ 개인정보처리시스템에 대한 개인정보취급자의 접근 권한 부여 및 전보 또는 퇴직에 따른 변경, 말소에 대한 기록을 최소 3년간 보관하고 있는지 확인		
증빙자료	☑ (필수제출) 접근 권한 변경·말소 내역 최소 3년간 보관 증빙 화면 또는 관리 기록		
관련근거	「개인정보 보호법」 제29조(안전조치 의무) 「개인정보의 안전성 확보조치 기준」 제5조(접근 권한의 관리) ③		
벌칙·과태료	3천만 원 이하의 과태료	고유식별정보 안전조치 관리실태 점검 항목(증빙필수)	7
세부설명	□ 권한 부여·변경 또는 말소에 대한 내역을 기록하고 최소 3년간 보관 □ 전보 또는 퇴직 등 인사이동이 발생하여 직원(개인정보취급자)이 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소 ※ 개인정보처리시스템에 기능이 없다면 수기문서로 관리		

번호	부서	사용자	계정	업무	접근권한	변경일시	변경사유	처리자
1	원무과	김 장	ki 3	환자관리	환자정보(입력, 조회, 수정, 삭제)	2021-08-10 10:00	입사	병원장
2	A병동	강 장	ka 23	환자관리	환자정보(입력, 조회, 수정, 삭제)	2021-12-22 15:45	부서변경	병원장
3	원무과	이 리	le 6	환자관리	환자정보(입력, 조회, 수정)	2022-05-06 16:50	입사	병원장
4	B병동	최 장	ch 36	환자관리	환자정보(입력, 조회)	2023-09-10 09:25	부서변경	병원장
5	원무과	박 원	pa 39	환자관리	환자정보(입력)	2024-03-15 14:06	입사	병원장
6	C병동	정 원	ju 39	환자관리	환자정보(입력)	2024-08-22 09:30	입사	병원장

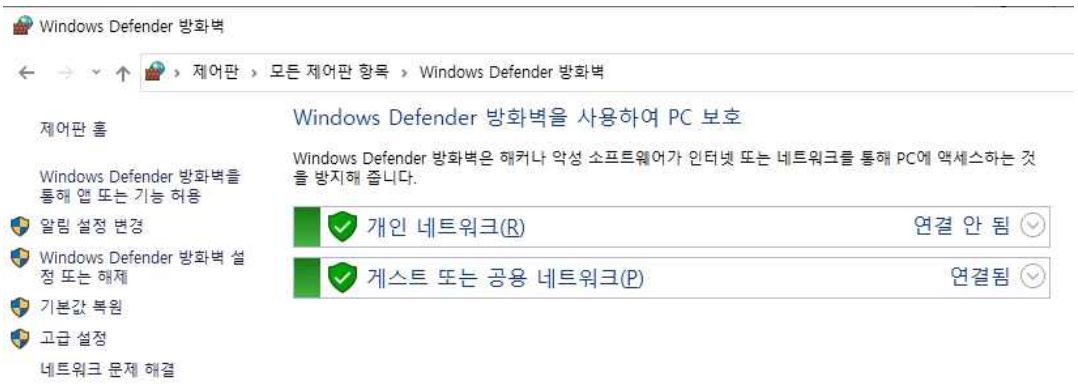
주요 확인사항	□ 개인정보처리시스템 구축 이후 최소 3년간 접근 권한 부여·변경·말소 내역 기록 여부를 확인하였는가?

3.2.4	**개인정보취급자별로 개인정보처리시스템에 대한 사용자계정(ID)을 발급하고 해당 사용자계정을 다른 개인정보취급자 등과 공유하고 있지는 않는가?**		
점검기준	☑ 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 취급자별로 한 개의 사용자계정을 발급하고 다수의 사용자가 공유하는지 여부 확인(1인 1계정 부여, 계정공유금지)		
증빙자료	☑ 개인정보처리시스템 관리자, 사용자, 개인정보취급자 계정 목록		
관련근거	「개인정보 보호법」 제29조(안전조치 의무) 「개인정보의 안전성 확보조치 기준」 제5조(접근 권한의 관리) ④		
벌칙·과태료	3천만 원 이하의 과태료	고유식별정보 안전조치 관리실태 점검 항목	8
세부설명	□ 개인정보취급자를 식별하고, 계정이 개별로 발급되었는지 확인 ○ 개인정보처리시스템에서 고유식별정보에 접근 가능한 개인정보취급자를 식별 ○ 개인정보처리시스템에 접속할 수 있는 사용자계정이 개인정보취급자별로 발급되었는지 확인 □ 동일 계정 동시 사용 시 제한 여부 확인(계정 공유 여부 확인) ○ 발급된 계정을 여러 사람이 동시에 사용할 수 없도록 시스템 상 제한하고 있는지 확인		
주요 확인사항	○ 사용자 및 개인정보취급자별로 고유한 사용자 계정 발급 및 공유를 금지하고 있는가?		

<table>
<tr><td>3.2.5</td><td colspan="3">개인정보취급자 또는 정보주체의 비밀번호 등 인증수단을 안전하게 적용하고 관리하고 있는가?</td></tr>
<tr><td>점검기준</td><td colspan="3">☑ 개인정보취급자 또는 정보주체의 비밀번호 등 인증수단을 안전하게 적용하고 관리하고 있는지 여부 확인</td></tr>
<tr><td>증빙자료</td><td colspan="3">☑ 비밀번호 관리 정책 및 절차 등 인증 수단, 비밀번호 설정 화면 등</td></tr>
<tr><td>관련근거</td><td colspan="3">「개인정보 보호법」 제29조(안전조치 의무)
「개인정보의 안전성 확보조치 기준」 제5조(접근 권한의 관리) ⑤</td></tr>
<tr><td>벌칙·과태료</td><td>3천만 원 이하의 과태료</td><td>고유식별정보 안전조치 관리실태 점검 항목</td><td>9</td></tr>
<tr><td>세부설명</td><td colspan="3">□ 사용자 및 관리자가 안전한 비밀번호를 설정하여 사용할 수 있도록 비밀번호 관리절차 및 작성규칙을 수립·이행
○ 비밀번호 작성규칙(불가피한 경우를 제외하고는 시스템적으로 강제화)
<table>
<tr><th>구 분</th><th>내 용</th></tr>
<tr><td>조합 규칙 적용</td><td>▪ 영문, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 8자리 이상
▪ 문자로만 구성한 경우 최소 10자리 이상 (단, 숫자로만 구성할 경우 취약할 수 있음)</td></tr>
<tr><td>변경주기 설정</td><td>▪ 비밀번호 유효기간을 최소 3개월 마다 설정하여 주기적으로 변경(단, 주기적 변경 여부 및 변경주기는 위험평가 결과 등을 고려하여 자체적으로 결정)</td></tr>
<tr><td>추측하기 쉬운 비밀번호 설정 제한</td><td>▪ 동일한 문자 반복, 키보드 상에서 나란히 있는 문자열(qwer), 일련번호, 연속적인 숫자(12345678), 생일, 전화번호 등 추측하기 쉬운 개인정보 및 ID와 비슷한 비밀번호 사용 제한</td></tr>
<tr><td>동일한 비밀번호 재사용 제한</td><td>▪ 비밀번호 변경 시 이전에 사용한 비밀번호 재사용 제한</td></tr>
</table></td></tr>
<tr><td>주요 확인사항</td><td colspan="3">□ 개인정보처리시스템, 접근통제시스템, 인터넷 홈페이지 등에 정당한 권한을 가진 개인정보 취급자 또는 정보주체를 인증하기 위해 인증수단을 안전하게 적용하고 있는가?
□ 개인정보처리자는 적용된 인증수단에 대하여 정당한 접근 권한을 가지지 않은 자가 추측하거나 탈취하는 등 접근이 어렵도록 적용하고 관리하고 있는가?</td></tr>
</table>

3.2.6	**개인정보취급자 또는 정보주체가 일정 횟수 이상 인증에 실패한 경우, 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 조치를 하고 있는가?**		
점검기준	☑ 개인정보처리시스템 접속 시 일정 횟수 이상 인증에 실패한 경우, 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 조치를 하고 있는지 확인		
증빙자료	☑ 정보시스템 및 개인정보처리시스템에 대한 접근 시 사용자 인증, 로그인 횟수 제한, 불법 로그인 시도 경고 등 또는 메시지 화면 캡처 등		
관련근거	「개인정보 보호법」 제29조(안전조치 의무) 「개인정보의 안전성 확보조치 기준」 제5조(접근 권한의 관리) ⑥		
벌칙과태료	3천만 원 이하의 과태료	고유식별정보 안전조치 관리실태 점검 항목	10
세부설명	□ 개인정보처리자는 권한 있는 개인정보취급자 또는 정보주체만이 개인정보처리시스템에 접근할 수 있도록 일정 횟수 이상 인증에 실패한 경우 개인정보처리시스템에 대한 접근을 제한 적용 ※ 인증 실패횟수는 개인정보처리시스템의 특성 및 위험성 등을 고려하여 정할 수 있음(예: 5회 등) ※ 개인정보취급자 또는 정보주체에게 개인정보처리시스템에 대한 접근을 재부여하는 경우에도 반드시 개인정보취급자 여부를 확인 후 계정 잠금 해제 등의 조치가 필요함		
주요 확인사항	□ 개인정보처리시스템에 일정 횟수 이상 인증에 실패하는 경우 등에 대한 접근을 제한하는가?		

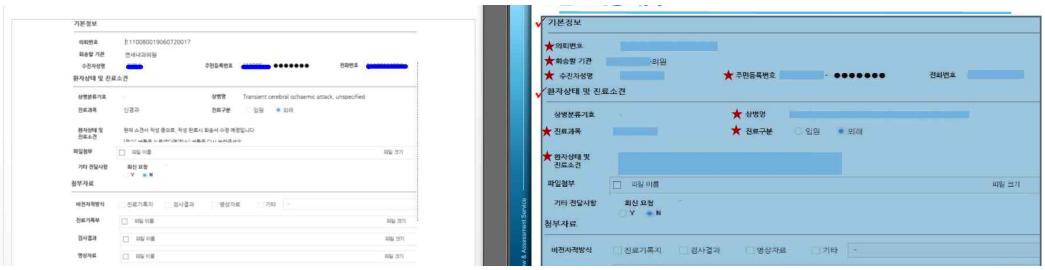
3.3.1	정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하고 있는가?		
점검기준	☑ 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속권한을 IP주소로 제한하는지 여부 확인		
증빙자료	☑ (서버급 이상) 침입통제시스템을 도입한 경우 정책적용 내역 ☑ (업무용 컴퓨터) 컴퓨터 운영체제(Windows OS 등) 및 백신프로그램에서 제공하는 방화벽 설정 화면 캡처		
관련근거	「개인정보 보호법」 제29조(안전조치의무) 「개인정보의 안전성 확보조치 기준」 제6조(접근통제) ① 1		
벌칙과태료	3천만 원 이하의 과태료	고유식별정보 안전조치 관리실태 점검 항목	11
세부설명	□ 개인정보처리시스템 접근통제 정책 적용 ○ 개인정보처리시스템에 지정된 IP만 접근할 수 있도록 설정 ○ 단순 ID별, 사용자 그룹별 접근제한이 아닌 IP(Internet protocol)주소, 포트(Port), MAC(Media Access Control) 주소로 제한 □ 침입차단시스템 등을 통한 개인정보처리시스템의 접근통제 ○ (침입차단 기능) 개인정보처리시스템에 대한 접속권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한 * (예시) 방화벽, N/W장비 ACL 등 ○ 불법적인 접근 및 침해사고 방지를 위해서는 침입차단 및 침입탐지 기능을 갖는 장비의 설치 등과 더불어 적절한 침입차단 및 침입탐지 정책 설정, 로그 분석 및 이상 행위 대응, 로그 훼손 방지 등 적절한 운영·관리 필요 - 서비스 제공 및 운영을 위해 필요한 IP, Port만 허용 □ 업무용 컴퓨터에 아래 3가지 중 반드시 1가지 이상 적용 ○ 컴퓨터의 운영체제(윈도우 등)의 기본 기능을 이용하여 방화벽 사용 * 윈도우의 [설정] - [제어판] - [Windows방화벽] '사용' 클릭 ○ 보안프로그램(알약, V3 등)의 방화벽 사용 ○ 보안업체에서 제공하는 보안 서비스 (침입방지시스템 등)		
주요 확인사항	□ 운영중인 개인정보처리시스템에 접근통제 정책을 적용하고 있는가?		

3.3.2	**정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 접속한 IP주소 등을 분석하여 개인정보 유출시도를 탐지 및 대응하고 있는가?**		
점검기준	☑ 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 IP 주소 등을 분석하여 개인정보 유출 시도 탐지 및 대응하고 있는지 여부 확인		
증빙자료	☑ 침입탐지시스템 또는 침입방지시스템 화면 캡처 등		
관련근거	「개인정보 보호법」 제29조(안전조치의무) 「개인정보의 안전성 확보조치 기준」 제6조(접근통제) ① 2		
벌칙과태료	3천만 원 이하의 과태료	고유식별정보 안전조치 관리실태 점검 항목	12
세부설명	□ 침입탐지시스템 및 침입방지시스템을 설치하여 운영 ○ 스위치 등의 네트워크 장비에서 제공하는 ACL(Access Control List: 접근제어목록) 등 기능을 이용하여 IP주소 등을 제한함으로써 침입차단 기능을 구현할 수 있음 ○ 공개용 소프트웨어를 사용하거나, 운영체제(OS)에서 제공하는 기능을 활용하여 해당 기능을 포함한 시스템을 설치·운영하는지 확인 (다만, 공개용 소프트웨어를 사용하는 경우 보안기능을 사전에 점검하고 정기적인 업데이트 여부 등 확인 후 적용 필요) * (예시) IDS(침입탐지시스템), IPS(침입방지시스템), UTM(침입차단시스템), WAF(웹방화벽) 등 ○ 인터넷데이터센터(IDC), 클라우드 서비스, 보안업체 등에서 제공하는 보안서비스 등도 활용 가능 ○ 불법적인 데이터가 탐지되면 관리자에게 보고 후 대응·조치하여야 함 ※ Windows 방화벽(예시)  		

	※ 백신 방화벽(예시)
주요 확인사항	□ 침입탐지시스템 및 침입방지시스템을 설치하였는가?

3.3.3	**외부에서 개인정보취급자가 정보통신망을 통해 개인정보처리시스템에 접속 시, 인증서, 보안토큰, 일회용비밀번호 등 안전한 인증수단을 적용하고 있는가?**		
점검기준	☑ 외부에서 정보통신망을 통한 접속 시 인증서, 보안토큰, 일회용 비밀번호 등 안전한 인증수단 제공 여부 확인		
증빙자료	☑ (필수제출) 외부에서 개인정보처리시스템 접속 시 인증 화면 캡처 등		
관련근거	「개인정보 보호법」 제29조(안전조치 의무) 「개인정보의 안전성 확보조치 기준」 제6조(접근통제) ②		
벌칙·과태료	3천만 원 이하의 과태료	고유식별정보 안전조치 관리실태 점검 항목(증빙필수)	13
세부설명	□ 외부에서 접근 가능한 개인정보처리시스템을 운영하는 경우 ○ 외부에서 개인정보처리시스템에 접속*하여 이용자**의 개인정보를 처리하거나, 이용자가 아닌 정보주체의 개인정보를 처리하는 경우가 있는지 확인 * 출장, 재택근무 등 기관 외 장소에서 개인정보처리시스템에 접근하는 경우 ** 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제4호에 따른 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자 □ 이용자의 개인정보를 처리하는 개인정보처리시스템에 접속 시 안전한 인증수단 적용 ○ 외부에서 개인정보처리시스템에 접속하여 이용자의 개인정보를 처리하는 경우가 있는지 확인 ○ 외부에서 개인정보처리시스템에 접속 시 아이디/비밀번호 입력 외에 추가로 안전한 인증수단을 통해 접속하는지 확인 – 안전한 인증수단: 인증서(PKI), 일회용 비밀번호(OTP), 보안토큰 등 □ 이용자가 아닌 정보주체의 개인정보를 처리하는 개인정보처리시스템에 접속 시 안전한 접속 수단 또는 안전한 인증수단 적용 여부 확인 ○ 외부에서 개인정보처리시스템에 접속 시 안전한 접속수단 또는 안전한 인증수단을 적용 – 안전한 접속수단: 가상사설망(VPN), 전용선 등 – 안전한 인증수단: 인증서(PKI), 일회용 비밀번호(OTP), 보안토큰 등		
주요 확인사항	□ 외부에서 개인정보처리시스템에 접속 시 안전한 접속수단 및 인증수단을 적용하고 있는가?		

3.3.4	**개인정보가 인터넷 홈페이지, P2P, 공유설정 등으로 유출되지 않도록 개인정보처리시스템, 개인정보취급자 컴퓨터 등에 접근통제 조치를 하고 있는가?**		
점검기준	☑ 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람 권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터, 모바일 기기 등에 조치하는지 여부 확인		
증빙자료	☑ (업무용 컴퓨터) 백신 유해사이트 차단, 공유폴더 제거 화면 캡처 등 ☑ (서버급 이상) 비업무사이트(P2P 등) 차단시스템 관리화면 캡처 등		
관련근거	「개인정보 보호법」 제29조(안전조치 의무) 「개인정보의 안전성 확보조치 기준」 제6조(접근통제) ③		
벌칙과태료	3천만 원 이하의 과태료	고유식별정보 안전조치 관리실태 점검 항목	14
세부설명	□ 인터넷 홈페이지 운영 시 개인정보 유·노출 방지 대책 마련 및 조치 ○ 웹 취약점 점검 및 취약점 발견 시 개선 조치 ○ 인터넷 홈페이지 중 사용되지 않거나 관리되지 않는 사이트 또는 URL을 삭제·차단 조치 ○ 인터넷 홈페이지 관리자 페이지가 외부에 노출되지 않도록 조치 ○ 웹 방화벽 설치·운영을 통한 개인정보 유·노출을 탐지 및 차단 □ P2P, 웹하드, 공유설정 등 사용가능 여부를 확인 ○ 원칙적으로 P2P 사용은 금지이며, 잘 알려진 공유 프로그램에 대해서는 반드시 보안장비의 접근통제 정책 적용이 필요 ○ P2P, 공유설정이 업무상 꼭 필요한 경우라도 드라이브 전체 또는 불필요한 폴더가 공유되지 않도록 조치하고, 공유폴더에 개인정보 파일이 포함되지 않도록 정기적으로 점검하여야 함 ※ P2P, 웹하드 등의 사용을 제한하는 경우에도 단순히 사용금지 조치를 취하는 것이 아닌 시스템 상에서 해당 포트를 차단하는 등 근본적인 안전조치를 취하는 것이 필요		
주요 확인사항	□ 개인정보처리시스템, 업무용 컴퓨터 및 모바일 기기 등에서 취급중인 개인정보가 인터넷, P2P, 공유설정, 공개된 무선망(Wifi) 이용 등의 외부 경로에서 유출되지 않도록 조치하였는가? □ 공유폴더 이용하는 업무 진행 시 공유폴더 암호 설정 및 사용 후 공유폴더를 해제하였는가?		

3.3.5	홈페이지의 개인정보 노출 방지를 위한 보안 조치를 실시하고 있는가?
점검기준	☑ 홈페이지 개인정보 노출방지 점검 및 보안 조치 여부 확인 ☑ 홈페이지 웹 취약점 점검 여부 확인
증빙자료	☑ 홈페이지 개인정보 노출방지 점검, 웹 취약점 점검 수행 결과
관련근거	「개인정보 보호법」 제29조(안전조치 의무) 「개인정보의 안전성 확보조치 기준」 제6조(접근통제) ③
벌칙과태료	3천만 원 이하의 과태료
세부설명	□ 홈페이지를 통해 개인정보가 유출되지 않도록 연 1회 이상 홈페이지를 점검하는 것을 권장함(KISA 보호나라 보안취약점 점검 서비스 이용 등) ○ 외부에 공개한 자료 내 개인정보가 포함되어 있는지 점검 ○ 개인정보가 포함되어 있는 경우 완전삭제 또는 마스킹* 처리 * 필요한 부분만을 노출하기 위해 불필요한 부분을 원하는 형태로 가리는 행위 ※ 잘못된 마스킹 처리(예시) – 문서 편집 프로그램을 통해 마스킹 처리 후 PDF로 변환하여 게재하였으나, 원본 이미지가 남아 있어 개인정보를 취득할 수 있음. 
주요 확인사항	□ 정보시스템 취약점 점검 절차를 수립하고, 정기적으로 점검을 수행하고 있는가? □ 발견된 취약점에 대해 조치를 수행하고 그 결과를 책임자에게 보고하고 있는가?

3.3.6	**일정시간 이상 업무처리를 하지 않을 시 자동으로 시스템 접속이 차단되도록 하고 있는가?**		
점검기준	☑ 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우, 자동으로 개인정보처리시스템에 접속을 차단하고 있는지 여부 확인		
증빙자료	☑ (필수제출) 일정시간 이상 개인정보처리시스템 미사용으로 인한 접근 제한 적용화면 또는 시스템 시간제한 설정 화면 캡처 등		
관련근거	「개인정보 보호법」 제29조(안전조치 의무) 「개인정보의 안전성 확보조치 기준」 제6조(접근통제) ④		
벌칙과태료	3천만 원 이하의 과태료	고유식별정보 안전조치 관리실태 점검 항목(증빙필수)	15
세부설명	□ 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 접속이 차단되도록 하는 등 필요한 조치를 하여야 함. ○ 시스템 내 세션 설정 기능이 있는지 확인 후 적절하게 사용 ○ 세션 시간의 경우 업무에 따라 설정 가능하도록 하여야 함. 다만, 세션 시간에 대한 입증 책임은 개인정보처리자가 부담 ○ 시스템 접속차단은 개인정보처리시스템 연결해제를 의미하며, 업무용 컴퓨터의 화면보호기 등은 접속차단에 해당하지 않음. ○ 개인정보처리시스템에 접속 후 일정시간 이상 업무처리를 하지 않는 경우, 자동으로 로그아웃되며 재접속 시 최초 로그인할 때와 동일한 방법으로 접속해야 함.		
주요 확인사항	□ 개인정보처리시스템 내 세션차단 기능을 확인했는가? □ 시스템 내 세션 설정 기능을 적절하게 사용 중인가? □ 세션 시간을 업무에 맞게 적절하게 설정하였는가? □ Windows 화면보호기 설정만을 하고, 터미널 서비스에 대한 세션 타임아웃으로 여기는지 확인하였는가?		

3.3.7	**업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하고 있는가?**		
점검기준	☑ 업무용 모바일 기기의 분실·도난 등으로 고유식별정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치 여부 확인 * (해당없음) 모바일 기기를 이용하지 않는 경우		
증빙자료	☑ 업무용 모바일 기기 보호조치 설정 화면 등		
관련근거	「개인정보 보호법」 29조(안전조치 의무) 「개인정보의 안전성 확보조치 기준」 제6조(접근통제) ⑤		
벌칙·과태료	3천만 원 이하의 과태료	고유식별정보 안전조치 관리실태 점검 항목	16
세부설명	□ 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치 여부 ○ 비밀번호, 패턴, PIN, 지문, 홍채 등을 사용하여 화면 잠금 설정 ○ 디바이스 암호화 기능을 사용하여 애플리케이션, 데이터 등 암호화 ○ USIM 카드에 저장된 개인정보 보호를 위한 USIM 카드 잠금 설정 ○ 모바일 기기 제조사 및 이동통신사가 제공하는 기능을 이용한 원격 잠금, 원격 데이터 삭제 ○ 중요한 개인정보를 처리하는 모바일 기기는 MDM(Mobile Device Management) 등 모바일 단말 관리 프로그램을 설치하여 원격 잠금, 원격 데이터 삭제, 접속 통제 등 * MDM은 무선망을 이용해 원격으로 스마트폰 등의 모바일 기기를 제어하는 솔루션으로서, 분실된 모바일 기기의 위치 추적, 잠금 설정, 정보 삭제, 특정 사이트 접속 제한 등의 기능 제공		
주요 확인사항	□ PC, 노트북, 가상PC, 태블릿 등 업무에 사용되는 단말기에 대하여 기기인증, 승인, 접근범위 설정, 기기 보안설정 등의 보안 통제 정책을 수립·이행하고 있는가? □ 개인정보 처리업무에 이용되는 모바일 기기에 대하여 비밀번호 설정 등 도난·분실에 대한 보호대책이 적용되어 있는가? □ 업무용 단말기를 통하여 개인정보 및 중요정보가 유출되는 것을 방지하기 위하여 자료공유 프로그램 사용 금지, 공유설정 제한, 무선망 이용 통제 등의 정책을 수립·이행하고 있는가?		

3.3.8	**개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근 권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등에 대하여, 인터넷망 차단 조치를 하고 있는가?**		
점검기준	☑ 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근 권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등에 대한 인터넷망 차단 조치 여부 * (점검대상) 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상인 개인정보처리자		
증빙자료	☑ 특정 권한을 보유한 개인정보취급자(시스템 운영자)의 컴퓨터에 대한 인터넷망 차단 조치 화면 캡처 등		
관련근거	「개인정보 보호법」 제29조(안전조치 의무) 「개인정보의 안전성 확보조치 기준」 제6조(접근통제) ⑥		
벌칙·과태료	3천만 원 이하의 과태료	고유식별정보 안전조치 관리실태 점검 항목	17
세부설명	□ 업무망과 인터넷망의 분리 대상 구분 ○ 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있는 개인정보취급자의 컴퓨터 등 ○ 개인정보처리시스템에 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등 * 개인정보처리시스템에서 단순히 개인정보를 열람, 조회 등만을 할 때에는 인터넷망 차단조치를 적용하지 아니할 수 있음 □ 인터넷망 차단조치 방안 ○ 물리적 방식: 통신망, 장비 등을 물리적으로 이원화하여 인터넷 접속이 불가능한 컴퓨터와 인터넷 접속만 가능한 컴퓨터로 분리하는 방식 ○ 논리적 방식: 물리적으로 하나의 통신망, 장비 등을 사용하지만 가상화 등의 방법으로 인터넷 접속이 불가능한 내부 업무영역과 인터넷 접속 영역으로 분배하는 방식 □ 클라우드컴퓨팅서비스를 이용하여 개인정보처리시스템을 구성·운영하는 경우 ○ 클라우드컴퓨팅법 제2조제3호에 따른 클라우드컴퓨팅서비스를 이용하여 개인정보처리시스템을 구성·운영하는 경우에는 해당 클라우드컴퓨팅서비스에 대한 접속 외에 다른 인터넷의 접속을 차단하는 조치를 하여야 함		

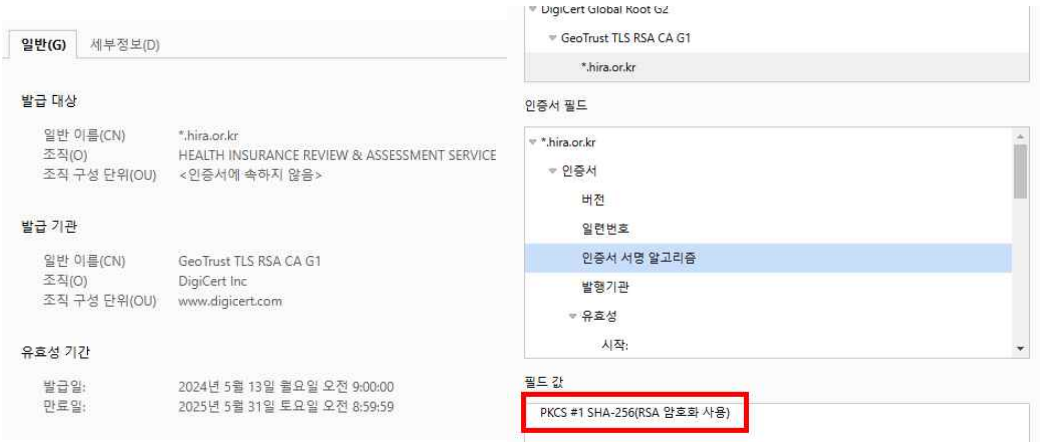
	※ 클라우드컴퓨팅서비스 유형(클라우드컴퓨팅법 시행령 제3조) ① 서버, 저장장치, 네트워크 등을 제공하는 서비스(IaaS) ② 응용프로그램 등 소프트웨어를 제공하는 서비스(SaaS) ③ 응용프로그램 등 소프트웨어의 개발·배포·운영·관리 등을 위한 환경을 제공하는 서비스(PaaS) ④ ①~③까지의 서비스를 둘 이상 복합하는 서비스
주요 확인사항	□ 업무망과 인터넷망의 분리 대상에 대한 차단조치를 하였는가?

<table>
<tr><td>3.4.1</td><td colspan="3">개인정보처리시스템에 고유식별정보, 비밀번호 및 생체인식정보를 저장하는 경우, 안전한 알고리즘으로 암호화 조치를 하고 있는가?</td></tr>
<tr><td>점검기준</td><td colspan="3">☑ 개인정보처리시스템에 고유식별정보, 비밀번호 및 생체인식정보를 저장하는 경우, 안전한 알고리즘으로 암호화 조치를 하고 있는지 여부 확인</td></tr>
<tr><td>증빙자료</td><td colspan="3">☑ 개인정보처리시스템에 암호화되어 저장된 고유식별정보, 비밀번호, 생체인식정보 캡처 화면 등(암호화 적용현황, 암호화 솔루션 관리 화면)</td></tr>
<tr><td>관련근거</td><td colspan="3">「개인정보 보호법」 제29조(안전조치 의무)
「개인정보의 안전성 확보조치 기준」 제7조(개인정보의 암호화) ①②③</td></tr>
<tr><td>벌칙과태료</td><td>3천만 원 이하의 과태료</td><td>고유식별정보 안전조치 관리실태 점검 항목</td><td>19</td></tr>
<tr><td>세부설명</td><td colspan="3">□ 고유식별정보, 비밀번호 및 생체인식정보 등 인증정보를 저장하는 경우
○ 주민등록번호, 인증정보(비밀번호, 생체인식정보 등)
– 저장 위치와 무관하게 암호화 조치
– 비밀번호의 경우 복호화 되지 아니하도록 일방향 암호화하여 저장

□ 개인정보처리시스템에 이용자의 고유식별정보를 저장하는 경우
○ 암호화 필수 조치 대상
– 주민등록번호, 여권번호, 운전면허번호, 외국인 등록번호
○ 이 외 암호화 조치 대상
– 신용카드번호, 계좌번호, 생체인식정보

□ 개인정보처리시스템에 이용자가 아닌 정보주체의 개인정보를 암호화하여 저장하는 경우
<table>
<tr><th>구 분</th><th>암호화 조치 여부</th></tr>
<tr><td>주민등록번호
인증정보(비밀번호, 생체인식정보)</td><td>▪ 무조건 암호화
▪ 단, 비밀번호는 일방향 암호화</td></tr>
<tr><td>여권번호, 운전면허번호,
외국인등록번호</td><td>▪ (인터넷망 구간 및 DMZ) 암호화하여 저장
▪ (내부망) 개인정보 보호책임자 또는 해당부서의 장의 결재를 득한 ‘위험도 분석 결과보고서’의 ‘위험도 분석 기준’ 중 어느 하나의 점검 항목이라도 ‘아니오’에 해당하는 경우 암호화</td></tr>
</table></td></tr>
</table>

<table>
<tr><td></td><td>※ 안전한 암호 알고리즘(예시)(‘개인정보의 암호화 조치 안내서’ 참고)
<table>
<tr><th>구분</th><th>알고리즘 명칭</th></tr>
<tr><td>대칭키 암호 알고리즘</td><td>▪ SEED, ARIA-128/192/256, AES-128/192/256, HIGHT, LEA 등</td></tr>
<tr><td>공개키 암호 알고리즘</td><td>▪ RSAES-OAEP 등</td></tr>
<tr><td>일방향 암호 알고리즘</td><td>▪ SHA-256/384/512 등</td></tr>
</table>
– 안전하지 않은 알고리즘: DES, 자체 개발 알고리즘</td></tr>
<tr><td>주요
확인사항</td><td>□ 개인정보 및 주요정보의 보호를 위하여 법적 요구사항을 반영한 암호화 대상, 암호강도, 암호사용 등이 포함된 암호정책을 수립하고 있는가?
□ 암호정책에 따라 개인정보 및 주요정보의 저장 시 암호화를 수행하고 있는가?
□ 개인정보취급자의 비밀번호에 대하여 일방향 암호화를 적용하였으나, 안전하지 않은 MD5 알고리즘을 사용하였는가?</td></tr>
</table>

3.4.2	**개인정보를 정보통신망을 통하여 인터넷망 구간으로 송·수신하는 경우 안전한 알고리즘에 의한 암호화 조치를 하고 있는가?**		
점검기준	☑ 고유식별정보 등 개인정보를 정보통신망을 통하여 인터넷망 구간으로 송·수신하는 경우 안전한 알고리즘에 의한 암호화 조치하는지 여부 확인		
증빙자료	☑ SSL 등이 적용된 캡처 화면 등		
관련근거	「개인정보 보호법」 제29조(안전조치 의무) 「개인정보의 안전성 확보조치 기준」 제7조(개인정보의 암호화) ④		
벌칙과태료	3천만 원 이하의 과태료	고유식별정보 안전조치 관리실태 점검 항목	18
세부설명	□ 정보통신망을 통하여 고유식별정보 등 개인정보를 인터넷망 구간으로 송·수신하는 경우 안전한 암호화 알고리즘을 사용하여 암호화 적용 ○ 웹서버에 SSL(Secure Socket Layer) 인증서를 설치하여 전송하는 정보를 암호화 송수신 ○ 웹서버에 암호화 응용프로그램을 설치하여 전송하는 정보를 암호화하여 송수신 ○ 그 밖에 암호화 기술 활용: VPN, PGP 등 ※ SSL 인증서 적용 화면  ※ HTTPS 적용 화면 		
주요 확인사항	□ 정보통신망을 통해 인터넷망으로 개인정보 송·수신 시 SSL인증서를 설치하여 암호화를 적용하고 있는가? (HTTPS 적용 여부 확인)		

3.4.3	컴퓨터, 모바일 기기, 보조저장매체 등에 고유식별정보, 비밀번호 및 생체인식정보를 저장하는 경우, 안전한 알고리즘으로 암호화 조치를 하고 있는가?		
점검기준	☑ 컴퓨터, 모바일 기기 및 보조저장매체 등에 고유식별정보, 비밀번호 및 생체인식정보를 저장하는 경우, 안전한 알고리즘으로 암호화 조치를 하고 있는지 여부 확인 ☑ 개인정보처리시스템에서 파일 다운로드 기능이 있는 경우 암호화 여부 확인		
증빙자료	☑ (필수제출) 업무용 컴퓨터 내 전자문서 암호 입력 화면 또는 암호화 솔루션 적용 화면		
관련근거	「개인정보 보호법」 29조(안전조치 의무) 「개인정보의 안전성 확보조치 기준」 제7조(개인정보의 암호화) ⑤		
벌칙·과태료	3천만 원 이하의 과태료	고유식별정보 안전조치 관리실태 점검 항목(증빙필수)	21
세부설명	□ 업무용 컴퓨터 또는 모바일 기기 및 보조저장매체 등에 고유식별정보, 비밀번호 및 생체인식정보를 저장하여 관리하는 경우 ○ 개인정보처리시스템 또는 업무용 컴퓨터 내에 고유식별정보를 포함한 데이터베이스, 파일 등 암호화하여 안전하게 보관 ○ 업무용 컴퓨터 내 파일 암호화 방법 – 한컴오피스 파일: 다른이름으로 저장하기 > 문서 암호 설정 – MS오피스 파일: 다른이름으로 저장하기 > 도구 > 일반옵션 – DRM(Digital Right Management) 기술 적용 등 ○ 보조저장매체 내 저장하는 경우 파일 암호화 또는 암호화 기능을 제공하는 보안 저장매체 이용(보안USB 등) ○ 상용 암호화 소프트웨어를 사용하여 암호화하는 경우, 안전한 암호 알고리즘이 적용되었는지 확인하여 적용 * 암호 적용 시 단순 숫자 또는 문자열 사용 금지(3.2.5 지표 참고) □ 업무용 컴퓨터 외 원격 저장소 등에 고유식별정보, 비밀번호 및 생체인식정보 등 개인정보를 저장하는 경우에도 암호화하여 안전하게 보관		
주요 확인사항	□ 개인정보 및 주요정보의 보호를 위하여 법적 요구사항을 반영한 암호화 대상, 암호강도, 암호사용 등이 포함된 암호정책을 수립하고 있는가? □ 암호정책에 따라 개인정보 및 주요정보의 저장 시 암호화를 수행하고 있는가?		

3.4.4	암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차 수립하였는가?		
점검기준	☑ 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차 수립 여부 확인 * (점검대상) 개인정보의 보유량 10만명 이상 대기업·중견기업 또는 100만명 이상 중소기업·단체		
증빙자료	☑ 내부 암호키 관리 절차서		
관련근거	「개인정보 보호법」 제29조(안전조치 의무) 「개인정보의 안전성 확보조치 기준」 제7조(개인정보의 암호화) ⑥		
벌칙과태료	3천만 원 이하의 과태료	고유식별정보 안전조치 관리실태 점검 항목	20
세부설명	□ 암호화 된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 정책 및 절차를 다음과 같은 내용을 포함하여 수립・시행 ○ 암호키 관리 담당자 ○ 암호키 생성, 보관(소산 백업 등) 방법 ○ 암호키 배포 대상자 및 배포방법(복호화 권한 부여 포함) ○ 암호키 사용 유효기간(변경 주기): 암호키 변경 시 비용, 업무 중요도 등을 고려하여 결정 ○ 암호키 복구 및 폐기 절차와 방법 ○ 소스코드에 하드코딩 방식의 암호키 기록 금지에 관한 사항 등 □ 암호키는 필요 시 복구가 가능하도록 별도의 안전한 장소에 보관하고 암호키 사용에 관한 접근권한을 최소화하여 관리 ○ 암호키 손상 시 시스템 또는 암호화된 정보의 복구를 위하여 암호키는 별도의 매체에 저장한 후 안전한 장소에 보관(암호키 관리시스템, 물리적 분리된 곳 등) ○ 암호키에 대한 접근권한 최소화 및 접근 모니터링 등		
주요 확인사항	□ 암호키 생성, 이용, 보관, 배포, 변경, 복구, 파기 등에 관한 절차를 수립·이행하고 있는가?		

<table>
<tr><td>3.5.1</td><td colspan="3">개인정보취급자가 개인정보처리시스템에 접속한 식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행한 업무내용 등이 포함된 접속기록을 2년 이상 보관·관리하고 있는가?</td></tr>
<tr><td>점검기준</td><td colspan="3">☑ 개인정보처리시스템에 접속한 기록에 5개의 필수 항목을 포함하여 2년 이상 보관 · 관리하고 있는지 여부 확인</td></tr>
<tr><td>증빙자료</td><td colspan="3">☑ (필수제출) 5개의 필수 항목을 포함한 2년 이상의 개인정보처리시스템 접속기록(로그)</td></tr>
<tr><td>관련근거</td><td colspan="3">「개인정보 보호법」 제29조(안전조치 의무)
「개인정보의 안전성 확보조치 기준」 제8조(접속기록의 보관 및 점검) ① ③</td></tr>
<tr><td>벌칙·과태료</td><td>3천만 원 이하의 과태료</td><td>고유식별정보 안전조치 관리실태 점검 항목(증빙필수)</td><td>22</td></tr>
<tr><td>세부설명</td><td colspan="3">□ 개인정보처리시스템에 대한 접속기록은 필요한 항목을 모두 포함하여 일정기간 안전하게 기록·보관
○ 개인정보처리시스템 내 접속기록(로그) 확인
○ 개인정보취급자의 접속기록을 일정기간 안전하게 보관 및 관리
<table>
<tr><th>구 분</th><th>보존 기간</th></tr>
<tr><td>5만명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리시스템에 해당하는 경우</td><td rowspan="3">최소 2년 이상</td></tr>
<tr><td>고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템에 해당하는 경우</td></tr>
<tr><td>개인정보처리자로서 「전기통신사업법」 제6조제1항에 따라 등록을 하거나 같은 항 단서에 따라 신고한 기간통신사업자에 해당하는 경우</td></tr>
<tr><td>위의 3가지 조건에 해당하지 않을 경우</td><td>최소 1년 이상</td></tr>
</table>
○ 접속기록에 반드시 포함되어야 할 5개 필수항목
<table>
<tr><th>필수 접속기록</th><th>접속기록 내용</th></tr>
<tr><td>식별자(사용자계정)</td><td>개인정보취급자 ID 등 접속한 자의 식별정보</td></tr>
<tr><td>접속일시</td><td>접속한 시간 또는 업무를 수행한 시간(연월일 및 시분초)</td></tr>
<tr><td>접속지 정보</td><td>접속자 IP주소 등</td></tr>
<tr><td>처리한 정보주체 정보</td><td>정보주체의 ID, 고객번호, 학번, 사번 등</td></tr>
<tr><td>수행업무 내용</td><td>개인정보 조회, 변경, 입력, 삭제, 출력, 다운로드 등</td></tr>
</table></td></tr>
</table>

※ 접속기록(예시)

번호	계정(ID)	접속일시	접속지정보 (IP)	접속 DB명 / File명	정보주체 정보	수행업무 내용
1	A101234	20250101.hhmmss	nnn.nn.nn.nnn	abcd001_table	환자A	입력
2	A101234	20250102.hhmmss	nnn.nn.nn.nnn	abcd002_table	환자B	삭제
3	A101234	20250103.hhmmss	nnn.nn.nn.nnn	abcd003_table	환자C	변경
4	A101234	20250104.hhmmss	nnn.nn.nn.nnn	abcd004_table	환자D	Download
5	A101234	20250105.hhmmss	nnn.nn.nn.nnn	abcd005_table	환자E	Download
6	A101234	20250106.hhmmss	nnn.nn.nn.nnn	abcd006_table	환자F	출력

□ 개인정보처리시스템에 접속한 기록이 위 · 변조 및 도난, 분실되지 않도록 안전하게 보관 · 관리

※ 접속기록의 안전한 보관방법(예시)

- 상시적으로 접속기록 백업을 수행하여 개인정보처리시스템 이외의 별도의 보조저장매체나 별도의 저장장치, 오브젝트 스토리지 등에 보관
- 접속기록에 대한 위·변조를 방지하기 위해서는 CD-ROM, DVD-R, WORM(Write Once Read Many) 등과 같은 덮어쓰기 방지 매체를 사용
- 접속기록을 수정 가능한 매체(하드디스크, 자기 테이프 등)에 백업하는 경우에는 무결성 보장을 위해 위·변조 여부를 확인할 수 있는 정보(MAC값, 전자서명값 등)를 별도의 장비에 보관·관리 등

주요 확인사항	□ 개인정보처리시스템에 대한 접속기록은 법적 요구사항을 준수할 수 있도록 필요한 항목을 모두 포함하여 일정기간 안전하게 보관하고 있는가?

3.5.2	**개인정보의 오·남용, 분실, 도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록, 다운로드가 확인된 경우 사유 확인 등을 월 1회 이상 점검하고 있는가?**		
점검기준	☑ 개인정보처리시스템에 접속한 기록 및 다운로드가 확인된 경우 사유 확인을 월 1회 이상 점검하고 있는지 여부 확인		
증빙자료	☑ (필수제출) 개인정보처리시스템의 접속기록을 월 1회 이상 점검한 내역		
관련근거	「개인정보 보호법」 제29조(안전조치 의무) 「개인정보의 안전성 확보조치 기준」 제8조(접속기록의 보관 및 점검) ②③		
벌칙·과태료	3천만 원 이하의 과태료	고유식별정보 안전조치 관리실태 점검 항목(증빙필수)	23
세부설명	□ 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위해 개인정보처리시스템의 접속기록을 월 1회 이상 점검 ○ 점검 대상, 점검 기준 및 방법, 담당자 및 책임자, 오·남용(비인가접속, 과다조회 등) 의심 발견 시 대응절차 등을 포함하여 월 1회 이상 점검하고 그 결과를 관련 책임자에게 보고 □ 다운로드가 확인된 경우 내부 관리계획 등으로 정하는 바에 따라 사유 확인 ○ 사전에 내부 관리계획 등으로 개인정보 다운로드가 확인된 경우를 대비한 사유 확인 기준 및 절차 수립 ○ 다운로드 사유 확인이 필요한 기준은 개인정보처리자가 개인정보처리시스템의 운영 환경 등을 고려하여 자율적으로 수립 ○ 다운로드한 정보주체의 수, 일정기간 내 다운로드 횟수, 업무시간 외 다운로드 수행 사유 등을 포함 ○ 개인정보의 오·남용이나 유출 목적으로 다운로드한 것이 확인되었다면 지체 없이 개인정보취급자가 다운로드한 개인정보를 회수하여 파기하는 등 필요한 조치 이행		
주요 확인사항	□ 월 1회 이상 다운로드 사유 확인 내용이 포함하여 접속기록을 점검한 내역이 있는가?		

3.6.1	**악성 프로그램을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영 및 최신의 상태로 유지하고 있는가?**		
점검기준	☑ 최신 보안 프로그램 설치 여부 확인 ☑ 자동 업데이트 혹은 일 1회 이상의 업데이트 실시 확인 ☑ 발견된 악성프로그램 등에 대한 조치 여부 확인		
증빙자료	☑ (필수제출) 백신(보안) 프로그램 설치 및 최신의 상태로 운영되고 있는지 확인할 수 있는 자료(기업용 백신프로그램의 최근 업데이트 날짜 캡처 화면 등)		
관련근거	「개인정보 보호법」 제29조(안전조치 의무) 「개인정보의 안전성 확보조치 기준」 제9조(악성프로그램 등 방지) ①②		
벌칙과태료	3천만 원 이하의 과태료	고유식별정보 안전조치 관리실태 점검 항목(증빙필수)	24
세부설명	□ 악성프로그램 등을 예방 및 치료할 수 있는 보안 프로그램을 설치·운영 ○ 업무용 컴퓨터에는 개인용 백신S/W가 아닌 기업용 백신S/W 사용 * 기업용 백신S/W가 없을 시: 심평원 제공 DUR모듈에 포함된 백신S/W(AhnLab Online Security) 사용 가능 ○ 백신S/W는 상시 활성화 □ 보안 프로그램의 자동 업데이트 기능 사용 또는 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지		
주요 확인사항	□ 바이러스, 웜, 트로이목마, 랜섬웨어 등의 악성코드로부터 정보시스템 및 업무용 단말기 등을 보호하기 위하여 보안 프로그램을 설치 하였는가? □ 백신 소프트웨어 등 보안프로그램을 일 1회 이상 업데이트를 하고 있는가? □ 보안프로그램이 항상 실시간 감시 상태로 실행되고 있는가?		

<table>
<tr><td>3.7.1</td><td>개인정보 등 중요자료가 보관된 물리적 장소에 대한 출입 통제 절차를 수립하여 운영하고 있는가?</td></tr>
<tr><td>점검기준</td><td>☑ 물리적 보관장소에 대한 출입 통제 절차 수립 여부 확인
☑ 출입관리 대장 작성·관리 여부 확인</td></tr>
<tr><td>증빙자료</td><td>☑ 출입 통제 절차서, 출입 관리대장 및 출입로그 등</td></tr>
<tr><td>관련근거</td><td>「개인정보 보호법」 제29조(안전조치의무)
「개인정보의 안전성 확보조치 기준」 제10조(물리적 안전조치) ①②③</td></tr>
<tr><td>벌칙과태료</td><td>3천만 원 이하의 과태료</td></tr>
<tr><td>세부설명</td><td>□ 요양기관 내 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 장소를 별도로 설치하고 이에 대한 출입통제 절차를 수립·운영

□ 출입 통제방법
○ 업무목적에 따라 최소한의 인원만 출입할 수 있도록 통제
○ 출입절차: 출입신청, 책임자 승인, 출입권한 부여 및 회수, 출입내역 기록, 출입기록 정기적 검토 등
○ 출입통제 장치 설치: 비밀번호 기반, ID카드 기반, 생체정보 기반 등
○ 출입통제 절차 수립·운영: 출입자 등록·삭제, 출입권한 관리, 방문자 관리, 출입대장 관리 등

※ 물리적 보호구역(예시)
<table>
<tr><th>구 분</th><th>설명</th></tr>
<tr><td>접견구역</td><td>외부인이 별다른 출입증 없이 출입이 가능한 구역
(예: 접견장소 등)</td></tr>
<tr><td>제한구역</td><td>비인가 접근을 방지하기 위하여 별도의 출입통제 장치 및 감시 시스템이 설치된 장소로 출입 시 직원카드와 같은 출입증이 필요한 장소(예: 부서별 사무실 등)</td></tr>
<tr><td>통제구역</td><td>제한구역의 통제항목을 모두 포함하고 출입자격이 최소인원으로 유지되며 출입을 위하여 추가 절차가 필요한 곳
(예: 전산실, 통신장비실, 관제실, 공조실, 발전실, 전원실 등)</td></tr>
</table></td></tr>
<tr><td>주요
확인사항</td><td>□ 보호구역별로 허가된 자만이 출입할 수 있도록 내·외부자 출입통제 절차를 마련하고, 출입 가능한 인원 현황을 관리하였는가?

□ 각 보호구역에 대한 내·외부자 출입기록을 일정기간 보존하고, 출입기록 및 출입권한을 주기적으로 검토하였는가?</td></tr>
</table>

3.7.2	**개인정보가 포함된 종이 인쇄물, 개인정보가 복사된 외부 저장매체 등 개인정보의 출력·복사물을 안전하게 관리하기 위해 필요한 안전조치를 하였는가?**		
점검기준	☑ 개인정보가 포함된 종이 인쇄물, 개인정보가 복사된 외부 저장매체 등 개인정보의 출력·복사물을 안전하게 관리하기 위해 필요한 안전조치 여부 확인		
증빙자료	☑ 사무실 및 공용공간 보안점검 보고서, 출력·복사물 보호조치 현황 등		
관련근거	「개인정보 보호법」 제29조(안전조치 의무) 「개인정보의 안전성 확보조치 기준」 제12조(출력·복사 시 안전조치) ①②		
벌칙·과태료	3천만 원 이하의 과태료	고유식별정보 안전조치 관리실태 점검 항목	26
세부설명	□ 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관 ○ 안전한 장소에 보관하지 않고 책상 등 공개된 장소에 방치 금지 □ 개인정보처리자는 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련 □ 개인정보의 출력(인쇄, 화면표시, 파일생성 등) 시 용도 특정 및 출력 항목의 최소화 ○ 개인정보처리시스템 내 개인정보 출력 여부 확인 ○ 업무 수행 형태 및 목적, 유형, 장소 등 여건 및 환경에 따라 개인정보처리시스템에 대한 접근 권한 범위 내에서 최소한의 개인정보를 출력하는지 확인 ※ 출력 시 업무에 필수적인 최소한의 정보만 출력되도록 주의 필요 – 오피스(엑셀 등)에서 개인정보가 숨겨진 필드 형태로 저장되지 않도록 조치 – 웹페이지 소스 보기 등을 통하여 불필요한 개인정보가 출력되지 않도록 조치 등 ※ 용도에 따라 개인정보의 출력 항목을 최소화 하는 방법 예시 – 개인정보의 출력(인쇄, 화면표시, 파일생성 등) 시 접근 권한에 따라 출력 항목을 다르게 설정 – 개인정보 출력 시 업무상 불필요한 개인정보 항목에 대해 표시제한 조치(마스킹 등)를 적용		

	□ 개인정보가 포함된 종이 인쇄물, 개인정보가 복사된 외부 저장매체 등 개인정보의 출력·복사물을 안전하게 관리하기 위해 필요한 보호조치 ※ 출력·복사물 보호조치 예시 – 출력·복사물 보호 및 관리 정책, 규정, 지침 등 마련 – 출력·복사물 생산·관리 대장 마련 및 기록 – 출력·복사물 운영·관리 부서 지정·운영 – 출력·복사물 외부 반출 및 재생산 통제·신고·제한 등 ※ (보안기술 활용 예시) 응용프로그램, DRM 솔루션 등을 통해 출력 시 워터마크, 이력관리 등
주요 확인사항	□ 문서고, 공용 PC, 복합기, 파일서버 등 공용으로 사용하는 시설 및 사무용 기기에 대한 보호대책을 수립·이행하고 있는가? □ 업무용 PC, 책상, 서랍 등 개인업무 환경을 통한 개인정보 및 중요정보의 유·노출을 방지하기 위한 보호대책을 수립·이행하고 있는가? □ 개인정보가 포함된 종이 인쇄물 등 개인정보의 출력·복사물을 안전하게 관리하기 위해 필요한 보호조치를 하고 있는가?

3.8.1	**재해·재난 발생 시, 개인정보의 손실·훼손 등을 방지하기 위하여 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응 절차를 마련하고 있는가?**		
점검기준	☑ 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응 절차를 마련하고 있는지 확인 * **(대상) 개인정보의 보유량 10만 명이상 대기업·중견기업 또는 100만 명이상 중소기업·단체**		
증빙자료	☑ 개인정보처리시스템 위기대응 매뉴얼 ☑ 개인정보처리시스템 백업 및 복구 계획서		
관련근거	「개인정보 보호법」 제29조(안전조치 의무) 「개인정보의 안전성 확보조치 기준」 제11조(재해·재난 대비 안전조치)		
벌칙과태료	3천만 원 이하의 과태료	고유식별정보 안전조치 관리실태 점검 항목	25
세부설명	□ 10만명 이상의 개인정보를 처리하는 대기업 · 중견기업 · 공공기관 또는 100만명 이상의 개인정보를 처리하는 중소기업 · 단체 등은 화재 · 홍수 · 단전 등의 재해 · 재난 발생 시 개인정보처리시스템 보호를 위한 다음 각 호의 조치를 하여야 함 ① 위기대응 매뉴얼 등 대응절차 마련 및 정기점검 ② 개인정보처리시스템 백업 및 복구 계획 마련 ※ 개인정보처리시스템 위기대응 매뉴얼 및 백업·복구 계획(예시) – 개인정보처리시스템 구성 요소(개인정보 보유량, 종류·중요도, 시스템 연계 장비·설비 등) – 재해·재난 등에 따른 파급효과(개인정보 유출, 손실, 훼손 등) 및 초기대응 방안 – 개인정보처리시스템 백업 및 복구 우선순위, 복구 목표시점, 복구 목표시간 – 개인정보처리시스템 백업 및 복구 방안(복구센터 마련, 백업계약 체결, 비상가동 등) – 업무분장, 책임 및 역할 – 실제 발생 가능한 사고에 대한 정기적 점검, 사후처리 및 지속관리 등		
주요 확인사항	□ 조직의 핵심 서비스(업무) 연속성을 위협할 수 있는 IT 재해 유형을 식별하고, 유형별 피해규모 및 업무에 미치는 영향을 분석하여 핵심 IT 서비스(업무) 및 시스템을 식별하고 있는가? □ 핵심 IT 서비스 및 시스템의 중요도 및 특성에 따른 복구 목표시간, 복구 목표시점을 정의하고 있는가?		

서식 모음

목 차

개인정보 수집· 이용 동의서 87

개인정보 파기 관리대장 89

민감정보 수집 · 이용 동의서 90

고정형 영상정보처리기기 운영·관리 방침 91

고정형 영상정보 처리기기(CCTV) 설치 안내 93

개인영상정보 관리대장 94

표준 개인정보처리위탁 계약서 95

수탁업체 개인정보 보호 실태점검표 98

보안 서약서 99

비밀유지 서약서 100

개인정보 보호 교육 서명록 101

개인정보 내부관리계획 102

사용자 ID 관리대장 120

출입통제 절차 수립 예시 121

출입관리대장 122

개인정보 처리방침 123

개인정보 접속기록 점검표 136

개인정보 유출시 필수 조치요령 137

개인정보 유출 등 신고서 138

서식(증빙자료) 리스트

연번	서 식 명	지표번호
1	개인정보 수집·이용 동의서	1.1.1 1.1.2 1.2.1 1.2.2 1.2.3 1.3.1
2	개인정보 파기 관리대장	1.4.1
3	민감정보 수집·이용 동의서	2.1.1
4	고정형 영상정보 처리기기 운영·관리 방침	2.3.1
5	고정형 영상정보 처리기기(CCTV) 설치 안내	2.3.2
6	개인영상정보 관리대장	2.3.3
7	표준 개인정보처리위탁 계약서	2.4.1
8	수탁업체 개인정보 보호 실태점검표	2.4.3
9	보안 서약서 / 비밀유지 서약서	2.5.1
10	개인정보 보호 교육 서명록	2.5.2
11	개인정보 내부관리 계획	3.1.1
12	사용자 ID 관리대장	3.2.1 3.2.2
13	출입통제 절차 수립 예시 / 출입관리대장	3.7.1
14	개인정보 처리방침	2.6.1
15	개인정보 접속기록 점검표	3.5.2
16	개인정보 유출시 필수 조치요령 / 개인정보 유출 등 신고서	2.7.2

개인정보 수집·이용 동의서 예시(요양기관)

1.1.1	1.1.2	1.2.1
1.2.2	1.2.3	1.3.1

○○○서비스 제공을 위한 개인정보 수집·이용, 제공 동의서(예시)

[요양기관명]은 ○○○서비스 제공을 위하여 아래와 같이 개인정보를 수집·이용하고 제3자에게 제공하고자 합니다.

내용을 자세히 읽으신 후 동의 여부를 결정하여 주십시오.

□ 선택적 개인정보 수집·이용 내역 (선택사항, 동의거부 가능)

항 목	수집목적	보유기간
□ 성명 □ 전화번호	예방접종 안내, 최신의학정보	1년

※ 위의 개인정보 수집·이용에 대한 동의를 거부할 권리가 있습니다.
그러나 동의를 거부할 경우 맞춤형 건강정보(서비스명 구체화) 제공이 제한됩니다.

☞ 위와 같이 개인정보를 수집·이용하는데 동의하십니까? (예, 아니오)

□ 개인정보 제3자 제공 내역 (선택사항, 동의거부 가능)

제공받는 기관	제공목적	제공하는 항목	보유기간
oo연구소	맞춤형 의학정보 수집	성별, 연령, 관심분야	1년

※ 위의 개인정보 제공에 대한 동의를 거부할 권리가 있습니다.
그러나 동의를 거부할 경우 맞춤형 의학정보 이용에 제한을 받을 수 있습니다.

☞ 위와 같이 개인정보를 제3자 제공하는데 동의하십니까? (예, 아니오)

<기타 고지 사항>

개인정보 보호법 제15조 제1항 제2호에(의료법) 따라 진료목적인 경우 환자(정보주체)의 동의 없이 개인정보를 수집·이용합니다.

개인정보 수집·이용 목적	개인정보 항목	수집 근거
진료기록부 작성	주소·성명·연락처·주민등록번호 등 인적사항, 주된 증상, 진단결과, 진료경과, 치료내용, 진료일시	「의료법」 제22조, 동법 시행규칙 제14조

년 월 일

본인 성명 (서명 또는 인)

법정대리인 성명 (서명 또는 인)

[요양기관명]장 귀중

개인정보 수집·이용 동의서 예시(약국)

1.1.1 1.1.2 1.2.1 1.2.2 1.2.3 1.3.1

○○○서비스 제공을 위한 개인정보 수집·이용, 제공 동의서(예시)

[○○약국]은 ○○○서비스 제공을 위하여 아래와 같이 개인정보를 수집·이용하고 제3자에게 제공하고자 합니다.

내용을 자세히 읽으신 후 동의 여부를 결정하여 주십시오.

□ 선택적 개인정보 수집·이용 내역 (선택사항, 동의거부 가능)

항 목	수집목적	보유기간
□ 성명 □ 전화번호	예방접종 안내, 최신의학정보	1년

※ 위의 개인정보 수집·이용에 대한 동의를 거부할 권리가 있습니다.
그러나 동의를 거부할 경우 맞춤형 건강정보(서비스명 구체화) 제공이 제한됩니다.

☞ 위와 같이 개인정보를 수집·이용하는데 동의하십니까? (예, 아니오)

□ 개인정보 제3자 제공 내역 (선택사항, 동의거부 가능)

제공받는 기관	제공목적	제공하는 항목	보유기간
00연구소	맞춤형 의학정보 수집	성별, 연령, 관심분야	1년

※ 위의 개인정보 제공에 대한 동의를 거부할 권리가 있습니다.
그러나 동의를 거부할 경우 맞춤형 의학정보 이용에 제한을 받을 수 있습니다.

☞ 위와 같이 개인정보를 제3자 제공하는데 동의하십니까? (예, 아니오)

<기타 고지 사항>

개인정보 보호법 제15조 제1항 제2호에(약사법) 따라 조제, 복약지도 등 진료목적인 경우 환자(정보주체)의 동의 없이 개인정보를 수집·이용 할 수 있습니다.

개인정보 수집·이용 목적	개인정보 항목	수집 근거
조제기록부 작성	인적사항, 조제년월일, 처방약품명과 일수, 조제내용, 복약지도 내용	「약사법」 제24조 「약사법」 제30조

년 월 일

본인 성명 (서명 또는 인)

법정대리인 성명 (서명 또는 인)

[약국명]장 귀중

1.4.1
1.4.2

개인정보 파기 관리대장(예시)

번호	개인정보 파일명	자료의 종류	생성일	폐기일	폐기사유	처리담당자	처리부서장
1	환자 종이 청구 정보	종이처방전	2010.9.8	2015.9.8	보존기간 경과	○○○	○○○
2	환자 조제 내역 정보	전산데이터	2010.3.12	2015.3.12	보존기간 경과	○○○	○○○

○○○을 위한 민감정보 수집·이용 동의서(별도) (예시)

[요양기관명] 은(는) 개인정보보호법 등 관련 법령상의 개인정보 보호 규정을 준수하며 회원의 개인정보 보호에 최선을 다하고 있습니다. *[요양기관명]* 은(는)「개인정보 보호법」제23조제1호에 근거하여, 다음과 같이 민감정보를 수집·이용하는데 동의를 받고자 합니다.

항 목	수집목적	보유기간
민감정보 항목 기재	*수집목적 기재*	*보유기간 기재*

※ 위와 같이 개인정보를 처리하는데 동의를 거부할 권리가 있습니다.
그러나 동의를 거부할 경우 관련 서비스 제공이 제한 될 수 있습니다.

위와 같이 민감정보를 처리하는데 동의하십니까? (예, 아니오)

년 월 일

본인 성명 (서명 또는 인)

※ 정보주체가 만14세 미만의 아동인 경우

위와 같이 민감정보를 처리하는데 동의하십니까? (예, 아니오)

년 월 일

본 인 성명 (서명 또는 인)
법정대리인 성명 (서명 또는 인)

[요양기관명]장 귀중

고정형 영상정보처리기기 운영·관리 방침(예시)

본 *[요양기관명]* (이하 본 사라 함)는 고정형 영상정보처리기기 운영·관리 방침을 통해 본 사에서 처리하는 개인영상정보가 어떠한 용도와 방식으로 이용·관리되고 있는지 알려드립니다.

1. 영상정보처리기기의 설치 근거 및 설치 목적

본 사는 개인정보 보호법 제25조 제1항에 따라 다음과 같은 목적으로 영상정보처리기기를 설치・운영 합니다.

- 시설안전 및 화재 예방

- 고객의 안전을 위한 범죄 예방

(주차장에 설치하는 경우)

- 차량도난 및 파손방지

※ 주차대수 30대를 초과하는 규모의 경우 「주차장법 시행규칙」 제6조제1항을 근거로 설치・운영 가능

2. 설치 대수, 설치 위치 및 촬영범위

설치 대수	설치 위치 및 촬영 범위
00대	*건물로비, 주차장 입구*

3. 관리책임자 및 접근권한자

귀하의 개인영상정보를 보호하고 개인영상정보와 관련한 불만을 처리하기 위하여 아래와 같이 개인영상정보 관리책임자 및 접근권한자를 두고 있습니다.

구분	성명	직위	소속	연락처
관리책임자	*홍길동*	*과장*	*0000과*	*00-0000-0000*
접근권한자				

4. 영상정보의 촬영시간, 보관기간, 보관장소 및 처리방법

촬영시간	보관기간	보관장소
24시간	*촬영일로부터 30일*	*000실 (보관시설 명)*

- 처리방법: 개인영상정보의 목적 외 이용, 제3자 제공, 파기, 열람 등 요구에 관한 사항을 기록・관리하고, 보관기간 만료 시 복원이 불가능한 방법으로 영구 삭제(출력물의 경우 파쇄 또는 소각)합니다.

5. 개인영상정보의 확인 방법 및 장소에 관한 사항

- 확인 방법: 영상정보 관리책임자에게 미리 연락하고 본 사를 방문하시면 확인 가능합니다.

- 확인 장소: OO부서 OO팀

6. 정보주체의 영상정보 열람 등 요구에 대한 조치

귀하는 개인영상정보에 관하여 열람 또는 존재확인·삭제를 원하는 경우 언제든지 고정형영상정보처리기기운영자에게 요구하실 수 있습니다. 단, 귀하가 촬영된 개인영상정보에 한정됩니다. 본 사는 개인영상정보에 관하여 열람 또는 존재확인·삭제를 요구한 경우 지체 없이 필요한 조치를 하겠습니다.

7. 영상정보의 안전성 확보조치

본 사에서 처리하는 개인영상정보는 암호화 조치 등을 통하여 안전하게 관리되고 있습니다. 또한 본 사는 개인영상정보보호를 위한 관리적 대책으로서 개인정보에 대한 접근 권한을 차등 부여하고 있고, 개인영상정보의 위·변조 방지를 위하여 개인영상정보의 생성 일시, 열람 시 열람 목적·열람자·열람 일시 등을 기록하여 관리하고 있습니다. 이 외에도 개인영상정보의 안전한 물리적 보관을 위하여 잠금장치를 설치하고 있습니다.

8. 영상정보처리기기 설치 및 관리 등의 위탁에 관한 사항 *(해당하는 경우만)*

본 사는 아래와 같이 영상정보처리기기 설치 및 관리 등을 위탁하고 있으며, 관계 법령에 따라 위탁계약 시 개인정보가 안전하게 관리될 수 있도록 필요한 사항을 규정하고 있습니다.

수탁업체	담당자	연락처
OO시스템	*홍길동*	*00-000-0000*

9. 영상정보처리기기 운영·관리방침 변경에 관한 사항

이 고정형 영상정보처리기기 운영・관리방침은 2024년 O월 OO일에 제정되었으며 법령・정책 또는 보안기술의 변경에 따라 내용의 추가・삭제 및 수정이 있을 시에는 시행하기 최소 7일전에 본 사 홈페이지를 통해 변경사유 및 내용 등을 공지하도록 하겠습니다.

- 공고일자: 2000년 O월 OO일 / 시행일자: 2000년 O월 OO일

고정형 영상정보처리기기(CCTV) 설치 안내

[요양기관명] 은 시설의 안전 및 관리, 화재 예방을 위해 고정형 영상정보처리기기를 운영하고 있습니다.

◈ 설치 목적: *범죄예방 및 시설안전*

◈ 설치 장소: *출입구의 벽면/천장,*
엘리베이터/각층의 천장

◈ 촬영 범위: *출입구, 엘리베이터 및 각층 복도(360°회전)*

◈ 촬영 시간: *24시간 연속 촬영*

◈ 관리책임자: *OO과 홍길동 (00-000-0000)*

(설치·운영을 위탁한 경우)

◈ 위탁관리자: *OO업체 박길동 (00-000-0000)*

※ 안내판에 CCTV 그림을 표시하여 정보주체가 쉽게 인식할 수 있도록 하는 것이 바람직함

2.3.3

개인영상정보 관리대장

번호	구분	일시	파일명/형태	담당자	목적/사유	이용·제공받는 제3자 /열람 등 요구자	이용·제공 근거	이용·제공 형태	이용 제공 기간 및 파기 예정일자	파기 여부 등 결과 및 처리일자	안전관리 요청내용 및 결과
1	□ 이용 □ 제공 □ 열람 □ 파기										
2	□ 이용 □ 제공 □ 열람 □ 파기										
3	□ 이용 □ 제공 □ 열람 □ 파기										
4	□ 이용 □ 제공 □ 열람 □ 파기										
5	□ 이용 □ 제공 □ 열람 □ 파기										
6	□ 이용 □ 제공 □ 열람 □ 파기										
7	□ 이용 □ 제공 □ 열람 □ 파기										
8	□ 이용 □ 제공 □ 열람 □ 파기										
9	□ 이용 □ 제공 □ 열람 □ 파기										
10	□ 이용 □ 제공 □ 열람 □ 파기										

※ 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 고시,「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시) 및「표준 개인정보 보호지침」(개인정보보호위원회 고시)에서 정의된 바에 따른다.

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

1. 개인정보의 암호화 *2. 프로그램의 유지보수*

제4조 (위탁업무 기간) 이 계약서에 의한 개인정보 처리업무의 기간은 다음과 같다.

계약 기간 : 년 월 일 ~ 년 월 일

제5조 (재위탁 제한) ① "수탁자"는 "위탁자"의 사전 승낙을 얻은 경우를 제외하고 "위탁자"와의 계약상의 권리와 의무의 전부 또는 일부를 제3자에게 양도하거나 재위탁할 수 없다.

② "수탁자"가 다른 제3의 회사와 수탁계약을 할 경우에는 "수탁자"는 해당 사실을 계약 체결 7일 이전에 "위탁자"에게 통보하고 협의하여야 한다.

---

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

제6조 (개인정보의 안전성 확보조치) "수탁자"는「개인정보 보호법」제23조제2항 및 제24조제3항 및 제29조, 같은 법 시행령 제21조 및 제30조, 「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시)에 따라 개인정보의 안전성 확보 조치를 하여야 한다.

제7조 (개인정보의 처리제한) ① "수탁자"는 계약기간은 물론 계약 종료 후에도 위탁업무 수행 목적 범위를 넘어 개인정보를 이용하거나 이를 제3자에게 제공 또는 누설하여서는 안 된다.

② "수탁자"는 계약이 해지되거나 또는 계약기간이 만료된 경우 위탁업무와 관련하여 보유하고 있는 개인정보를 「개인정보 보호법」시행령 제16조 및「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시)에 따라 즉시 파기하거나 "위탁자"에게 반납하여야 한다.

③ 제2항에 따라 "수탁자"가 개인정보를 파기한 경우 지체없이 "위탁자"에게 그 결과를 통보하여야 한다.

제8조 (수탁자에 대한 관리·감독 등) ① "위탁자"는 "수탁자"에 대하여 다음 각 호의 사항을 감독할 수 있으며, "수탁자"는 특별한 사유가 없는 한 이에 응하여야 한다.

1. 개인정보의 처리 현황
2. 개인정보의 접근 또는 접속현황
3. 개인정보 접근 또는 접속 대상자
4. 해당업무 범위를 초과한 이용 및 제3자 제공 금지 준수여부
5. 위탁업무 수행 목적 외 처리 금지 및 재 위탁 제한 준수여부
6. 암호화 등 안전성 확보조치 이행여부
7. 그 밖에 개인정보의 보호를 위하여 필요한 사항

② "위탁자"는 "수탁자"에 대하여 제1항 각 호의 사항에 대한 실태를 점검하여 시정을 요구할 수 있으며, "수탁자"는 특별한 사유가 없는 한 이행하여야 한다.

③ "위탁자"는 처리위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 1년에 ( )회 "수탁자"를 교육할 수 있으며, "수탁자"는 이에 응하여야 한다.[2)]

④ 제1항에 따른 교육의 시기와 방법 등에 대해서는 "위탁자"는 "수탁자"와 협의하여 시행한다.

제9조 (정보주체 권리보장) ① "수탁자"는 정보주체의 개인정보 열람, 정정·삭제, 처리정지 요청 등에 대응하기 위한 연락처 등 민원 창구를 마련해야 한다.

제10조 (개인정보의 파기) ① "수탁자"는 제4조의 위탁업무기간이 종료되면 특별한 사유가 없는 한 지체 없이 개인정보를 파기하고 이를 "위탁자"에게 확인받아야 한다.

---

2)「개인정보 안전성 확보조치 기준 고시」(개인정보보호위원회 고시 제2021-2호) 및「개인정보 보호법」제26조에 따라 개인정보처리자 및 취급자는 개인정보보호에 관한 교육을 의무적으로 시행하여야 한다.

제11조 (손해배상) ① “수탁자” 또는 “수탁자”의 임직원 기타 “수탁자”의 수탁자가 이 계약에 의하여 위탁 또는 재위탁 받은 업무를 수행함에 있어 이 계약에 따른 의무를 위반하거나 “수탁자” 또는 “수탁자”의 임직원 기타 “수탁자”의 수탁자의 귀책사유로 인하여 이 계약이 해지되어 “위탁자” 또는 개인정보주체 기타 제3자에게 손해가 발생한 경우 “수탁자”는 그 손해를 배상하여야 한다.

② 제1항과 관련하여 개인정보주체 기타 제3자에게 발생한 손해에 대하여 “위탁자”가 전부 또는 일부를 배상한 때에는 “위탁자”는 이를 “수탁자”에게 구상할 수 있다.

본 계약의 내용을 증명하기 위하여 계약서 2부를 작성하고, “위탁자”와 “수탁자”가 서명 또는 날인한 후 각 1부씩 보관한다.

20 . . .

위탁자	수탁자
주 소 :	주 소 :
기관(회사)명 :	기관(회사)명 :
대표자 성명 : (인)	대표자 성명 : (인)

2.4.3

수탁업체 개인정보 보호 실태 점검표

○ 업 체 명: *○○정보기술*
○ 점검일자: *20XX년 XX월 XX일*

연번	점검항목	점검결과		해당 없음	비고
		예	아니오		
1	*개인정보 목적 외 이용제공 여부*				
2	*재위탁 여부*				
3	*안전성 확보조치 여부*				

※ 위탁 업무내용에 따라 점검항목 조정 가능함

보안 서약서(예시)

□ 성　명:
□ 소　속:
□ 직　책:

본인은 *OOO* 업무 중에 알게 된 환자의 개인정보에 대하여 업무 수행 중이나 업무 수행 후에도 비밀을 지킬 것을 서약합니다.

또한 환자의 개인정보의 보호를 위해 *OOO*에서 정하는 개인정보 처리방침 또는 내부관리계획을 준수할 것이며, 적법한 절차 없이 환자의 개인정보를 무단으로 조회하거나 유출하지 않을 것을 서약합니다.

본인은 개인정보 보호책임자로부터 개인정보 처리 및 보호의 법적 근거가 되는「개인정보 보호법」관련 규정을 충분히 설명을 듣고 숙지하였습니다.

만약, 이러한 서약에도 불구하고 업무상 알게 된 사항에 대하여 비밀을 누설하거나 정당한 사유 없이 조회, 유출, 오용할 경우 민·형사상 처벌은 물론 징계처분을 받을 수 있음을 통고 받았으며, 이러한 제재에 대하여 이의를 제기하지 않을 것을 본인의 자의로 서약합니다.

년　　월　　일

성 명:　　(인)

2.5.1

비밀유지 서약서(예시)

소 속 :
직 명 :
성 명 :

위 본인은 재직 중 직무상 지득한 모든 비밀을 퇴직 후에도 절대로 누설하지 않을 것이며 공무상 비밀을 누설하였을 경우에는 형사상의 처벌 등 어떠한 경우에도 이의를 제기하지 않겠음

20 년 월 일

성 명 (인)

○○○ 의원 원장 ○○○ 귀하

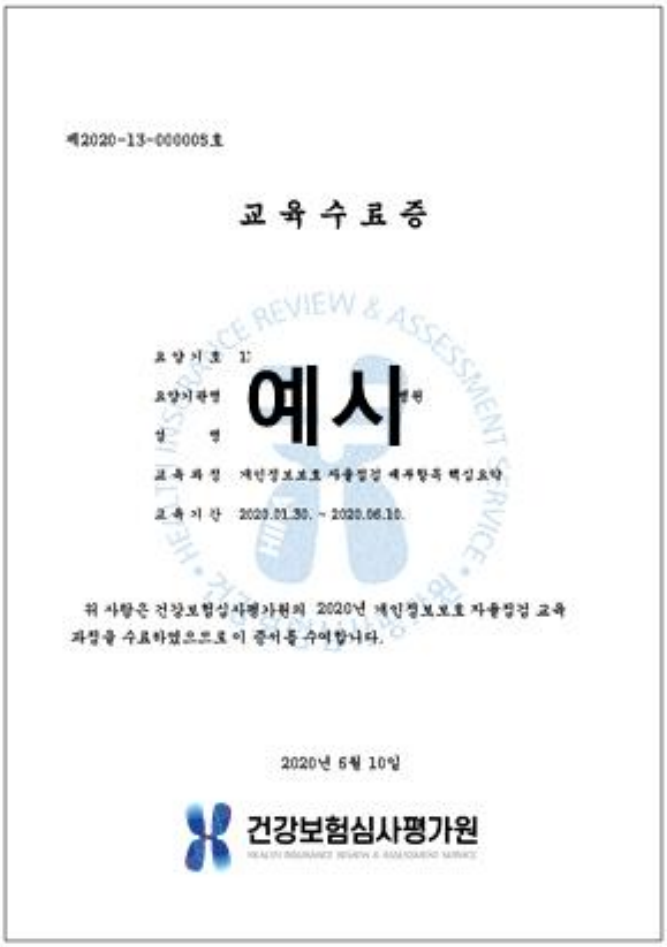
2.5.2

개인정보 보호 교육 서명록

○ 교육일자:
○ 교육장소:
○ 교육내용(예시)
- *정보보호 및 개인정보 보호의 기본 개요, 관리체계 구축 및 방법, 관련 법률*
- *정보보호 및 개인정보 보호 관련 내부규정, 관리적·기술적·물리적 조치사항*
- *중요정보 및 개인정보 침해(유출)사고 사례 및 대응방안, 규정 위반 시 법적 책임 등*

연번	부서명	직급	성명	서명
1	*○○과*	*과장*	*○○○*	*○○○*
2	*○○과*	*대리*	*○○○*	*○○○*

개인정보보호 교육 수료증 예시


제2020-13-000005호

교 육 수 료 증

요양기호 1
요양기관명
성 명
교육과정 개인정보보호 자율점검 세부항목 핵심요약
교육기간 2020.01.30. ~ 2020.06.10.

예시

위 사람은 건강보험심사평가원의 2020년 개인정보보호 자율점검 교육 과정을 수료하였으므로 이 증서를 수여합니다.

2020년 6월 10일

건강보험심사평가원

3.1.1

결재	CEO	실장	부서장

○○○○○ (개인정보처리자명)
개인정보 내부 관리계획

0000. 00. 00.

[제·개정 이력]

순 번	구 분	시행 일자	제정 · 개정 주요내용
○	제정	○○○○. ○○. ○○.	1. ○○○○○ 2. ○○○○○ 3. ○○○○○
○	일부개정	○○○○. ○○. ○○.	1. ○○○○○ 2. ○○○○○ 3. ○○○○○
○	전부개정	○○○○. ○○. ○○.	1. ○○○○○ 2. ○○○○○ 3. ○○○○○

목 차

제1장 총 칙 ····· 00
제1조(목적)
제2조(적용 범위)
제3조(용어 정의)

제2장 내부 관리계획의 수립 및 시행 ····· 00
제4조(내부 관리계획의 수립, 변경 및 승인)
제5조(내부 관리계획의 공표)

제3장 개인정보 보호책임자의 역할 및 책임 ····· 00
제6조(개인정보 보호책임자의 지정)
제7조(개인정보 보호책임자의 역할 및 책임)
제8조(개인정보취급자의 역할 및 책임)

제4장 개인정보 보호 교육 ····· 00
제9조(개인정보취급자의 교육)

제5장 기술적 • 관리적 • 물리적 안전조치 ····· 00
제10조(접근 권한의 관리)
제11조(접근 통제)
제12조(개인정보의 암호화)
제13조(접속기록의 보관 및 점검 등)
제14조(악성프로그램 등 방지)
제15조(물리적 안전조치)
제16조(개인정보의 파기)
제17조(출력 복사 시 안전조치)

제6장 개인정보 침해대응 및 피해구제 ····· 00
제18조(개인정보 유출사고 대응)
제19조(권익침해 구제방법)

제7장 개인정보의 위 • 수탁 관리계획 ····· 00
제20조(개인정보의 위 • 수탁 관리)

제8장 고정형 영상정보 보호계획 ····· 00
제21조(고정형 영상정보 관리책임자의 지정, 역할 및 책임)
제22조(고정형영상정보처리기기 안전조치)
제23조(고정형 개인영상정보취급자의 책임과 역할)
제24조(고정형영상정보처리기기 설치 • 운영 사무의 위탁)

제9장 이동형 영상정보 보호계획 ····· 00
제25조(이동형 개인영상정보 보호책임자의 지정, 역할 및 책임)
제26조(이동형영상정보처리기기 안전조치)
제27조(이동형 개인영상정보취급자의 책임과 역할)
제28조(고정형영상정보처리기기 설치 • 운영 사무의 위탁)

개인정보 내부관리 계획

제1장 총칙

제1조(목적)

개인정보보호 내부관리계획은 개인정보보호법 제29조(안전조치의무) 내부관리계획의 수립 및 시행 의무에 따라 제정된 것으로 *[요양기관명]*에 근무하는 직원들이 취급하는 개인정보를 체계적으로 관리하여 개인정보가 분실, 도난, 누출, 변조, 훼손, 오·남용 등이 되지 아니하도록 함을 목적으로 한다.

제2조(적용범위)

본 계획은 홈페이지 등의 온라인을 통하여 수집, 이용, 제공 또는 관리되는 개인정보뿐만 아니라 오프라인(*인적사항, 챠트, 진료사진, 전화, 팩스 등*)을 통해 수집, 이용, 제공 또는 관리되는 개인정보에 대해서도 적용되며, 이러한 개인정보를 취급하는 내부 직원 및 외부업체 직원에 대해 적용된다.

제3조(용어 정의)

1. "내부관리계획"이란 요양기관이 보유한 개인정보가 분실·도난·유출·위조· 변조 또는 훼손되지 않도록 내부 의사결정절차를 통하여 수립·시행 및 점검을 해야 하는 개인정보보호에 관한 내부기준을 말한다.
2. "개인정보"란 살아 있는 개인에 관한 정보로서 다음 어느 하나에 해당하는 정보를 말한다.
   가. 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보.
   나. 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보. 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다.
   다. 가목 또는 나목을 가명처리 함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보.(이하"가명 정보"라 한다)
3. "민감정보"란 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 유전자검사 등의 결과로 얻어진 유전정보, 범죄경력자료, 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보, 인종이나 민족에 관한 정보에 해당하는 정보를 말한다.
4. "고유식별정보"란 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 주민등록

번호, 여권번호, 운전면허번호, 외국인등록번호를 말한다.

5. “진료정보”란 진료를 목적으로 수집하여 처리하는 개인정보가 포함된 정보로 진료기록부, 수술기록부, 조산기록부, 간호기록부, 환자명부 등으로 관리되는 정보를 말하고, 사망한 자의 진료정보도 포함한다.
6. “처방전 정보”란 약국에서 조제를 위해 접수하는 처방전에 기록된 개인정보가 포함된 정보로 성명, 주민등록번호, 질병분류기호, 처방의약품 등 법령에서 정하는 항목이 포함된다.
7. “조제정보”란 처방전에 따라 의약품 조제(「약사법」에 따라 처방전 없이 조제 하는 경우 포함) 및 복약지도를 목적으로 수집하여 처리하는 개인정보가 포함된 정보로써 조제기록부(전자문서로 작성된 것을 포함)로 관리되는 정보를 말한다.
8. “조제기록부”란 약사가 약국에서 환자에게 의약품을 조제할 때 필요한 기록을 남기는 문서를 말하며, 개인정보가 포함된 정보로써 그 내용으로 환자의 인적사항, 조제연월일, 처방약품명과 처방일수, 조제내용 및 복약지도 내용 등을 포함한다.
9. “복약지도(服藥指導)”란 다음 각 목의 어느 하나에 해당하는 것을 말한다.
   가. 의약품의 명칭, 용법・용량, 효능・효과, 저장 방법, 부작용, 상호 작용이나 성상(性狀) 등의 정보를 제공하는 것
   나. 일반의약품을 판매할 때 진단적 판단을 하지 아니하고 구매자가 필요한 의약품을 선택할 수 있도록 도와주는 것
10. “요양급여청구 정보”란 요양기관에서 건강보험심사평가원에 보험급여를 청구하기 위해 제출하는 개인정보가 포함된 정보이며 성명, 건강보험증번호, 주민등록번호 등 법령에서 정하는 항목이 포함된다.
11. “정보주체”란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
12. “이용자”란 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제2조제1항 제4호에 따른 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자를 말한다.
13. “처리”란 개인정보의 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.
14. “개인정보처리자”란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
15. “개인정보 보호책임자”란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지는 자로서,「개인정보 보호법 시행령」제32조(개인정보 보호책임자의 업무 및 지정요건 등)제3항에 해당하는 자를 말한다.
16. “개인정보취급자”란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 직접 개인정보에 관한 업무를 담당하는 자와 그 밖에 업무상 필요에 의해 개인정보에 접근하여 처리하는 모든 자를 말한다.
17. “개인정보처리시스템”이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다.

18. “위험도 분석”이란 개인정보 유출에 영향을 미칠 수 있는 다양한 위험요소를 식별·평가하고 해당 위험요소를 적절하게 통제할 수 있는 방안 마련을 위한 종합적으로 분석하는 행위를 말한다.
19. "비밀번호"라 함은 이용자 및 개인정보취급자 등이 시스템 또는 정보통신망에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.
20. "접속기록"이라 함은 이용자 또는 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 식별자, 접속일시, 접속지를 알 수 있는 정보, 수행업무 등 접속한 사실을 전자적으로 기록한 것을 말한다.
21. "생체정보"라 함은 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 인증·식별하거나 개인에 관한 특징을 알아보기 위해 일정한 기술적 수단을 통해 처리되는 정보를 말한다.
22. "생체인식정보"라 함은 생체정보 중 특정 개인을 인증 또는 식별할 목적으로 일정한 기술적 수단을 통해 처리되는 정보를 말한다.
23. "P2P(Peer to Peer)"라 함은 정보통신망을 통해 서버의 도움 없이 개인과 개인이 직접 연결되어 파일을 공유하는 것을 말한다.
24. "공유설정"이라 함은 컴퓨터 소유자의 파일을 타인이 조회·변경·복사 등을 할 수 있도록 설정하는 것을 말한다.
25. "다운로드"라 함은 개인정보처리시스템에 접속하여 개인정보취급자의 컴퓨터 등에 개인정보를 엑셀, 워드, 텍스트, 이미지 등의 파일 형태로 저장하는 것을 말한다.
26. "보안서버"라 함은 정보통신망에서 송·수신하는 정보를 암호화하여 전송하는 웹서버를 말한다.
27. "인증정보"라 함은 개인정보처리시스템 또는 정보통신망을 관리하는 시스템 등이 요구한 식별자의 신원을 검증하는데 사용되는 정보를 말한다.
28. "모바일 기기"란 스마트폰, 태블릿PC 등 무선망을 이용할 수 있는 휴대용 기기를 말한다.
29. “내부망”이란 인터넷망 차단, 접근 통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.
30. "보조저장매체"란 이동형 하드디스크(HDD), USB메모리, CD(Compact Disk) 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 쉽게 분리·접속할 수 있는 저장매체를 말한다.
31. “개인영상정보” 라 함은 법 제2조제1호에 따른 개인정보 중 고정형 또는 이동형 영상정보처리 기기에 의하여 촬영·처리되는 영상 형태의 개인정보 중 개인의 초상, 행동 등과 관련된 영상으로서 해당 개인을 식별할 수 있는 정보를 말한다(표준 개인정보 보호지침 제2조제9호).
32. “고정형영상정보처리기기”란 일정한 공간에 설치되어 지속적 또는 주기적으로 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 일

체의 장치로서「개인정보 보호법 시행령」제3조에 따른 폐쇄회로 텔레비전(CCTV) 및 네트워크 카메라를 의미한다.

33. “이동형영상정보처리기기”란 사람이 신체에 착용 또는 휴대하거나 이동 가능한 물체에 부착 또는 거치(据置)하여 사람 또는 사물의 영상 등을 촬영하거나 이를 유・무선망을 통하여 전송하는 장치로서 대통령령이 정하는

가. 착용형 장치: 안경 또는 시계 등 사람의 신체 또는 의복에 착용하여 영상 등을 촬영하거나 촬영한 영상정보를 수집・저장 또는 전송하는 장치

나. 휴대형 장치: 이동통신단말장치 또는 디지털 카메라 등 사람이 휴대하면서 영상 등을 촬영하거나 촬영한 영상정보를 수집・저장 또는 전송하는 장치

다. 부착・거치형 장치: 차량이나 드론 등 이동 가능한 물체에 부착 또는 거치(据置)하여 영상 등을 촬영하거나 촬영한 영상정보를 수집・저장 또는 전송하는 장치를 말한다.

34. “고정형영상정보처리기기운영자” 라 함은 개인정보보호법 제25조제1항 각 호에 따라 고정형 영상정보처리 기기를 설치·운영하는 자를 말한다.

35. “이동형영상정보처리기기운영자” 라 함은 개인정보보호법 제25조의2제1항 각 호에 따라 업무를 목적으로 공개된 장소에서 사람 또는 그 사람과 관련된 사물의 영상(개인정보에 해당하는 영상을 말함, 이하 ‘개인영상정보’라 함)을 촬영하기 위하여 이동형 영상정보처리기기를 운영하는 자를 의미한다.

36. “고정형영상정보 관리책임자” 라 함은 고정형영상정보처리기기의 개인영상정보 처리에 관한 업무를 총괄하여 책임을 지는 자를 말한다.

37. “이동형영상정보 보호책임자” 라 함은 이동형영상정보처리기기의 개인영상정보 처리에 관한 업무를 총괄하여 책임을 지는 자를 말한다.

38. “개인영상정보취급자” 라 함은 업무 목적 달성을 위해 필요한 범위에서 개인영상정보를 처리하는 임직원, 파견근로자, 시간제근로자 등을 말한다.

39. “대기업”이란 「독점규제 및 공정거래에 관한 법률」제14조에 따라 공정거래위원회가 지정한 기업집단을 말한다.

40. “중견기업”이란「중견기업 성장촉진 및 경쟁력 강화에 관한 특별법」제2조에 해당하는 기업을 말한다.

41. “중소기업”이란 「중소기업기본법」제2조 및 동법 시행령 제3조에 해당하는 기업을 말한다.

42. “소상공인”이란 「소상공인 보호 및 지원에 관한 법률」제2조에 해당하는 자를 말한다.

제2장(내부관리계획의 수립 및 시행)

제4조(내부관리계획의 수립, 변경 및 승인)

1. 개인정보 보호책임자는 임직원이 개인정보보호와 관련한 법령 및 규정 등을 준수할 수 있도록 내부 의사결정 절차를 통하여 내부관리계획을 수립하여야 한다.
2. 개인정보 보호책임자는 내부관리계획의 각 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부 관리계획을 수정하여야 한다.
3. 개인정보 보호책임자는 내부관리계획을 수립하거나 수정하는 경우에는 *[최고경영층 000]*으로부터 내부결재 등의 승인을 받아야 하며, 그 이력을 보관·관리하여야 한다.
4. 내부 관리계획의 세부 이행을 위한 각종 지침 등을 마련하여 시행할 수 있다.
5. 개인정보 보호책임자는 연 1회 이상으로 내부 관리계획의 이행 실태를 점검·관리하고 그 결과에 따라 적절한 조치를 취하여야 한다.

제5조(내부관리계획의 공표)

1. 개인정보 보호책임자는 개인정보 보호책임자는 4조에 따라 승인한 내부관리계획을 모든 임직원 및 관련자에게 알림으로써 이를 준수하도록 하여야 한다.
2. 내부관리계획은 임직원 등이 언제든지 열람할 수 있는 방법으로 비치하거나 제공하여야 하며, 변경사항이 있는 경우에는 이를 공지하여야 한다.

제3장 개인정보 보호책임자의 역할 및 책임

제6조(개인정보 보호책임자의 지정)

1. 다음 각 목의 어느 하나에 해당하는 자를 개인정보 보호책임자로 임명한다.(개인정보보호법 시행령 제32조제2항)
   가. *[요양기관명]*의 사업주 또는 대표자 *[000]*
   나. 임원(임원이 없는 경우 개인정보 처리 관련 업무를 담당하는 부서의 장 *[000]*

제7조(개인정보 보호책임자의 역할 및 책임)

1. 개인정보 보호책임자는 정보주체의 개인정보 보호를 위하여 다음 각 목의 업무를 수행한다.
   가. 개인정보 보호 계획의 수립 및 시행
   나. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
   다. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
   라. 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
   마. 개인정보 보호 교육 계획의 수립 및 시행
   바. 개인정보파일의 보호 및 관리 감독

사. 법 제30조에 따른 개인정보 처리방침의 수립·변경 및 시행
아. 개인정보 보호 관련된 인적・물적 자원 및 정보의 관리
자. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기

2. 개인정보 보호책임자는 업무를 수행함에 있어서 필요한 경우 개인정보의 처리 현황, 처리 체계 등에 대하여 수시로 조사하거나 관계 당사자로부터 보고를 받을 수 있다.
3. 개인정보 보호책임자는 개인정보 보호와 관련하여 이 법 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 하며, 필요하면 *[요양기관명]*의 최고경영층에게 개선조치를 보고하여야 한다.

제8조(개인정보취급자의 역할 및 책임)

1. 개인정보취급자는 *개인정보처리자명([요양기관명] 임직원 OOO)*의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을 말한다.
2. 개인정보취급자는 개인정보를 처리함에 있어서 개인정보가 안전하게 관리될 수 있도록 동 계획은 물론, 개인정보 보호와 관련한 법령 및 규정 등을 준수하여야 한다.

제4장 개인정보 보호 교육

제9조(개인정보취급자의 교육)

1. 개인정보 보호책임자는 다음 각 호의 사항을 포함하는 연간 개인정보보호 교육계획을 수립하고 실시하여야 한다.
   가. 교육목적 및 대상: *[전 직원을 대상으로 개인정보보호 교육]*
   나. 교육내용: *[개인정보보호 동영상교육 이수 등]*
   다. 교육 일정 및 방법: *[정기 또는 수시 온라인, 오프라인(연수과정 등) 교육 이수]*
2. 개인정보 보호책임자는 정보주체정보보호에 대한 직원들의 인식제고를 위해 노력해야 하며, 개인정보의 오·남용 또는 유출 등을 적극 예방하기 위해 임·직원을 대상으로 매년 정기적으로 *연1회 이상*의 개인정보보호 교육을 실시한다.
3. 개인정보보호 교육 방법은 집체 교육뿐만 아니라, 인터넷 교육, 그룹웨어 교육 등 다양한 방법을 활용하여 실시하고, 필요한 경우 외부 전문기관이나 전문요원에 위탁하여 교육을 실시한다.
4. 개인정보 보호에 대한 중요한 전파 사례가 있거나 개인정보 보호 업무와 관련하여 변경된 사항이 있는 경우, 개인정보 보호책임자는 *직원 회의* 등을 통해 수시 교육을 실시할 수 있다.
5. 개인정보 보호책임자는 제4장에 따라 개인정보 보호 교육을 실시한 결과 또는 이를 입증할 수 있는 관련 자료 등을 기록·보관하여야 한다.

제5장 기술적 · 관리적 · 물리적 안전조치

제10조(접근권한의 관리)

1. 개인정보처리시스템(청구 S/W 등)에 대한 접근권한을 업무수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.
2. 개인정보취급자의 휴직 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여야 하며, 또한 비밀유지의무 등에 대한 보안서약서를 받아야 한다.
3. 개인정보취급자의 1, 2에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.
4. 개인정보처리시스템에 접속할 수 있는 사용자 계정을 발급하는 경우, 정당한 사유가 없는 한 개인정보취급자 별로 계정을 발급하여야 하며, 다수의 개인정보취급자가 동일한 업무를 수행한다 하더라도 하나의 계정을 공유하지 않도록 하여야 한다.
5. 개인정보처리시스템(청구S/W 등), 접근통제시스템, 인터넷 홈페이지 등에 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 다음의 사항을 적용하여야 한다.
   가. 문자, 숫자의 조합·구성에 따라 최소 8자리 또는 10자리 이상의 길이로 구성
      - 최소 8자리 이상: 두 종류 이상의 문자를 이용하여 구성한 경우
        ※ 문자 종류: 알파벳 대문자와 소문자, 특수문자, 숫자
      - 최소 10자리 이상: 하나의 문자종류로 구성한 경우(숫자로만 구성할 경우 취약)
   나. 비밀번호는 추측하거나 유추하기 어렵도록 설정
      - 동일한 문자 반복(aaabbb, 123123 등), 키보드 상에서 나란히 있는 문자열(qwer 등), 일련번호(12345678 등), 가족이름, 생일, 전화번호 등은 사용하지 않음
   다. 비밀번호가 제3자에게 노출되었을 경우 지체 없이 새로운 비밀번호로 변경해야 함
6. 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 조치를 하여야 한다.

제11조(접근통제)

1. 정보통신망을 통한 인가되지 않은 내·외부자의 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 조치를 하여야한다.
   가. 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol)주소 등으로 제한하여 인가받지 않은 접근을 제한 *[백신 및 윈도우 방화벽을 이용한 접근통제 설정]*
   나. 개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등을 재분석하여 불법적

인 개인정보 유출 시도를 탐지 *[접속기록 2년 이상 보관 및 분석]*

2. 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다.
3. 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일 기기 등에 조치를 취하여야 한다. *[P2P 프로그램 사용 금지 및 무선LAN(Wifi) 비밀번호 설정]*
4. 고유식별정보를 처리하는 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하고 필요한 보완 조치를 하여야 한다.
5. 개인정보처리시스템의 불법적인 접근 및 침해사고를 방지하기 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않을 때에는 자동으로 시스템 접속이 차단되게 하는 등 접속 제한에 필요한 조치를 취하여야 한다.
6. 업무용 모바일 기기의 분실도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.

제12조(개인정보의 암호화)

1. 다음에 해당하는 이용자의 개인정보에 대해서는 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.
   가. 주민등록번호
   나. 여권번호
   다. 운전면허번호
   라. 외국인등록번호
   마. 신용카드번호
   바. 계좌번호
   사. 생체인식정보
2. 비밀번호, 생체인식정보 등 인증정보를 저장 또는 정보통신망을 통하여 송·수신하는 경우에 이를 안전한 암호 알고리즘으로 암호화하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화 되지 아니하도록 일방향 암호화하여 저장하여야 한다.
3. 이용자가 아닌 정보주체의 개인정보를 다음과 같이 저장하는 경우에는 암호화하여야 한다.
   가. 인터넷망 구간 및 인터넷망 구간과 내부망의 중간 지점(DMZ: Demilitarized Zone)에 고유식별정보를 저장하는 경우
   나. 내부망에 고유식별정보를 저장하는 경우
   (다만, 주민등록번호 외의 고유식별정보를 저장하는 경우에는 다음의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다)

1) 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공의료기관 등의 경우에는 해당 개인정보 영향평가의 결과
2) 암호화 미적용시 위험도 분석에 따른 결과

4. 개인정보를 정보통신망을 통하여 인터넷망 구간으로 송·수신하는 경우에는 이를 안전한 암호 알고리즘으로 암호화하여야 한다.
5. 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.
6. 이용자의 개인정보 또는 이용자가 아닌 정보주체의 고유식별정보, 생체인식정보를 개인정보취급자의 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장 할 때에는 안전한 암호 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

제13조(접속기록 보관 및 점검 등)

1. 개인정보취급자가 개인정보처리시스템에 접속한 기록을 최소 2년 이상 보관하여야 한다.
2. 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다.
3. 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다. *[외장하드 등에 데이터 백업]*
4. 개인정보를 다운로드한 것이 발견되었을 경우에는 그 사유를 반드시 확인하여야 하며, 개인정보취급자가 개인정보의 오남용이나 유출을 목적으로 다운로드한 것의 확인 등, 이상 징후가 있는 경우에는 지체없이 다운로드한 개인정보를 회수하여 파기하는 등 필요한 조치를 하여야 한다.(월 1회 이상 접속기록 점검 시 다운로드 사유 확인 내용(다운로드한 정보주체의 수, 일정기간 내 다운로드 횟수, 업무시간 외 다운로드 수행 사유 등)을 포함하여 점검 할 수 있다.)

제14조(악성프로그램 등 방지)

1. 개인정보처리시스템 또는 업무용 컴퓨터에 악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 한다.
2. 보안 프로그램의 자동 업데이트 기능을 사용하거나, 정당한 사유가 없는 한 일 1회 이상 업데이트를 실시하는 등 최신의 상태로 유지하여야 한다.
3. 악성 프로그램관련 경보가 발령된 경우 또는 사용 중인 응용프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 정당한 사유가 없는 한 즉시 이에 따른 업데이트를 적용하여야 한다.
4. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치를 하여야 한다.

제15조(물리적 안전조치)

1. *원장실[CCTV보관 PC, 메인 PC], 차트실,* 전산실, 자료보관실, 영상정보처리기기

등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차*[외부인 출입 시, 출입통제 관리대장을 작성한 후 출입]*를 수립·운영하여야 한다.

2. 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.
3. 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하여야 한다. 다만, 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있다.

제16조(개인정보의 파기)

1. 개인정보를 파기할 경우 다음 각 호 중 어느 하나의 조치를 하여야 한다.
   가. 완전파괴(소각·파쇄 등)
   나. 전용 소자장비를 이용하여 삭제
   다. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행
2. 개인정보의 일부만을 파기하는 경우, 제1항의 방법으로 파기하는 것이 어려울 때에는 다음 각 호의 조치를 하여야 한다.
   가. 전자적 파일 형태인 경우: 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독
   나. 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우: 해당 부분을 마스킹, 천공 등으로 삭제

제17조(출력·복사 시 안전조치)

1. 개인정보처리시스템에서 개인정보의 출력 시(인쇄, 화면표시, 파일생성 등) 용도를 특정하여야 하며, 용도에 따라 출력 항목을 최소화하여야 한다.
2. 개인정보가 포함된 종이 인쇄물, 개인정보가 복사된 외부 저장매체 등 개인정보의 출력·복사물을 안전하게 관리하기 위해 필요한 안전조치를 하여야 한다.

제6장 개인정보 침해대응 및 피해구제

제18조(개인정보 유출 등 사고 대응)

1. 의료인 또는 의료기관 개설자는 전자의무기록에 대한 전자적 침해행위로 진료정보가 유출되거나 의료기관의 업무가 교란·마비되는 등 대통령령으로 정하는 사고(이하 "진료정보 침해사고"라 한다)가 발생한 때에는 보건복지부장관에게 즉시 그 사실을 통지하여야 함(「의료법」 제23조의3)
2. 개인정보가 해킹, 분실, 도난 등으로 내·외부자에 의하여 유출된 경우 다음과 같이 대응한다.

단계	주요 내용
사고인지 및 긴급조치	• 개인정보 유출 등 사고 인지 및 신고 접수 - 유출 등사고 발생이 의심되는 경우, 지체 없이 개인정보 보호담당자에게 신고 • 개인정보 보호담당자는 사고 내용 등에 대해 개인정보 보호책임자에게 보고 • 개인정보 유출 등 신고 등 사고 신속 대응팀 구성 • 피해 최소화를 위한 긴급 조치 수행 - 유출 등 된 개인정보 비공개 또는 삭제 조치 - 유출 등 접속 경로 차단, 취약점 점검 및 보완 등 긴급조치, 재발방지 조치 등
↓	
정보주체 유출 등 통지	▪ 1건 이라도 개인정보 유출 등 시, 정보주체에게 개인정보 유출 등 사실 통지 (72시간 이내) - 유출 등 된 개인정보의 항목, 유출 등 된 시점과 그 경위, 피해 구제 절차 등
↓	
개인정보 유출 등 신고	▪ 1천명 이상의 정보주체에 관한 개인정보 유출 등 시 ▪ 민감정보 또는 고유식별정보 유출 시 ▪ 개인정보처리시스템 또는 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대한 외부로부터의 불법적인 접근에 의해 개인정보가 유출 등이 된 경우 ▪ 개인정보보호위원회 또는 한국인터넷진흥원(privacy.go.kr)에 유출신고 (72시간 이내)
↓	
사고분석	▪ 사고 원인 분석, 유출 등 규모 확인, 사고 원인에 대한 조치
↓	
민원대응	▪ 민원대응을 위한 별도의 온/오프라인 창구 개설 및 운영 - 피해자 구제방안, 수사 진행상황 등에 대한 답변 방향 결정 및 응대 - 2차 피해 방지를 위한 조치방법 안내 및 피해구제 절차 안내
↓	
유출 등 사고 결과보고	▪ 개인정보 유출 등 사고 결과보고서 작성 및 보고
↓	
개선 및 이행점검	▪ 개인정보 유출 등 사고 사례 전파 교육 및 개선(재발방지)

제19조(권익침해 구제방법)

1. 개인정보주체는 개인정보침해로 인한 구제를 받기 위하여 개인정보분쟁조정위원회, 한국인터넷진흥원 개인정보침해신고센터 등에 분쟁해결이나 상담 등을 신청한다. 이 밖에 기타 개인정보침해의 신고 및 상담에 대하여는 아래의 기관에 문의한다.

가. 개인정보 침해신고센터: (국번없이) 118 privacy.kisa.or.kr

나. 대검찰청 사이버범죄수사단: (국번없이) 1301 privacy@spo.go.kr(www.spo.go.kr)

다. 경찰청 사이버테러대응센터: (국번없이) 182 cyberbureau.police.go.kr

라. 개인분쟁조정위원회: 1833-6972 www.kopico.go.kr

제7장 개인정보의 위 • 수탁 관리계획

제20조(개인정보의 위 • 수탁 관리)

1. 개인정보처리 업무를 위탁하는 경우 아래 사항이 포함된 문서로 하여야 한다.
   가. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
   나. 개인정보의 기술적 · 관리적 보호조치에 관한 사항
   다. 위탁하는 업무의 목적 및 범위
   라. 재위탁 제한에 관한 사항
   마. 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
   바. 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항
   사. 수탁자가 준수해야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항
2. 개인정보처리 업무를 위탁하는 경우 위탁업무의 내용과 수탁자를 이용자 등이 언제든지 쉽게 확인할 수 있도록 인터넷 홈페이지를 통해 공개하여야 하며, 홈페이지에 공개할 수 없는 경우에는 사업장 등의 보기 쉬운 장소에 게시하는 방법으로 공개하여야 한다. 위탁업무의 공개는 개인정보처리방침 공개 시 그 내용에 포함하여 공개할 수 있다.
3. 개인정보처리 업무를 위탁하는 경우 수탁업체를 관리·감독하여야 한다.
   - 수탁자(위탁받는 업체)의 개인정보 처리현황 및 실태, 목적 외 이용·제공 여부, 재위탁 여부, 안전성 확보조치 여부 등을 정기적으로 관리·감독하고 그 결과를 '수탁업체 개인정보 보호 실태 점검표'를 이용하여 기록·보관 하여야 한다.
4. 개인정보처리 업무를 위탁하는 경우 수탁업체를 대상으로 직접 관리·감독이 어려운 경우 수탁업체 자체적으로 개인정보의 안전성 확보조치 등에 대한 점검 등을 실시하여 그 결과를 '수탁업체 개인정보 보호 실태 점검표'를 제출 받아 보관하는 것으로 대체할 수 있다.
5. 개인영상정보의 설치·운영 사무의 위탁과 관련하여서는 「개인정보 보호법」 제26조에 따른 법적 준수사항을 이행하여야 한다.

제8장 고정형 영상정보 보호계획

제21조(고정형 개인영상정보 관리책임자의 지정, 역할 및 책임)

1. 고정형영상정보처리기기를 운영할 경우 개인영상정보 관리책임자를 지정을 하여야 하며, 개인정보 보호책임자가 개인영상정보 관리책임자의 업무를 겸해서 수행 할 수 있다.

2. 개인영상정보 관리책임자는 정보주체의 개인영상정보 보호를 위하여 다음 각 목의 업무를 수행한다.
   가. 개인영상정보 보호 계획의 수립 및 시행
   나. 개인영상정보 처리 실태 및 관행의 정기적인 조사 및 개선
   다. 개인영상정보 처리와 관련한 불만의 처리 및 피해구제
   라 개인영상정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
   마. 개인영상정보 보호 교육 계획 수립 및 시행
   바. 개인영상정보 파일의 보호 및 파기에 대한 관리·감독
   사. 그 밖에 개인영상정보의 보호를 위하여 필요한 업무
3. 개인영상정보 관리책임자는 업무를 수행함에 있어서 필요한 경우 개인영상정보의 처리 현황, 처리 체계 등에 대하여 수시로 조사하거나 관계 당사자로부터 보고를 받을 수 있다.
4. 개인영상정보 관리책임자는 개인영상정보 보호와 관련하여 이 법 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 하며, 필요하면 최고경영층에게 개선조치를 보고하여야 한다.
5. 개인영상정보 관리책임자는 개인영상정보 보호계획의 각 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 개인영상정보 보호계획을 수정하여야 한다.
6. 개인영상정보 관리책임자는 개인영상정보 보호계획의 세부 이행을 위한 각종 지침 등을 마련하여 시행할 수 있다.
7. 개인영상정보 관리책임자는 연 1회 이상으로 개인영상정보 보호계획 이행 실태를 점검·관리 하고 그 결과에 따라 적절한 조치를 취하여야 한다.

제22조(고정형영상정보처리기기 안전조치)

1. 개인영상정보를 암호 화조치 등을 통하여 안전하게 관리하여야 한다.
2. 개인영상정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 필요한 조치를 취하여야 한다(법 제29조, 시행령 제30조제1항, 표준지침 제47조).
3. 개인영상정보보호를 위한 대책으로서 개인영상정보에 대한 접근 통제 및 접근 권한을 제한하는 조치를 하여야 한다.
4. 개인영상정보의 위ㆍ변조 방지를 위하여 개인영상정보를 안전하게 저장·전송할 수 있는 기술의 적용(네트워크 카메라의 경우 안전한 전송을 위한 암호화 조치, 개인영상정보파일에 대한 비밀번호 설정 등)하여야 한다.
5. 개인영상정보의 위ㆍ변조 방지를 위하여 개인영상정보의 생성 일시, 열람 시 열람 목적ㆍ열람자ㆍ열람 일시 등을 기록하여 관리하여야 한다.
6. 개인영상정보의 안전한 물리적 보관을 위하여 잠금장치를 설치하여 운영 하여야 한다.

제23조(고정형 개인영상정보취급자의 책임과 역할)

1. 고정형영상정보처리기기의 개인영상정보취급자는 개인영상정보를 처리함에 있어서 개인

영상정보가 안전하게 관리될 수 있도록 동 계획은 물론, 개인정보 보호와 관련한 법령 및 규정 등을 준수하여야 한다.

제24조(고정형영상정보처리기기 설치 • 운영 사무의 위탁)

1. 고정형영상정보처리기기의 설치·운영에 관한 사무를 위탁할 수 있으며, 고정형영상정보처리기기의 설치·운영에 관한 사무를 제3자에게 위탁하는 경우에는 다음의 내용이 포함된 문서로 하여야 한다.
   가. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
   나. 개인정보의 기술적·관리적 보호조치에 관한 사항
   다. 위탁하는 사무의 목적 및 범위
   라. 재위탁 제한에 관한 사항
   마. 개인영상정보에 대한 접근 제한 등 안전성 확보조치에 관한 사항
   바. 위탁업무와 관련하여 보유하고 있는 영상정보의 관리 현황 점검 등 감독에 관한 사항
   사. 수탁자가 준수해야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항
2. 개인영상정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 수탁자가 개인영상정보를 안전하게 처리하는지를 감독하여야 하며, 수탁자는 위탁받은 업무 범위를 초과하여 개인영상정보를 이용하거나 제3자에게 제공을 하여서는 아니 된다(법 제26조제4항·제5항).
3. 개인영상정보의 설치·운영 사무를 위탁 시에는 위탁업무의 내용과 수탁자를 이용자 등이 언제든지 쉽게 확인할 수 있도록 인터넷 홈페이지를 통해 공개하여야 하며, 홈페이지에 공개할 수 없는 경우에는 사업장 등의 보기 쉬운 장소에 게시하는 방법으로 공개하여야 한다. 위탁업무의 공개는 개인정보처리방침 공개 시 그 내용에 포함하여 공개 할 수 있다.
4. 개인영상정보의 설치·운영 사무의 위탁과 관련하여서는 「개인정보 보호법」 제26조에 따른 법적 준수사항을 이행하여야 한다.

제9장 이동형 영상정보 보호계획

제25조(이동형 개인영상정보 보호책임자의 지정, 역할 및 책임)

1. 이동형영상정보처리기기를 운영할 경우 개인영상정보 보호책임자를 지정을 하여야 하며, 개인정보 보호책임자가 개인영상정보 관리책임자의 업무를 겸해서 수행 할 수 있다.
2. 개인영상정보 보호책임자는 정보주체의 개인영상정보 보호를 위하여 다음 각 목의 업무를 수행한다.
   가. 개인영상정보 보호 계획의 수립 및 시행

나. 개인영상정보 처리 실태 및 관행의 정기적인 조사 및 개선
다. 개인영상정보 처리와 관련한 불만의 처리 및 피해구제
라. 개인영상정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
마. 개인영상정보 보호 교육 계획 수립 및 시행
바. 개인영상정보 파일의 보호 및 파기에 대한 관리·감독
사. 그 밖에 개인영상정보의 보호를 위하여 필요한 업무

3. 개인영상정보 보호책임자는 업무를 수행함에 있어서 필요한 경우 개인영상정보의 처리 현황, 처리 체계 등에 대하여 수시로 조사하거나 관계 당사자로부터 보고를 받을 수 있다.
4. 개인영상정보 보호책임자는 개인영상정보 보호와 관련하여 이 법 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 하며, 필요하면 최고경영층에게 개선조치를 보고하여야 한다.
5. 개인영상정보 보호책임자는 개인영상정보 보호계획의 각 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 개인영상정보 보호계획을 수정하여야 한다.
6. 개인영상정보 보호책임자는 개인영상정보 보호계획의 세부 이행을 위한 각종 지침 등을 마련하여 시행할 수 있다.
7. 개인영상정보 보호책임자는 연 1회 이상으로 개인영상정보 보호계획 이행 실태를 점검·관리 하고 그 결과에 따라 적절한 조치를 취하여야 한다.

제26조(이동형영상정보처리기기 안전조치)

이동형영상정보처리기기 안전조치에 관한 사항은 제24조(고정형영상정보처리기기 설치·운영 사무의 위탁)을 준용한다.

제27조(이동형 개인영상정보취급자의 책임과 역할)

이동형영상정보취급자의 책임과 역할에 관한 사항은 제23조(개인영상정보취급자의 책임과 역할)을 준용 한다.

제28조(이동형영상정보처리기기 설치 • 운영 사무의 위탁)

이동형영상정보처리기기의 설치·운영 사무의 위탁에 관한 사항은 제24조(고정형영상정보처리기기 설치·운영 사무의 위탁)을 준용 한다.

3.2.1
3.2.2

사용자 ID 관리대장

연번	처리일시	사용자 ID	소속	직급	성명	접근권한	유형	사유	처리자ID (성명)
1	20XX.XX.XX. 00:00	ABCD	○○과	과장	○○○	건강보험 청구업무	부여	입사	○○○○ (○○○)
2	20XX.XX.XX. 00:00	ABCD	○○과	과장	○○○	접수업무	변경	부서 변경	○○○○ (○○○)
3	20XX.XX.XX. 00:00	ABCD	○○과	과장	○○○	접수업무	말소	퇴사	○○○○ (○○○)

※ 개인정보처리시스템에 ID별 권한 부여·변경 기능이 없는 경우 본 서식을 사용할 수 있음
※ 위의 서식을 참고하여 요양기관의 환경에 맞게 수정하여 사용

출입통제 절차 수립 예시

3.7.1

방문자 신분확인

⬇

출입관리대장 작성
(방문자명 및 소속, 입실시간, 방문목적)

⬇

담당직원 동행 입실

⬇

출입관리대장 작성
(퇴실시간)

⬇

업무종료 후 잠금 확인

3.7.1

출 입 관 리 대 장

일자	방문자		시간		방문목적	확인자
	회사명	성명	입실	퇴실		
20XX.XX.XX.	건강보험심사평가원	홍길동	10:00	18:00	A/S	

【 개인정보 처리방침 】

OO의료기관(**이하 "*A*"이라 함**)은 귀하의 개인정보보호를 매우 중요시하며, 『개인정보 보호법』을 준수하고 있습니다. ***A***는 개인정보 처리방침을 통하여 귀하께서 제공하시는 개인정보가 어떠한 용도와 방식으로 이용되고 있으며 개인정보 보호를 위해 어떠한 조치가 취해지고 있는지 알려드리기 위하여 다음과 같이 개인정보 처리방침을 수립·공개합니다.

[주요 개인정보 처리 표시(라벨링)]

 개인정보	*성명,* *주민등록번호,* *연락처, 주소 등*	 개인정보 처리목적	*의료법에 근거한* *진료행위 등*
 개인정보 처리위탁	*위탁기관:* ***A*** *수탁기관* *(위탁수행):* ***AAA, BBB, CCC, DDD***	 고충 처리 안내	*담당자:* ***홍길동*** *연락처:* ***<전화번호>***

개인정보 처리방침의 순서는 다음과 같습니다.

1. 개인정보의 처리목적, 수집항목, 보유 및 이용기간
2. 개인정보의 제 3자 제공
3. 개인정보의 보유 및 이용기간 및 파기절차 및 파기방법
4. 이용자 및 법정대리인의 권리와 그 행사방법
5. 개인정보 처리의 위탁
6. 개인정보 보호책임자 및 열람청구
7. 권익침해 구제방법
8. 개인정보의 안전성 확보조치
9. 추가적인 이용·제공 판단 기준
10. 개인정보 자동 수집 장치의 설치·운영 및 거부에 관한 사항
11. 행태정보의 수집·이용 및 거부 등에 관한 사항
12. 고정형 영상정보처리기기 운영·관리에 관한 사항
13. 정책 변경에 따른 공지의무

1. 개인정보의 처리목적, 수집항목, 보유 및 이용기간(해당되는 부분만 작성)

처리목적	수집항목	보유 및 이용기간
진료서비스 제공 및 환자 명부 관리	*(필수) 주소, 성명, 주민등록번호, 전화번호*	*5년 (의료법 시행규칙 제15조)*
진료기록부 관리	*(필수) 주소, 성명 연락처, 주민등록번호, 병력 및 가족력, 주된 증상, 진단 결과 또는 진단명, 진료 경과, 치료내용, 진료일시*	*10년 (의료법 시행규칙 제15조)*
진료 예약 등 서비스 제공	*(필수) 성명, 주민등록번호, 휴대폰번호*	*의료법 시행규칙 제15조에 준하여 관리*
진료비 수납 등 원무서비스	*(필수) 카드사명, 카드번호 등 결제 승인정보*	*의료법 시행규칙 제15조에 준하여 관리*
홈페이지 회원가입 (홈페이지가 있는 경우)	*(필수) 성명, 생년월일, ID, 비밀번호, 이메일 주소, 만 14세 미만 아동의 경우 법정대리인 정보(성명, 생년월일, 성별, 휴대전화번호)* *(선택) 자택전화번호*	*회원 탈퇴 시까지*

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

2. 개인정보의 제3자 제공

*A*는 정보주체의 개인정보를 명시한 범위 내에서만 처리하며, 정보주체의 동의, 법률의 특별한 규정 등『개인정보 보호법』제17조 및 제18조에 해당하는 경우에만 개인정보를 제3자에게 제공하고 그 외에는 정보주체의 개인정보를 제3자에게 제공하지 않습니다.

*A*는 의료법 제21조 제3항 각 호에 해당하는 경우 환자에 관한 기록을 열람하게 하거나 사본을 내주는 등 내용을 확인할 수 있도록 하고 있습니다.

*A*는 응급의료에 관한 법류 제11조에 따라 응급환자를 다른 의료기관으로 이송할 경우 이송받는 의료기관에 진료에 필요한 의무기록을 제공할 수 있습니다.

*A*는 생명윤리 및 안전에 관한 법률 제18조에 따라 인간대상연구를 수행하는 경우 정보주체의 서면동의와 동법에 따른 기관위원회의 심의를 거쳐참여자의 개인정보를 제3자에게 제공할 수 있습니다.

*A*는 정보주체의 동의를 얻어 다음과 같이 개인정보를 제공할 수 있습니다.(해당되는 경우 작성)

제공받는 자	제공목적	제공항목	제공 근거 / 보유 및 이용기간
건강보험 심사평가원	*급여비용 심사·지급·대상여부 확인 및 적정성 평가*	*성명, 주민등록번호, 진단명, 진료내역 등*	*국민건강보험법 제 13조, 제43조, 제56조*
국민건강 보험공단	*건강보험 자격득실*	*성명, 주민등록번호, 국적, 체류자격(외국인), 연락처 등*	*국민건강보험법 제7조, 제8조, 제9조, 제10조 등*
<제3자명>	*<제공목적>*	*<제공항목>*	*<제공받는자의 법적 근거 / 보유 및 이용기간*

3. 개인정보의 보유 및 이용기간 및 파기절차 및 파기방법

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

정보주체로부터 동의받은 개인정보 보유기간이 경과하거나 처리목적이 달성되었음에도 불구하고 다른 법령에 따라 개인정보를 계속 보존하여야 하는 경우에는, 해당 개인정보를 별도의 데이터베이스(DB)로 옮기거나 보관장소를 달리하여 보존합니다.

또한 A는 폐업 또는 휴업 신고를 할 때에는 기록·보존하고 있는 진료기록부, 조산기록부, 간호기록 등 진료에 관한 기록을 관할 보건소장에게 이관합니다.

- 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.

또한 정보주체의 위임을 받은 자 등 대리인이 보건복지부령으로 정하는 요건을 갖추어 요청한 경우에도 기록 열람 등 정보주체의 권리를 행사할 수 있습니다.

5. 개인정보 처리의 위탁(해당하는 부분만 작성)

개인정보를 정보시스템을 통해 관리하기 위해 다음의 회사에 개인정보를 위탁하고 있습니다.

위탁받는 자(수탁자)	위탁업무	보유 및 이용기간
AAA	*청구프로그램 (업무 및 기록의 전산관리)*	*위탁계약 종료시까지*
BBB	*진료기록부 등 폐기*	*위탁계약 종료시까지*
CCC	*CCTV 프로그램*	*위탁계약 종료시까지*
DDD	*CT/팍스(파노라마) 프로그램*	*위탁계약 종료시까지*
EEE	*홈페이지 유지보수*	*위탁계약 종료시까지*
FFF	*기공소(치과의원만 해당)*	*위탁계약 종료시까지*
GGG	*혈액검사*	*위탁계약 종료시까지*
HHH	*PC 유지보수*	*위탁계약 종료시까지*

6. 개인정보 보호책임자 및 열람청구

정보주체는 *A*의 서비스를 이용하시면서 발생한 모든 개인정보보호 관련 문의, 불만처리, 피해구제 등에 관한 사항을 개인정보 보호책임자에게 문의할 수 있습니다. *A*는 정보주체의 문의에 대해 지체없이 답변 및 처리해드릴 것입니다.

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

정보주체는 「개인정보 보호법」 제35조에 따른 개인정보의 열람 청구를 아래의 부서에 할 수 있습니다. *A*는 정보주체의 개인정보 열람청구가 신속하게 처리되도록 노력하겠습니다.

부서명: *A*
담당자: *홍길동*
연락처: *<전화번호>, <이메일>, <팩스번호>*

정보주체는 *A*의 서비스를 이용하시면서 발생한 모든 개인정보보호 문의, 불만처리, 피해구제 등에 관한 사항을 개인정보 보호책임자 및 담당부서로 문의할 수 있습니다. *A*는 정보주체의 문의에 대해 지체없이 답변 및 처리해드릴 것입니다.

7. 권익침해 구제방법

정보주체는 개인정보침해로 인한 구제를 받기 위하여 개인정보분쟁조정위원회, 한국인터넷진흥원 개인정보침해신고센터 등에 분쟁해결이나 상담 등을 신청할 수 있습니다. 이 밖에 기타 개인정보침해의 신고, 상담에 대하여는 아래의 기관에 문의하시기 바랍니다.

1. 개인정보분쟁조정위원회: (국번없이) 1833-6972 (www.kopico.go.kr)
2. 개인정보침해신고센터: (국번없이) 118 (privacy.kisa.or.kr)
3. 대검찰청: (국번없이) 1301 (www.spo.go.kr)
4. 경찰청: (국번없이) 182 (ecrm.cyber.go.kr)

*A*는 정보주체의 개인정보자기결정권을 보장하고 개인정보침해로 인한 상담 및 피해 구제를 위해 노력하고 있으며, 신고나 상담이 필요한 경우 아래의 담당부서로 연락해 주시기 바랍니다.
담당자: *홍길동*
연락처: *<전화번호>, <이메일>, <팩스번호>*

「개인정보 보호법」 제35조(개인정보의 열람), 제36조(개인정보의 정정·삭제), 제37조(개인정보의 처리정지 등)의 규정에 의한 요구에 대 하여 공공기관의 장이 행한 처분 또는 부작위로 인하여 권리 또는 이익의 침해를 받은 자는 행정심판법에 정하는 바에 따라 행정심판을 청구할 수 있습니다.

1. 중앙행정심판위원회: (국번없이) 110 (www.simpan.go.kr)

8. 개인정보의 안전성 확보조치

*A*는 이용자의 개인정보보호를 위한 기술적 대책으로서 여러 보안장치를 마련하고 있습니다. 이용자께서 제공하신 모든 정보는 방화벽 등 보안장비에 의해 안전하게 보호/관리되고 있습니다. 또한 *A*는 이용자의 개인정보보호를 위한 관리적 대책으로서 이용자의 개인정보에 대한 접근 및 관리에 필요한 절차를 마련하고, 이용자의 개인정보를 처리하는 인원을 최소한으로 제한하고

개인정보를 처리하는 시스템의 접근권한 관리, 접근통제시스템 설치, 보안프로그램 설치 및 갱신 등의 방법으로 안전하게 관리합니다.

9. 추가적인 이용·제공 판단 기준(해당되는 경우에만 작성)

*A*는 「개인정보 보호법」 제15조제3항 및 제17조제4항에 따라 「개인정보 보호법」 시행령 제14조의2에 따른 사항을 고려하여 정보주체의 동의 없이 개인정보를 추가적으로 이용·제공할 수 있습니다.

항목	이용·제공 목적	보유 및 이용기간
이름, 연락처, 주소	*조제약을 잘못 수령한 사실을 알리기 위한 연락*	*목적 달성 즉시 파기*

이에 따라 *A*는 정보주체의 동의 없이 추가적인 이용·제공을 하기 위해서 다음과 같은 사항을 고려하였습니다.

▶ 개인정보를 추가적으로 이용·제공하려는 목적이 당초 수집 목적과 관련성이 있는지 여부
▶ 개인정보를 수집한 정황 또는 처리 관행에 비추어 볼 때 추가적인 이용·제공에 대한 예측 가능성이 있는지 여부
▶ 개인정보의 추가적인 이용·제공이 정보주체의 이익을 부당하게 침해하는지 여부

10. 개인정보 자동 수집 장치의 설치·운영 및 거부에 관한 사항(홈페이지가 없는 경우 해당없음)

*A*는 이용자에게 개별적인 맞춤서비스를 제공하기 위해 이용 정보를 제공하고 수시로 불러오는 '쿠키(cookie)'를 사용합니다. 웹사이트를 운영하는데 이용되는 서버(http)가 이용자의 컴퓨터 브라우저에게 보내는 소량의 정보이며 이용자들의 PC 컴퓨터내의 하드디스크에 저장되기도 합니다.

가. 쿠키의 사용목적: 이용자가 방문한 각 서비스와 웹 사이트들에 대한 방문 및 이용형태, 인기 검색어, 보안접속 여부 등을 파악하여 이용자에게 최적화된 정보 제공을 위해 사용됩니다.
나. 쿠키의 설치·운영 및 거부: 웹브라우저 상단의 도구>인터넷 옵션>개인정보 메뉴의 옵션 설정을 통해 쿠키 저장을 거부 할 수 있습니다.
다. 쿠키 저장을 거부할 경우 맞춤형 서비스 이용에 어려움이 발생할 수 있습니다.

11. 행태정보의 수집·이용 및 거부 등에 관한 사항(홈페이지가 없는 경우 해당없음)

*A*는 서비스 이용과정에서 정보주체에게 최적화된 맞춤형 서비스 및 혜택, 온라인 맞춤형 광고 등을 제공하기 위하여 행태정보를 아래와 같이 행태정보를 수집·이용합니다.

수집하는 행태정보의 항목	행태정보 수집 방법	행태정보 수집 목적	보유·이용기간 및 이후 정보처리 방법
이용자의 웹사이트/앱 서비스 방문이력, 검색이력, 구매이력,	*이용자의 웹 사이트 및 앱 방문/실행 시 자동 수집*	*이용자의 관심, 성향에 기반한 개인 맞춤형 상품추천 서비스를 제공*	*수집일로부터 00일 후 파기*

*A*는 다음과 같이 온라인 맞춤형 광고 사업자가 행태정보를 수집·처리하도록 허용하고 있습니다.

- 행태정보를 수집 및 처리하려는 광고 사업자: ○○○
- 행태정보 수집 방법: 이용자가 당사 웹사이트를 방문하거나 앱을 실행할 때 자동 수집 및 전송
- 수집·처리되는 행태정보 항목: 이용자의 웹/앱 방문이력, 검색이력, 구매이력

- 보유·이용기간: 00일

A는 온라인 맞춤형 광고 등에 필요한 최소한의 행태정보만을 수집하며, 사상, 신념, 가족 및 친인척관계 학력·병력, 기타 사회활동 경력 등 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 민감한 행태정보를 수집하지 않습니다.

A는 만 14세 미만임을 알고 있는 아동이나 만14세 미만의 아동을 주 이용자로 하는 온라인 서비스로부터 맞춤형 광고 목적의 행태정보를 수집하지 않고, 만 14세 미만임을 알고 있는 아동에게는 맞춤형 광고를 제공하지 않습니다.

A는 모바일 앱에서 온라인 맞춤형 광고를 위하여 광고식별자를 수집·이용합니다. 정보주체는 모바일 단말기의 설정 변경을 통해 앱의 맞춤형 광고를 차단·허용할 수 있습니다.

▶ 스마트폰의 광고식별자 차단/허용

1. (안드로이드) ① 설정 → ② 개인정보보호 → ③ 광고 → ③광고 ID 재설정 또는 광고ID 삭제
2. (아이폰) ① 설정 → ② 개인정보보호 → ③ 추적 → ④ 앱이 추적을 요청하도록 허용 끔

※ 모바일 OS 버전에 따라 메뉴 및 방법이 다소 상이할 수 있습니다.

정보주체는 웹브라우저의 쿠키 설정 변경 등을 통해 온라인 맞춤형 광고를 일괄적으로 차단·허용할 수 있습니다. 다만, 쿠키 설정 변경은 웹사이트 자동로그인 등 일부 서비스의 이용에 영향을 미칠 수 있습니다.

12. 고정형 영상정보처리기기 운영·관리에 관한 사항

A의 고정형 영상정보처리기기 운영・관리방침을 알려드립니다.

▶ 고정형 영상정보처리기기의 설치 근거 및 설치 목적

A의 영상정보처리기기를 설치・운영 목적

- 시설안전 및 관리, 화재 예방
- 고객의 안전을 위한 범죄 예방
- 차량도난 및 파손방지(주차장에 설치하는 경우)

▶ 설치 대수, 설치 위치 및 촬영범위

설치대수	설치위치 및 촬영 범위
00대	*건물로비, 주차장 입구*
00대	*약국내 접수대*

▶ 관리책임자 및 접근권한자

구분	이름	직위	소속	연락처
관리책임자	*홍길동*		*0000과*	*00-0000-0000*
접근권한자				

▶ 개인영상정보의 촬영시간, 보관기간, 보관장소 및 처리방법

촬영시간	보관기간	보관장소
24시간	*촬영일로부터 30일*	*OOO실(보관시설 명)*

- 처리방법: 개인영상정보의 목적 외 이용, 제3자 제공, 파기, 열람 등 요구에 관한 사항을 기록・관리하고, 보관기간 만료 시 복원이 불가능한 방법으로 영구삭제(출력물의 경우 파쇄 또는 소각)합니다.

▶ 영상정보처리기기 설치 및 관리 등의 위탁에 관한 사항 (해당하는 경우만)
A의 아래와 같이 고정형 영상정보처리기기 설치 및 관리 등을 위탁하고 있습니다.

수탁업체	담당자	연락처
OO시스템	*홍길동*	*02) 000-0000*

▶ 개인영상정보의 확인 방법 및 장소에 관한 사항
- 확인 방법 : 개인영상정보 관리책임자에게 미리 연락하고 A에 방문
- 확인 장소 : OO부서 OO팀

▶ 정보주체의 개인영상정보 열람 등 요구에 대한 조치
정보주체는 본인의 개인영상정보에 관하여 열람 또는 존재확인·삭제를 원하는 경우 언제든지 A에게 요구하실 수 있습니다.
A는 개인영상정보에 관하여 열람 또는 존재확인·삭제를 요구한 경우 지체없이 필요한 조치를 하겠습니다.

▶ 개인영상정보의 안전성 확보조치
A는 처리하는 개인영상정보를 암호화 등으로 안전하게 관리하고 있습니다.

▶ A는 개인영상정보보호를 위한 관리적 대책으로서 개인영상정보에 대한 접근권한을 차등 부여와 위·변조 방지를 위한 개인영상정보의 생성 일시, 열람 시 열람 목적·열람자·열람 일시 등을 기록·관리하고 있습니다. 또한 안전한 물리적 보관을 위하여 잠금장치를 설치하고 있습니다.

13. 정책 변경에 따른 공지의무

이 개인정보 처리방침은 *20XX년 X월 XX일*에 제정되었으며 법령·정책 또는 보안기술의 변경에 따라 내용의 추가·삭제 및 수정이 있을 시에는 변경되는 개인정보 처리방침을 시행하기 최소 7일전 *홈페이지 또는 접수창구*에 변경이유 및 내용 등을 공지하도록 하겠습니다.
이전의 개인정보 처리방침은 홈페이지 확인 또는 접수창구에 문의주시면 확인하실 수 있습니다.

- 20XX. X. X. ~ 20XX. X. X. 적용
- 20XX. X. X. ~ 20XX. X. X. 적용

【 개인정보 처리방침 】

OO약국(**이하 "*A*"이라 함)**은 귀하의 개인정보보호를 매우 중요시하며, 『개인정보 보호법』을 준수하고 있습니다. ***A***는 개인정보 처리방침을 통하여 귀하께서 제공하시는 개인정보가 어떠한 용도와 방식으로 이용되고 있으며 개인정보보호를 위해 어떠한 조치가 취해지고 있는지 알려드리기 위하여 다음과 같이 개인정보 처리방침을 수립·공개합니다.

[주요 개인정보 처리 표시(라벨링)]

 개인정보	*(조제)* *성명, 주민등록 번호, 연락처 등* *(청구)* *성명, 주민등록 번호, 연락처 등*	 개인정보 처리목적	*의약품 조제, 처방전 관리 및 요양급여 청구*
 개인정보 처리위탁	*위탁기관:* ***A*** *수탁기관* *(위탁수행):* ***AAA, BBB, CCC, DDD***	 고충 처리 안내	*담당자: 홍길동* *연락처:* *<전화번호>*

개인정보 처리방침의 순서는 다음과 같습니다.

1. 개인정보의 처리목적, 수집항목, 보유 및 이용기간
2. 개인정보의 제 3자 제공
3. 개인정보의 보유 및 이용기간 및 파기절차 및 파기방법
4. 이용자 및 법정대리인의 권리와 그 행사방법
5. 개인정보 처리의 위탁
6. 개인정보 보호책임자 및 열람청구
7. 권익침해 구제방법
8. 개인정보의 안전성 확보조치
9. 추가적인 이용·제공 판단 기준
10. 고정형 영상정보처리기기 운영·관리에 관한 사항
11. 정책 변경에 따른 공지의무

1. 개인정보의 처리목적, 수집항목, 보유 및 이용기간(해당되는 부분만 작성)

처리목적	수집항목	보유 및 이용기간
의약품 조제 및 처방전 관리	*(필수) 성명, 주민등록번호, 전화번호 의료기관 명칭, 질병분류기호, 의료인의 성명 및 면허종류, 처방의약품, 발급연원일, 사용기간*	*2년 (약사법 제 29조) ※보험급여청구 처방전은 3년간 보관*
조제기록부 관리 및 요양급여 청구	*(필수) 성명, 연락처, 주민등록번호, 질병명, 요양급여비용, 본인부담금 및 비용청구액, 처방전 내용 및 가입자 성명, 건강보험증 번호*	*5년 (약사법 제30조 1항)*
홈페이지 회원가입 (홈페이지가 있는 경우)	*(필수) 성명, 생년월일, ID, 비밀번호, 이메일 주소, 만 14세 미만 아동의 경우 법정대리인 정보(성명, 생년월일, 성별, 휴대전화번호) (선택) 자택전화번호*	*회원 탈퇴 시까지*

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

2. 개인정보의 제3자 제공(요양기관 환경에 맞게 가감하여 작성)

*A*는 정보주체의 개인정보를 명시한 범위 내에서만 처리하며, 정보주체의 동의, 법률의 특별한 규정 등『개인정보 보호법』제17조 및 제18조에 해당하는 경우에만 개인정보를 제3자에게 제공하고 그 외에는 정보주체의 개인정보를 제3자에게 제공하지 않습니다.

*A*는 약사법 제30조 제3항 각 호에 해당하는 경우 조제기록부를 열람하게 하거나 사본을 내주는 등 내용을 확인할 수 있도록 하고 있습니다.

*A*는 응급의료에 관한 법류 제11조에 따라 응급환자를 다른 의료기관으로 이송할 경우 이송받는 의료기관에 진료에 필요한 의무기록을 제공할 수 있습니다.

제공받는 자	제공목적	제공항목	제공 근거 / 보유 및 이용기간
건강보험심사평가원	*요양급여비용의 청구*	*성명, 건강보험증 번호, 주민등록번호, 질병명, 요양급여비용의 내용, 본인부담금 및 비용청구액, 처방전 내용*	*국민건강보험법 제47조*
한국의약품안전관리원	*부작용 등의 확인*	*성명, 성별, 생년월일, 체중, 신장, 임신기간, 월경일, 과거 병력 및 치료 정보, 부모정보, 사망정보*	*약사법 제68조의8*

3. 개인정보의 보유 및 이용기간 및 파기절차 및 파기방법

「약사법」, 「국민건강보험법」에서 정한 보유기간 동안 개인정보를 보유하며 개인정보가 불필요하게 되었을 때에는 지체 없이 개인정보를 파기합니다.

정보주체로부터 동의받은 개인정보 보유기간이 경과하거나 처리목적이 달성되었음에도 불구하고 다른 법령에 따라 개인정보를 계속 보존하여야 하는 경우에는, 해당 개인정보를 별도의 데이터베이스(DB)로 옮기거나 보관장소를 달리하여 보존합니다.

- 보유기간: *처방전 2년(요양급여비용 청구 처방전 3년), 건강보험청구 관련 자료 5년(법령기간),*
- 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 *A*에 연락을 하여 개인정보 열람 등의 권리를 행사할 수 있으며, *A*는 지체 없이 필요한 조치를 합니다.

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

또한 정보주체의 위임을 받은 자 등 대리인이 보건복지부령으로 정하는 요건을 갖추어 요청한 경우에도 기록 열람 등 정보주체의 권리를 행사할 수 있습니다.

5. 개인정보 처리의 위탁(요양기관 환경에 맞게 가감하여 작성)

개인정보를 정보시스템을 통해 관리하기 위해 다음의 회사에 개인정보를 위탁하고 있습니다.

위탁받는 자(수탁자)	위탁업무	보유 및 이용기간
AAA	*청구프로그램 (업무 및 기록의 전산관리)*	*위탁계약 종료시까지*
BBB	*조제기록부 등 폐기*	*위탁계약 종료시까지*
CCC	*CCTV 프로그램 및 내부 보안*	*위탁계약 종료시까지*
DDD	*홈페이지 유지보수*	*위탁계약 종료시까지*

6. 개인정보 보호책임자 및 열람청구

정보주체는 *A*의 서비스를 이용하시면서 발생한 모든 개인정보보호 관련 문의, 불만처리, 피해구제 등에 관한 사항을 개인정보 보호책임자에게 문의할 수 있습니다. *A*는 정보주체의 문의에 대해 지체없이 답변 및 처리해드릴 것입니다.

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

정보주체는 「개인정보 보호법」 제35조에 따른 개인정보의 열람 청구를 아래의 담당자에 할 수 있습니다. *A*는 정보주체의 개인정보 열람청구가 신속하게 처리되도록 노력하겠습니다.

담당자: *홍길동*

연락처: *<전화번호>, <이메일>, <팩스번호>*

7. 권익침해 구제방법

정보주체는 개인정보침해로 인한 구제를 받기 위하여 개인정보분쟁조정위원회, 한국인터넷진흥원 개인정보침해신고센터 등에 분쟁해결이나 상담 등을 신청할 수 있습니다. 이 밖에 기타 개인정보침해의 신고, 상담에 대하여는 아래의 기관에 문의하시기 바랍니다.

1. 개인정보분쟁조정위원회: (국번없이) 1833-6972 (www.kopico.go.kr)
2. 개인정보침해신고센터: (국번없이) 118 (privacy.kisa.or.kr)
3. 대검찰청: (국번없이) 1301 (www.spo.go.kr)
4. 경찰청: (국번없이) 182 (ecrm.cyber.go.kr)

*A*는 정보주체의 개인정보자기결정권을 보장하고 개인정보침해로 인한 상담 및 피해 구제를 위해 노력하고 있으며, 신고나 상담이 필요한 경우 아래의 담당부서로 연락해 주시기 바랍니다.

담당자: *홍길동*

연락처: *<전화번호>, <이메일>, <팩스번호>*

「개인정보 보호법」 제35조(개인정보의 열람), 제36조(개인정보의 정정·삭제), 제37조(개인정보의 처리정지 등)의 규정에 의한 요구에 대 하여 공공기관의 장이 행한 처분 또는 부작위로 인하여 권리 또는 이익의 침해를 받은 자는 행정심판법에 정하는 바에 따라 행정심판을 청구할 수 있습니다.

1. 중앙행정심판위원회: (국번없이) 110 (www.simpan.go.kr)

8. 개인정보의 안전성 확보조치

*A*는 이용자의 개인정보보호를 위한 기술적 대책으로서 여러 보안장치를 마련하고 있습니다. 또한 *A*는 이용자의 개인정보보호를 위한 관리적 대책으로서 이용자의 개인정보에 대한 접근 및 관리에 필요한 절차를 마련하고, 이용자의 개인정보를 처리하는 인원을 최소한으로 제한하고 개인정보를 처리하는 시스템의 접근권한 관리, 접근통제시스템 설치, 보안프로그램 설치 및 갱신 등의 방법으로 안전하게 관리합니다.

9. 추가적인 이용·제공 판단 기준

*A*는 「개인정보 보호법」 제15조제3항 및 제17조제4항에 따라 「개인정보 보호법」 시행령 제14조의2에 따른 사항을 고려하여 정보주체의 동의 없이 개인정보를 추가적으로 이용·제공할 수 있습니다.

항목	이용·제공 목적	보유 및 이용기간
이름, 연락처, 주소	*조제약을 잘못 수령한 사실을 알리기 위한 연락*	*목적 달성 즉시 파기*

이에 따라 *A*는 정보주체의 동의 없이 추가적인 이용·제공을 하기 위해서 다음과 같은 사항을 고려하였습니다.

▶ 개인정보를 추가적으로 이용·제공하려는 목적이 당초 수집 목적과 관련성이 있는지 여부

▶ 개인정보를 수집한 정황 또는 처리 관행에 비추어 볼 때 추가적인 이용·제공에 대한 예측 가능성이 있는지 여부

▶ 개인정보의 추가적인 이용·제공이 정보주체의 이익을 부당하게 침해하는지 여부

10. 고정형 영상정보처리기기 운영·관리에 관한 사항

A의 고정형 영상정보처리기기 운영·관리방침을 알려드립니다.

▶ 고정형 영상정보처리기기의 설치 근거 및 설치 목적

A의 영상정보처리기기를 설치·운영 목적

- 시설안전 및 관리, 화재 예방
- 고객의 안전을 위한 범죄 예방
- 차량도난 및 파손방지(주차장에 설치하는 경우)

▶ 설치 대수, 설치 위치 및 촬영범위

설치대수	설치위치 및 촬영 범위
00대	*건물로비, 주차장 입구*
00대	*약국내 접수대*

▶ 관리책임자 및 접근권한자

구분	이름	직위	소속	연락처
관리책임자	*홍길동*		*0000과*	*00-0000-0000*
접근권한자				

▶ 개인영상정보의 촬영시간, 보관기간, 보관장소 및 처리방법

촬영시간	보관기간	보관장소
24시간	*촬영일로부터 30일*	*OOO실(보관시설 명)*

- 처리방법: 개인영상정보의 목적 외 이용, 제3자 제공, 파기, 열람 등 요구에 관한 사항을 기록·관리하고, 보관기간 만료 시 복원이 불가능한 방법으로 영구삭제(출력물의 경우 파쇄 또는 소각)합니다.

▶ 영상정보처리기기 설치 및 관리 등의 위탁에 관한 사항 (해당하는 경우만)

A의 아래와 같이 고정형 영상정보처리기기 설치 및 관리 등을 위탁하고 있습니다.

수탁업체	담당자	연락처
OO시스템	*홍길동*	*02) 000-0000*

▶ 개인영상정보의 확인 방법 및 장소에 관한 사항

- 확인 방법 : 개인영상정보 관리책임자에게 미리 연락하고 A에 방문
- 확인 장소 : OO부서 OO팀

▶ 정보주체의 개인영상정보 열람 등 요구에 대한 조치

정보주체는 본인의 개인영상정보에 관하여 열람 또는 존재확인·삭제를 원하는 경우 언제든지 A에게 요구하실 수 있습니다.

A는 개인영상정보에 관하여 열람 또는 존재확인·삭제를 요구한 경우 지체없이 필요한 조치를 하겠습니다.

▶ 개인영상정보의 안전성 확보조치

A는 처리하는 개인영상정보를 암호화 등으로 안전하게 관리하고 있습니다.

▶ A는 개인영상정보보호를 위한 관리적 대책으로서 개인영상정보에 대한 접근권한을 차등 부여와 위·변조 방지를 위한 개인영상정보의 생성 일시, 열람 시 열람 목적·열람자·열람

일시 등을 기록·관리하고 있습니다. 또한 안전한 물리적 보관을 위하여 잠금장치를 설치하고 있습니다.

11. 정책 변경에 따른 공지의무

이 개인정보 처리방침은 *20XX년 X월 XX일*에 제정되었으며 법령·정책 또는 보안기술의 변경에 따라 내용의 추가·삭제 및 수정이 있을 시에는 변경되는 개인정보 처리방침을 시행하기 최소 7일전 *홈페이지 또는 접수창구*에 변경이유 및 내용 등을 공지하도록 하겠습니다.

이전의 개인정보 처리방침은 홈페이지 확인 또는 접수창구에 문의주시면 확인하실 수 있습니다.

- 20XX. X. X. ~ 20XX. X. X. 적용
- 20XX. X. X. ~ 20XX. X. X. 적용

3.5.2

개인정보취급자 접속기록 점검표

점검자 /확인자 : 홍 길 동
점검일 : 0000년 00월 00일

개인정보처리시스템명	000시스템	부서명	00000부
개인정보파일명	- AAAA 신청자 정보 - BBBB 회원정보	대상기간	'00.01.01 ~ ' 00.01.30

점검항목		예	아니오	해당 없음	비 고
1. 접속기록이 기록되고 있는가?					
2. 접속기록은 1년 이상 보관되고 있는가? (5만건 이상 / 고유식별번호 또는 민감정보 보유 시스템은 2년 이상)					
3. 접속기록은 1개월에 1번이상 이상 유무 점검이 되고 있는가?					
4. 접속기록 항목은 적정한가? (계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등)					
5. 접속기록이 삭제되거나 분실 또는 변조된 항목이 없는가?					
6. 접속기록 점검	대량(1천건 이상)으로 개인정보를 처리(조회, 다운로드, 출력 등)한 사용자가 있는가?				
	개인정보를 다운로드하는 경우에는 내부 관리계획으로 정하는 바(시스템 또는 관리대장 등)에 따라 사유를 반드시 확인하고 있는가?				
	업무시간 이외 이상접속(휴일·공휴일 또는 새벽 시간 접속 등)을 한 사용자가 없는가?				
	인가되지 않은 사용자가 접속을 한 내역은 없는가?				
	업무 목적 외로 개인정보를 처리한 내역은 없는가?				
	동시 접속하여 비인가자가 개인정보를 처리한 내역은 없는가?				
	비정상 업무 처리한 내역이 없는가?				
	특정사용자의 비정상 패턴 내역이 없는가?				
7. 직전 점검 시 부적합 사항은 조치되었는가?					
8. 기타 특이사항은 없는가?					

[접속기록 분석] 2000.00.00.~00.00

○ 개인정보 접속 화면에 가장 많이 접속한 사용자 중 상위 10명

- AAA, BBB, CCC 등

○ 가장 많이 접속한 개인정보 처리화면 상위 5개 :

시스템명	업무분류	화면명	사용횟수

[특이사항] ○ 해당없음

개인정보 유출 사고 발생 시 이것만은 꼭 조치하세요!

1	**피해 최소화를 위한 대책 마련 및 필요한 조치 실시** ⇨ **「개인정보 보호법」 제34조 제2항** ✓ 개인정보 유출 사고 인지 및 신고 접수 ✓ 개인정보 보호담당자는 개인정보 보호책임자에게 보고 - 사고 내용 등 보고, 보호책임자는 사고 신속 대응팀 구성 ✓ 피해 최소화를 위한 긴급 조치 수행
2	**유출된 정보주체 개개인에게 지체 없이 통지** ⇨ **「개인정보 보호법」 제34조 제1항** ✓ 개인정보 유출시, 정보주체에게 유출사실 통지(72시간 이내) ✓ 통지 항목: ① 유출된 개인정보의 항목 ② 유출 시점과 및 그 경위 ③ 피해 최소화를 위한 정보주체의 조치방법 ④ 기관의 대응조치 및 피해구제 절차 ⑤ 피해 신고 접수 담당부서 및 연락처 *「개인정보 보호법」 제75조 제2항 제17호(**3천만원 이하의 과태료**)
3	**유출 신고(해당 시)** ⇨ **「개인정보 보호법」 제34조 제3항** ✓ 1천명 이상의 정보주체에 관한 개인정보가 유출 등이 된 경우 ✓ 민감정보 또는 고유식별정보가 유출된 경우 ✓ 외부로부터의 불법적인 접근에 의해 개인정보가 유출 등이 된 경우 →보호위원회 또는 전문기관(한국인터넷진흥원, privacy.kisa.or.kr)에 신고 *「개인정보 보호법」 제75조 제2항 제18호(**3천만원 이하의 과태료**)
4	**사고 분석, 결과보고 및 개선** ✓ 사고 원인 분석, 유출 규모 확인, 사고 원인에 대한 조치 등 ✓ 고객 불안 해소 조치 및 피해구제 절차 안내 ✓ 개인정보 유출사고 결과보고서 작성 및 보고 ✓ 유출사고 사례 전파 교육 및 개선 대책 시행(재발방지)

표준 개인정보 보호지침 별지 제1호 서식

2.7.2

개인정보 유출 등 신고서

기관명					
유출등이 된 개인정보 항목 및 규모	• *유출 등이 된 개인정보 항목을 모두 기재해야 하며, '등'과 같이 일부 생략하거나 휴대전화번호와 집 전화번호를 '전화번호'로 기재하여서는 안됨* • *유출 등이 된 개인정보의 모든 항목을 적어야 하며, 유출 등 규모도 현 시점에서 파악된 내용을 모두 작성*				
유출등이 된 시점과 그 경위	• *유출 등 시점, 인지시점을 명확히 구분하여 날짜 및 시간 모두 작성해야 하며, 유출 등 경위와 인지경위를 포함*				
유출등 피해 최소화를 위해 정보주체가 할 수 있는 방법 등	• *개인정보 유출 등으로 발생 가능한 스팸 문자, 보이스피싱, 금융사기와 같은 2차적인 피해 방지를 위해 이용자가 할 수 있는 조치를 기재 (예: 비밀번호 변경 등)*				
개인정보처리자의 대응 조치 및 피해 구제절차	• *유출 등 사실을 안 후 긴급히 조치한 내용과 향후 이용자의 피해구제를 위한 계획 및 절차를 기재* *ex) 경찰에 신고, 일시적 홈페이지 로그인 차단(홈페이지 해킹일 경우) 등*				
정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처	*실제 신고 접수 및 상담이 가능한 전담 처리부서와 해당 담당자 연락처를 기재*				
유출등 신고 담당자		성명	부서	직위	연락처
	개인정보 보호책임자				
	담당자				

유출등 신고 접수기관	기관명	담당자명	연락처

개인정보 자율보호 표준가이드 참고 출처

번호	내 용	비 고
1	개인정보 처리방침 작성지침(2025.4)	개인정보보호위원회
2	개인정보 유출 등 사고 대응 매뉴얼(2024.3.)	개인정보보호위원회
3	개인정보 보호 가이드라인(온라인 경품행사 편) (2023.5.)	개인정보보호위원회
4	개인정보의 안전성 확보조치 기준 안내서(2024.10.)	개인정보보호위원회
5	개인정보의 암호화 조치 안내서(2020.12.)	개인정보보호위원회 한국인터넷진흥원
6	개인정보 교육관련 별첨 자료(내부관리계획)(2021.5.)	한국인터넷진흥원
7	분야별 개인정보 보호 안내서-의료기관, 약국 편(2024.12.)	개인정보보호위원회 보건복지부
8	아동 청소년 개인정보 보호 안내서(2024.12.)	개인정보보호위원회
9	알기 쉬운 개인정보처리 동의 안내서(2022.3.)	개인정보보호위원회
10	암호 키 관리 안내서(2014.12.)	미래창조과학부 한국인터넷진흥원
11	고정형 영상정보처리기기 설치 운영 안내서(2024.12.)	개인정보보호위원회
12	이동형 영상정보처리기기를 위한 개인영상정보 보호·활용 안내서(2024.9.)	개인정보보호위원회 한국인터넷진흥원
13	홈페이지 개인정보 노출방지 안내서(2024.4.)	개인정보보호위원회 한국인터넷진흥원
14	2024년 고유식별정보 안전조치 관리실태 점검 매뉴얼(2024.9.)	개인정보보호위원회 한국인터넷진흥원
15	ISMS-P 인증기준 안내서(2023.11.)	개인정보보호위원회 과학기술정보통신부 한국인터넷진흥원