요양기관 개인정보보호 표준가이드

2020.

사전 질문	결과		점검제외 항목
진료(진찰, 치료)목적 외로 개인정보수집 및 이용(홍보용 SMS발송, 회원가입 등)을 하고 있습니까?	'아니오'	⇨	1.1.1, 1.1.3, 1.2.1, 1.2.2, 1.2.3, 2.1.1, 2.2.1
영상정보처리기기(CCTV)를 설치 운영하고 있습니까?	'아니오'	⇨	2.3.1, 2.3.2, 2.3.3, 2.3.4

사단법인 대한한의사협회
The Association of Korean Medicine

변경 이력

연번	일자	주요내용	비고
1	2015.	▪ 최초 작성	
2	2020.2.12.	▪ (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

분 야	1. 개인정보의 처리(수집・이용・제공 등)	
점검지표	1.1 개인정보의 수집・이용	
점검항목	1.1.1 진료(진찰, 치료) 목적 외로 서면(오프라인) 및 홈페이지(온라인) 등을 통한 개인정보수집 시 동의를 받고 있는가?	Seq: ①
판단기준 (해당여부)	☑ 진료(진찰, 치료) 목적 외로 서면 또는 홈페이지를 통한 회원가입 등 개인정보를 수집하지 않는 경우 해당 없음	
점검기준	☑ 필수항목(4개)을 환자(정보주체)에게 고지하고 동의를 받았는지 여부 확인 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 경우에는 그 불이익의 내용 ☑ 동의 시 명시한 항목과 실제 수집하는 항목간의 일치 여부 확인	
증빙자료	개인정보수집동의서, 회원가입신청서 등 개인정보수집 양식	
관련근거	「개인정보 보호법」 제15조(개인정보의 수집・이용)	
벌금과태료	3천만원 이하 과태료	
세부설명	【설명】 **진료(진찰, 치료) 목적 외**로 서면(오프라인) 또는 홈페이지(온라인) 등을 통해 환자(정보주체)의 개인정보를 수집·이용하는 경우 요양기관(개인정보처리자)은 필수항목 4가지를 환자(정보주체)에게 알리고 동의를 받아야 함 ⇒ 홈페이지를 운영하거나 별도의 서비스(홍보, 마케팅, 상담 등)를 환자(정보주체)에게 제공하는 경우 - 수집되는 개인정보(환자관리용)는 별도의 동의 필요 - **홈페이지 회원가입 개인정보 수집 시,** 정보주체의 동의 필요 ※ 홈페이지 회원가입 정보로 주민등록번호 수집은 불가함 (주민등록번호 수집 없이 회원가입 할 수 있는 방법을 제공) - **홈페이지 내 게시판(건의사항, 상담, 자유게시판 등)을 통해** 개인정보(작성자 성명, 전화번호, 이메일, 비밀번호 등)를 수집하는 경우 필수항목 4가지를 알려주고 동의를 받아야 함 【참고】 개인정보수집동의서 또는 회원가입 신청 서식에 개인정보 수집·이용에 관한 명시적 '동의' 표시(체크) 여부 확인	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

(개인정보 수집·이용 동의서 예시)

1.1.1, 1.1.3, 1.2.1, 1.2.2, 1.2.3, 1.3.1

*○○○서비스 제공*을 위한 개인정보 수집·이용, 제공 동의서(예시)

*[요양기관명]*은 *○○○서비스 제공*을 위하여 아래와 같이 개인정보를 수집·이용 및 제공하고자 합니다. 내용을 자세히 읽으신 후 동의 여부를 결정하여 주십시오.

☐ 선택적 개인정보 수집·이용 내역(선택사항, 동의거부 가능)

항 목	수집목적	보유기간
☐ 성별 ☐ 결혼 여부 ☐ 연령 ☐ 관심 분야	*맞춤형 건강정보 안내 SMS 발송*	*1년*

※ 위의 개인정보 수집·이용에 대한 동의를 거부할 권리가 있습니다. 다만, 이에 동의하지 않을 경우에는 *최신의학정보(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
○○연구소	*의학정보 연구*	*성별, 결혼 여부, 연령, 관심분야*	*1년*

※ 위의 개인정보 제공에 대한 동의를 거부할 권리가 있습니다. 다만, 이에 동의하지 않을 경우에는 *의학정보 연구(서비스명 구체화)* 서비스 제공이 제한됩니다.

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

<기타 고지 사항>

「의료법」에 따라 진료목적인 경우 환자(정보주체)의 동의 없이 개인정보를 수집·이용 할 수 있습니다.

개인정보 처리사유	개인정보 항목	수집 근거
진료기록부 작성	성명, 주민등록번호, 주소, 연락처 등 인적사항	「의료법」 제22조, 동법 시행규칙 제14조

년 월 일

본인 성명 (서명 또는 인)

법정대리인 성명 (서명 또는 인)

[요양기관명]장 귀중

분 야	1. 개인정보의 처리(수집 · 이용 · 제공 등)	
점검지표	1.1 개인정보의 수집 · 이용	
점검항목	1.1.3 진료(진찰, 치료) 목적 외로 만 14세 미만 아동의 개인정보를 수집 · 처리 시, 법정대리인의 동의를 받았는가?	Seq: ②
판단기준 (해당여부)	☑ 진료(진찰, 치료) 목적으로만 개인정보를 수집 · 처리하는 경우 해당 없음	
점검기준	☑ 진료(진찰, 치료) 목적 외 14세 미만 아동의 개인정보를 수집 · 처리 시, 법정대리인의 동의 여부 확인	
증빙자료	개인정보수집동의서, 회원가입신청서 등 개인정보수집 양식	
관련근거	「개인정보 보호법」 제22조(개인정보의 수집 제한)	
벌금과태료	5천만원 이하 과태료	
세부설명	【설명】 **진료(진찰, 치료) 목적**으로 만 14세 미만의 아동의 개인정보를 수집 · 처리하는 경우 「의료법 시행규칙」 제14조(진료기록부 등의 기재 사항)에 근거하여 **법정대리인의 동의 없이 수집 · 처리가 가능함** ⇒ **진료(진찰, 치료) 목적 외**로 수집한 개인정보 중 만 14세 미만 아동의 개인정보가 있을 경우, 해당 개인정보 수집 시 **법정대리인으로부터 동의를 받아야하며, 증빙자료를 통해 확인** 【참고】 요양기관(개인정보처리자)은 만 14세 미만 아동의 법정대리인의 동의를 받기 위하여 해당 아동으로부터 직접 법정대리인의 성명 · 연락처에 관한 정보를 수집할 수 있음	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

분 야	1. 개인정보의 처리(수집・이용・제공 등)	
점검지표	1.2 개인정보의 수집 제한	
점검항목	1.2.1 목적에 필요한 최소한의 개인정보만 수집하고 있는가?	Seq: ③
판단기준 (해당여부)	☑ 진료(진찰, 치료)에 필요한 개인정보만 수집하는 경우 및 서면 또는 홈페이지를 통한 개인정보 수집(회원가입 등)을 하지 않는 경우 해당 없음	
점검기준	☑ 목적달성을 위한 최소한의 개인정보(필수, 선택정보) 수집여부 확인 ☑ 환자(정보주체)에게 최소한의 정보 외의 개인정보(선택정보) 수집에는 동의하지 않을 수 있다는 사실을 고지하는지 여부 확인	
증빙자료	개인정보수집동의서, 회원가입신청서 등 개인정보수집 양식	
관련근거	「개인정보 보호법」 제16조(개인정보의 수집 제한)	
벌금과태료	3천만원 이하 과태료	
세부설명	【설명】 개인정보 수집 목적에 필요한 범위 내에서 **최소한의 개인정보(필수, 선택정보)**만을 수집하여야 함 - 서면(오프라인) 또는 홈페이지(온라인)등에서 개인정보를 수집하는 경우, 목적 달성을 위해 반드시 수집하여야 하는 최소한의 개인정보만을 수집 - 필수정보는 아니나, **추가적인 서비스 제공 등을 위해 필요한 정보(선택정보)**로 수집하는 경우에도 목적 달성을 위한 최소한의 정보를 수집 - 필요한 최소한의 정보(필수정보) 외의 개인정보(선택정보) 수집에는 동의하지 아니할 수 있다는 사실을 명확하게 알려야 함 예시) 홈페이지 회원가입을 통한 정보를 수집하고자 하는 경우 동의 필요**(필수정보)**: 성명, 전화번호 동의거부 가능**(선택정보)**: 성별, 나이 【참고】 최소한의 개인정보 수집 여부에 대한 입증 책임은 요양기관(개인정보처리자)에 있음	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

분 야	1. 개인정보의 처리(수집 · 이용 · 제공 등)	
점검지표	1.2 개인정보의 수집 제한	
점검항목	1.2.2 최소한의 개인정보 수집 외에 선택정보에 대한 미 동의를 이유로 재화 또는 부가서비스 제공을 거부하고 있지 않는가?	Seq: ④
판단기준 (해당여부)	☑ 진료(진찰, 치료)에 필요한 개인정보만 수집하는 경우 및 서면 또는 홈페이지를 통한 개인정보 수집(회원가입 등)을 하지 않는 경우 해당 없음	
점검기준	☑ 필수정보가 아닌 선택정보 미 동의 시에도 회원가입 등 기본적인 서비스를 제공하는지 여부 확인	
증빙자료	개인정보수집동의서, 회원가입신청서 등 개인정보수집 양식	
관련근거	「개인정보 보호법」 제16조(개인정보의 수집 제한)	
벌금과태료	3천만원 이하 과태료	
세부설명	【설명】 요양기관(개인정보처리자)은 환자(정보주체)의 동의를 받아 개인정보를 수집하는 경우, 진료(진찰, 치료) 목적에 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 않을 수 있다라는 사실을 구체적으로 알리고 수집하여야 함 ⇒ 최소한의 개인정보(필수정보) 외의 개인정보(선택정보) 수집에 동의하지 않아도 기본적인 서비스 제공(회원가입 등)이 가능하여야 함 - 환자(정보주체)에게 동의를 받을 시 선택정보에 대한 동의를 거부할 경우 재화 또는 부가서비스의 이용이 제한됨을 알리는 것은 가능 ☞ 홈페이지 회원가입 시 등 선택정보 수집에 동의하지 않으면 다음 페이지로 넘어가지 않는 사례가 있음	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

분 야	1. 개인정보의 처리(수집 · 이용 · 제공 등)	
점검지표	**1.2 개인정보의 수집 제한**	
점검항목	**1.2.3 개인정보 수집 시, 포괄 동의를 받고 있지 않은가?**	**Seq: ⑤**
판단기준 (해당여부)	☑ 진료(진찰, 치료)목적 외로 서면 및 홈페이지를 통한 회원가입, 별도의 서비스(홍보, 마케팅, 상담) 제공을 목적으로 개인정보 수집을 하지 않는 경우 해당 없음	
점검기준	☑ 각각의 개인정보 처리 동의 사항을 구분하여 각각 동의를 받는지 여부 확인	
증빙자료	개인정보수집동의서, 회원가입신청서 등 개인정보수집 양식	
관련근거	「개인정보 보호법」 제22조(동의를 받는 방법)	
벌금·과태료	1천만원 이하 과태료	
세부설명	【설명】 요양기관 담당자(개인정보처리자)가 개인정보의 처리에 대하여 환자(정보주체)의 동의를 받을 때에는 환자가 **동의사항을 명확하게 인지할 수 있도록 구분하고 각각 동의**를 받아야 함 【참고】 <구분 동의가 필요한 경우> ① 개인정보 수집·이용 동의 ② 마케팅 목적 처리 동의 ③ 제3자 제공 동의 ④ 목적 외 이용·제공 동의 ⑤ 법정대리인 동의 ⑥ 민감정보 처리 동의 ⑦ 고유식별정보 처리 동의 ⑧ 국외 제3자 제공 동의 ※ 위의 ②, ④와 같은 경우에는 **목적별로 각각 동의를 받아야 함** ☞ 위와 같이 각각 구분하여 동의를 받아야 하는 사항이나, 포괄 동의만 1회 받는 사례가 다수 존재함	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

분 야	1. 개인정보의 처리(수집・이용・제공 등)	
점검지표	1.3 개인정보의 제공	
점검항목	1.3.1 제3자에게 개인정보 제공 및 목적 외 이용 시 환자(정보주체)의 별도 동의는 받고 있는가?	Seq: ⑥
판단기준 (해당여부)	☑ 제3자*에게 정보제공 및 목적 외 이용 사실이 없는 경우 해당사항 없음 * 제3자: 환자(정보주체) 또는 그의 법정대리인으로부터 개인정보를 수집·보유한 요양기관을 제외한 모든 자(수탁자는 제외)	
점검기준	☑ 법률(의료법, 건강보험법 등)에 근거한 제3자 제공의 경우 해당 법률 준수여부 확인 ☑ 법률에 근거하지 않은 제3자 제공의 경우, 필수 고지항목(①~⑤)을 환자(정보주체)에게 고지하고 동의를 받았는지 여부 확인	
증빙자료	(법률엔 근거하지 않은 제3자 제공 사례가 있는 경우) 제3자 개인정보 제공 동의서(필수고지내용 ①~⑤이 포함된 동의서)	
관련근거	법 제17조(개인정보의 제공), 제18조(개인정보의 목적 외 이용·제공 제한)	
벌금·과태료	5년 이하 징역 또는 5천만원 이하 벌금	
세부설명	【설명】 **법률에서 정한 제3자 제공이 가능한 경우**에는 법률 준수와 별도로 환자(정보주체)에게 고지 후 동의 받을 필요 없음**(해당 법률에 따라 제공하면 됨)** 예시1) 의료법 제21조(기록 열람 등)에 의해 건강보험 급여비용 청구를 위한 개인정보 제공은 환자의 동의 없이 가능함 예시2) 의료법 제21조(기록 열람 등)에 의해 환자의 대리인이 환자의 동의서 및 위임장, 환자의 신분증 및 대리인의 신분증을 제출하는 경우에는 개인정보를 제공 가능함 **법률의 근거 없이** 개인정보 수집 목적을 넘어 이용하거나 제3자에게 제공하는 경우, 다른 개인정보의 처리에 대한 동의와 분리하여 다음 사항을 고지하고 목적 외 이용·제공에 대한 **별도의 동의를 받아야 함** ① 개인정보를 제공받는 자 ② 개인정보를 제공받는 자의 개인정보 이용 목적 ③ 제공하는 개인정보의 항목 ④ 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간 ⑤ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우 그 불이익의 내용	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

<table>
<tr><td>분 야</td><td colspan="2">1. 개인정보의 처리(수집・이용・제공 등)</td></tr>
<tr><td>점검지표</td><td colspan="2">1.5 개인정보 파기</td></tr>
<tr><td>점검항목</td><td>1.5.1 수집한 진료정보 및 개인정보의 보유기간 경과, 처리목적(제공받는 경우 제공받는 목적) 달성 후 지체 없이 개인정보를 파기하고 있는가?</td><td>Seq: ⑦</td></tr>
<tr><td>판단기준
(해당여부)</td><td colspan="2">☑ 필수사항</td></tr>
<tr><td>점검기준</td><td colspan="2">☑ 법률에 규정된 보존기한이 지난 진료정보 및 기타 목적으로 수집한 개인정보를 목적 달성 이후 파기하였는지 여부 확인</td></tr>
<tr><td>증빙자료</td><td colspan="2">파기 사실 확인서 등 증빙자료</td></tr>
<tr><td>관련근거</td><td colspan="2">「개인정보 보호법」 제21조(개인정보의 파기)</td></tr>
<tr><td>벌금과태료</td><td colspan="2">3천만원 이하 과태료</td></tr>
<tr><td>세부설명</td><td colspan="2">【설명】 법률(의료법, 약사법, 건강보험법 등)에 규정된 보존기한이 경과된 진료기록은 파기하여야 함
다만, 계속적인 진료를 위하여 필요한 경우에는 1회에 한정하여 동일 기간만큼 연장 가능함
*「의료법 시행규칙」 제15조(진료기록부 등의 보존)

진료(진찰, 치료)목적 외로 수집한 개인정보는 보유기간의 경과 및 처리목적 달성 시 지체 없이(5일 이내) 그 정보를 파기하여야 함

개인정보 파기 또는 연장 후 개인정보 파기관리대장에 파기사실 확인서와 함께 보관·관리하는 것을 권장함
(「표준개인정보보호지침」 제10조)

【참고】
<table>
<tr><th>법 근거</th><th>의료법(시행규칙 제15조)</th><th>약사법(법 29조, 30조)</th></tr>
<tr><td>기록물
(보존기간)</td><td>환자명부(5년), 진료기록부(10년),
처방전(2년, 건강보험 청구건 5년),
수술기록(10년), 검사소견기록(5년),
방사선 사진 및 그 소견서(5년),
간호기록부(5년), 조산기록부(5년),
진단서 등의 부본(3년)</td><td>처방전(2년, 건강보험 청구건 3년)
조제기록부(5년)</td></tr>
</table>
</td></tr>
<tr><td>점검결과</td><td colspan="2">✓ (양 호) 점검기준 준수
✓ (개선필요) 점검기준 일부 준수
✓ (취 약) 점검기준 미준수
✓ (해당없음) 판단 기준에 따라 해당사항이 없는 경우</td></tr>
</table>

(개인정보 파기 관리대장 예시)

1.5.1
1.5.2

연번	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	○○○	○○○

분 야	1. 개인정보의 처리(수집・이용・제공 등)	
점검지표	1.5 개인정보의 파기	
점검항목	1.5.2 개인정보 파기 시 복구 또는 재생되지 않도록 조치하고 있는가?	Seq: ⑧
판단기준 (해당여부)	☑ 필수사항	
점검기준	☑ 개인정보의 파기 시 복원 불가능한 방법으로 파기 여부 확인	
증빙자료	파기 사실 확인서 등 증빙서류	
관련근거	「개인정보 보호법」 제21조(개인정보의 파기)	
벌금과태료	3천만원 이하 과태료	
세부설명	【설명】 개인정보(파일)의 당초 수집목적이 달성되었거나, 보유기간이 경과되어 파기 시 **복원이 불가능한 방법**으로 영구 삭제하여야 함 개인정보 파기 또는 연장 후 개인정보 파기관리대장에 파기사실 확인서와 함께 보관·관리하는 것을 권장함 (표준개인정보보호지침 제10조) 【참고】 '복원이 불가능한 방법' 이란 현재의 기술수준에서 사회통념상 적정한 비용으로 파기한 개인정보의 복원이 불가능하도록 조치하는 방법을 말함 - 전자적 파일: 청구S/W 파기기능을 이용, 영구삭제S/W, 포맷 등 - 그 외: 소각, 파쇄, 천공, 마스킹 등	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

분 야	1. 개인정보의 처리(수집・이용・제공 등)	
점검지표	**1.5 개인정보의 파기**	
점검항목	**1.5.3 임시파일 및 출력자료 등은 목적달성 후 즉시 파기 하고 있는가?**	**Seq: ⑨**
판단기준 (해당여부)	☑ 개인정보가 포함된 임시파일(출력자료, 전자적 파일)이 없으면 해당 없음	
점검기준	☑ 임시로 출력하거나 PC에 보관하고 있는 개인정보 포함 자료는 사용 후 즉시 파기하는지 여부 확인	
증빙자료	※ 동 항목은 별도의 증빙자료가 없어도 점검기준을 만족하는 경우에 점검결과를 양호로 선택하실 수 있습니다.	
관련근거	「개인정보 보호법」 제21조(개인정보의 파기)	
벌금과태료	3천만원 이하 과태료	
세부설명	【설명】 업무 수행 상 보존 필요성은 없으나, 임시적으로 생성한 파일이나 출력자료는 사용 후 즉시 파기하여야 함 - 출력자료를 불필요하게 생산하지 말아야 하며 **환자의 정보가 담긴 문서(접수증, 진료기록부 사본, 처방전 등)가 대기실, 접수대에 방치되지 않도록 관리**해야 함 - 업무용 PC에 보관중인 개인정보가 포함된 임시파일(한글문서, 워드, 엑셀, 환자사진 등) 또한 목적 달성 후 즉시 파기해야 함 ▪ 임시 저장이 필요한 경우 반드시 암호화(비밀번호 설정)하여 저장 ※ 비밀번호 설정 시 단순 숫자·문자열 사용 금지 (3.2.3 항목의 안전한 비밀번호 작성규칙 준수 권장) ▪ 주기적으로 임시파일 존재여부 점검 및 삭제	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

분 야	1. 개인정보의 처리(수집・이용・제공 등)	
점검지표	**1.5 개인정보의 파기**	
점검항목	**1.5.4 법령(전자상거래법, 형사소송법, 민사소송법 등)에 따라 개인정보를 파기하지 않고 보존하는 경우 별도로 분리 보관하고 있는가?**	**Seq: ⑩**
판단기준 (해당여부)	☑ 파기대상임에도 불구하고 법령(전자상거래법, 형사소송법, 민사소송법 등)에 근거하여 파기하지 않고 계속 보존하는 개인정보가 없으면 해당 없음	
점검기준	☑ 파기대상임에도 불구하고 법령에 따라 보존하는 개인정보를 적절한 방법으로 분리 보관하는지 여부 확인	
증빙자료	※ 동 항목은 별도의 증빙자료가 없어도 점검기준을 만족하는 경우에 점검결과를 양호로 선택하실 수 있습니다.	
관련근거	「개인정보 보호법」 제21조(개인정보의 파기)	
벌금과태료	1천만원 이하 과태료	
세부설명	【설명】 **수집목적이 달성된 개인정보**나 **보존기한이 지난 진료기록**의 경우에도 전자상거래법, 형사소송법, 민사소송법 등의 **법령에 근거하여 개인정보 전부 또는 일부를 파기하지 않고 보존**한다면, 그 개인정보를 **별도로 분리**(서면인 경우 물리적 장소에, 전자적 파일인 경우 별도의 DB, Table, 파일 등으로 분리)하여 보관하여야 함 【참고】 접근권한은 해당업무 담당자 등의 필수요원으로 엄격히 제한 - 법령에 따라 분리 보관한다는 의미는 소송, 민원 등 특정한 상황이 아니면 접근할 필요가 없다는 것임 ※ 법원·경찰 등에서 법률에 의해서 보존요청이 올 경우 요청기간에 따라 보존하여야함	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

분 야	2. 개인정보의 처리 제한	
점검지표	2.1 민감정보의 처리제한	
점검항목	2.1.1 진료(진찰, 치료)목적 외로 사상, 정치, 건강 등 민감정보의 동의에 의한 수집 및 제공 시 별도로 동의 받고 있는가?	Seq: ⑪
판단기준 (해당여부)	☑ 진료(진찰, 치료)목적 외로 민감정보*를 수집하지 않는 경우 해당 없음 * 민감정보: 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 유전정보, 범죄경력자료 등	
점검기준	☑ 진료(진찰, 치료)목적 외로 민감정보를 수집 시 일반적인 개인정보 수집 동의와 별도로 동의를 받는지 여부 확인	
증빙자료	개인정보수집동의서, 민감정보 수집 동의서 등 민감정보 수집 양식	
관련근거	「개인정보 보호법」 제23조(민간정보의 처리 제한)	
벌금과태료	5년 이하 징역 또는 5천만원 이하 벌금	
세부설명	【설명】 **진료(진찰, 치료)목적의 민감정보 처리**는 법률에 의해 환자(정보주체)의 별도 **동의 없이 처리 가능함** **진료(진찰, 치료)목적 외** 또는 **법률에 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	
	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

(민감정보 수집·이용 동의서 예시)

2.1.1

○○○을 위한 민감정보 수집·이용 동의서(예시)

[기관명] 은(는) 개인정보보호법 등 관련 법령상의 개인정보 보호 규정을 준수하며 회원의 개인정보 보호에 최선을 다하고 있습니다. *[기관명]* 은(는) 개인정보보호법 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 일부 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

분 야	2. 개인정보의 처리 제한	
점검지표	**2.2 고유식별정보의 처리제한**	
점검항목	**2.2.1 관련법령에 의거하여 고유식별정보를 수집 및 처리하고 있는가?**	**Seq: ⑫**
판단기준 (해당여부)	☑ 고유식별정보를 수집하지 않는 경우 해당 없음 (고유식별정보: 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호)	
점검기준	☑ 관련법령에 의거하여 고유식별정보를 수집하는지 여부 확인	
증빙자료	※ 동 항목은 별도의 증빙자료가 없어도 점검기준을 만족하는 경우에 점검결과를 양호로 선택하실 수 있습니다.	
관련근거	법 제24조(고유식별정보의 처리 제한), 제24조의 2(주민등록번호 처리의 제한)	
벌금과태료	5년 이하의 징역 또는 5천만원 이하의 벌금, 3천만원 이하의 과태료	
세부설명	【설명】 **진료(진찰, 치료)목적의 고유식별정보 처리**는 법률에 의해 환자(정보주체)의 **별도 동의 없이 처리 가능함** **진료(진찰, 치료)목적 외** 또는 **법률에 근거하지 않고** 고유식별정보를 처리할 경우 환자(정보주체)에게 **별도의 동의를 받아야 함** ※ 단, **주민등록번호**는 **법령에서 구체적으로 처리를 요구하거나 허용한 경우***에 한하여 처리가능 * 법률, 대통령령, 국회규칙, 대법원규칙, 헌법재판소규칙, 중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우 - 고유식별정보(주민등록번호 제외) 수집·이용 시 고지사항 ▪ 고유식별정보의 수집·이용 목적 ▪ 수집하려는 고유식별정보의 항목 ▪ 고유식별정보의 보유 및 이용기간 ▪ 동의거부권 및 동의 거부에 따른 불이익 안내	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

분 야	2. 개인정보의 처리 제한	
점검지표	2.3 영상정보처리기기 설치운영 제한	
점검항목	2.3.1 영상정보처리기기(CCTV) 운영·관리방침을 수립하고 있는가?	Seq: ⑬
판단기준 (해당여부)	☑ 영상정보처리기기(CCTV)가 없는 경우는 해당 없음	
점검기준	☑ 영상정보처리기기(CCTV) 운영·관리방침 수립 여부 확인 ☑ 영상정보처리기기(CCTV) 운영·관리방침 공개 여부 확인	
증빙자료	영상정보처리기기(CCTV) 운영·관리 방침(필수 기재사항 ①~⑧ 포함하여 수립)	
관련근거	「개인정보 보호법」 제25조(영상정보처리기기의 설치운영 제한), 「개인정보 보호법 시행령」 제25조(영상정보처리기기의 운영.관리 방침)	
벌금·과태료	없음	
세부설명	【설명】 영상정보처리기기(CCTV) 운영자는 아래 내용이 포함된 영상정보처리기기(CCTV) 운영·관리방침을 마련하고, 이를 공개하여야 함 (법 제25조 제7항, 시행령 제25조) **<영상정보처리기기(CCTV) 운영·관리 방침에 포함되어야 할 사항>** ① 영상정보처리기기의 설치 근거 및 설 치 목적 ② 영상정보처리기기의 설치 대수, 설치 위치 및 촬영 범위 ③ 관리책임자, 담당 부서 및 영상정보에 대한 접근 권한이 있는 사람 (수탁자 포함) ④ 영상정보의 촬영시간, 보관기간, 보관 장소 및 처리방법 ⑤ 영상정보처리기기 운영자의 영상정보 확인 방법 및 장소 ⑥ 정보주체의 영상정보 열람 등 요구에 대한 조치 ⑦ 영상정보 보호를 위한 기술적·관리적 및 물리적 조치 ⑧ 그 밖에 영상정보처리기기의 설치·운영 및 관리에 필요한 사항 **<영상정보처리기기(CCTV) 운영·관리 방침 공개 방법>** 영상정보처리기기 운영·관리 방침은 개인정보 처리방침과 동일하게 인터넷 홈페이지 또는 보기 쉬운 장소(접수대 등)에 게시 하여야 함 ※ 개인정보 처리방침에 포함하여 수립·공개해도 됨 【참고】 영상정보처리기기 운영·관리 방침은 영상정보처리기기(CCTV)의 운영 책임기관에서 수립하여 관리 함(위탁 운영하는 경우에는 위탁자가 운영·관리 방침을 수립·관리)	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

2.3.1

【 영상정보처리기기(CCTV) 운영·관리 방침 】

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

1. 영상정보처리기기의 설치 근거 및 설치 목적

본 사는 개인정보보호법 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 영상정보를 보호하고 개인영상정보와 관련한 불만을 처리하기 위하여 아래와 같이 개인영상정보 보호책임자를 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. 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*

6. 개인영상정보의 확인 방법 및 장소에 관한 사항

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

- 확인 장소: OO부서 OO팀

7. 정보주체의 영상정보 열람 등 요구에 대한 조치

귀하는 개인영상정보에 관하여 열람 또는 존재확인·삭제를 원하는 경우 언제든지 영상정보처리기기 운영자에게 요구하실 수 있습니다. 단, 귀하가 촬영된 개인영상정보 및 명백히 정보주체의 급박한 생명, 신체, 재산의 이익을 위하여 필요한 개인영상정보에 한정됩니다.

본 사는 개인영상정보에 관하여 열람 또는 존재확인·삭제를 요구한 경우 지체 없이 필요한 조치를 하겠습니다.

8. 영상정보의 안전성 확보조치

본 사는 처리하는 영상정보는 암호화 조치 등을 통하여 안전하게 관리되고 있습니다. 또한 본 사는 개인영상정보보호를 위한 관리적 대책으로서 개인정보에 대한 접근 권한을 차등부여하고 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.

9. 영상정보처리기기 운영·관리방침 변경에 관한 사항

이 영상정보처리기기 운영·관리방침은 2012년 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

※ 본 서식은 반드시 요양기관의 실제 현황에 맞게 수정하여 사용하여야 함

분 야	2. 개인정보의 처리 제한	
점검지표	2.3 영상정보처리기기의 설치운영 제한	
점검항목	2.3.2 영상정보처리기기(CCTV)를 설치한 장소에 정보주체가 영상정보 처리기기(CCTV) 설치 사실을 인지할 수 있도록 필수 기재 사항을 포함한 안내판을 설치하고 있는가?	Seq: ⑭
판단기준 (해당여부)	☑ 영상정보처리기기(CCTV)가 없는 경우는 해당 없음	
점검기준	☑ 안내판 설치(필수 기재사항 ①~④ 포함) 여부 확인	
증빙자료	안내판 설치 장소 및 내용	
관련근거	「개인정보 보호법」 제25조(영상정보처리기기의 설치운영 제한)	
벌금과태료	1천만원 이하 과태료	
세부설명	【설명】 요양기관 내 공개된 장소에 영상정보처리기기(CCTV)를 설치·운영하는 경우 **환자(정보주체)가 쉽게 인식할 수 있도록 안내판을 설치**하여야 함 **안내판에 필수기재 하여야 할 사항** ① 설치 목적 및 장소 ② 촬영 범위 및 시간 ③ 관리책임자의 성명(또는 직책) 및 연락처 ④ (영상정보처리기기(CCTV) 설치·운영을 위탁한 경우) 수탁자의 명칭 및 연락처 건물 안에 다수의 영상정보처리기기(CCTV)를 설치하는 경우에는 출입구 등 잘 보이는 곳에 해당시설 또는 장소 전체가 영상정보처리기기 설치지역임을 표시하는 안내판을 설치할 수 있음 【참고】 요양기관의 진료실, 처치실, 수술실, 입원실 등의 공간에 영상정보처리기기(CCTV)를 설치하여 개인영상 등을 수집하고자 하는 경우에는 정보주체의 수집·이용 동의를 받아야 함 (단, 정신보건법에 의한 수용시설을 갖춘 정신의료기관, 정신질환자 사회복귀시설, 정신요양시설은 제외)	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

(CCTV 설치 안내판 예시)

2.3.2

CCTV 설치 안내

◈ 설치목적: *범죄예방 및 시설안전*
◈ 설치장소: *건물 출입문*
◈ 촬영범위: *50M 전방향*
◈ 촬영시간: *24시간*
◈ 관리책임자: *OO과 홍길동 (00-000-0000)*

(설치·운영을 위탁한 경우)
◈ 위탁관리자: *OO업체 박길동 (00-000-0000)*

분 야	2. 개인정보의 처리 제한	
점검지표	2.3 영상정보처리기기 설치운영 제한	
점검항목	2.3.3 영상정보처리기기(CCTV)에 대한 이용·제공·열람·파기 내역을 기록하고 관리 하는가?	Seq: ⑮
판단기준 (해당여부)	☑ 영상정보처리기기(CCTV)가 없는 경우는 해당 없음	
점검기준	☑ 개인영상정보 관리대장 작성·관리 여부 확인	
증빙자료	개인영상정보 관리대장	
관련근거	「표준 개인정보 보호지침」 제42조(이용·제3자 제공·파기의 기록 및 관리)	
벌금·과태료	없음	
세부설명	【설명】 영상정보처리기기(CCTV) 운영자는 개인영상정보를 ① 수집 목적 이외로 이용하거나 제3자에게 제공하는 경우, ② 파기하는 경우, ③ 열람 요청이 있는 경우에는 아래 사항을 기록하고 관리하여야 함 **- 이용 또는 제공하는 경우** ① 개인영상정보 파일의 명칭 ② 이용 하거나 제공받은 자(공공기관 또는 개인)의 명칭 ③ 이용 또는 제공의 목적(법령상 이용 또는 제공 근거가 있는 경우 그 근거) ④ 이용 또는 제공의 기간이 정하여져 있는 경우에는 그 기간 ⑤ 이용 또는 제공의 형태 **- 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 보관기관은 개인영상정보 수집 후 30일 이내로 파기하는 것을 권장함 **- 열람하는 경우** ① 개인영상정보 열람을 요구한 정보주체의 성명 및 연락처 ② 열람을 요구한 개인영상정보 파일 명칭 및 내용 ③ 열람의 목적 ④ 열람을 거부한 경우 거부의 구체적 사유, ⑤ 사본을 제공한 경우 해당 영상정보의 내용과 제공한 사유	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

(개인영상정보 관리대장)

2.3.3

개인영상정보 관리대장

연번	구분	일시	파일명 /형태	담당자/	목적/ 사유	이용·제공받는 제3자 /열람 등 요구자	이용·제공·열람 거부 시 구체적 사유	사본 제공 사유
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							

분 야	2. 개인정보의 처리 제한	
점검지표	2.3 영상정보처리기기의 설치운영 제한	
점검항목	2.3.4 영상정보처리기기(CCTV)가 분실·도난·유출·변조 또는 훼손되지 아니하도록 안전성 확보조치를 하고 있는가?	Seq: ⑯
판단기준 (해당여부)	☑ 영상정보처리기기(CCTV)가 없는 경우는 해당 없음	
점검기준	☑ 영상정보처리기기(CCTV)보관 시설 마련 또는 잠금장치 설치 여부 확인 ☑ 영상정보처리기기(CCTV)에 대한 접근통제 여부 확인	
증빙자료	※ 동 항목은 별도의 증빙자료가 없어도 점검기준을 만족하는 경우에 점검결과를 양호로 선택하실 수 있습니다.	
관련근거	「개인정보 보호법」 제25조(영상정보처리기기의 설치운영 제한)	
벌금·과태료	2년 이하 징역 또는 2천만원 이하 벌금, 3천만원 이하의 과태료	
세부설명	【설명】 개인영상정보가 분실·도난·유출·변조 또는 훼손되지 않도록 개인영상정보의 안전성 확보에 필요한 조치를 하여야 함 - 개인영상정보의 안전한 물리적 보관을 위한 별도 보관시설 마련 또는 잠금장치 설치 - 영상정보처리기기(CCTV)에 대한 접근 통제 및 접근 권한 제한	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

<table>
<tr><td>분 야</td><td colspan="2">2. 개인정보의 처리 제한</td></tr>
<tr><td>점검지표</td><td colspan="2">2.4 업무위탁에 따른 개인정보의 처리제한</td></tr>
<tr><td>점검항목</td><td>2.4.1 위탁 계약 시 문서(계약서)에 의한 계약을 하였는가?</td><td>Seq: ⑰</td></tr>
<tr><td>판단기준
(해당여부)</td><td colspan="2">☑ 위탁하는 업무*가 없으면 해당 없음
* 위탁업무 예시
· 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</td></tr>
<tr><td>점검기준</td><td colspan="2">☑ 위탁사업자별 계약서에 필수사항(7개)이 포함되었는지 여부 확인</td></tr>
<tr><td>증빙자료</td><td colspan="2">위탁사업자별 계약서(필수사항이 포함된 위·수탁 계약서, 협약서, 특약서 등)</td></tr>
<tr><td>관련근거</td><td colspan="2">「개인정보 보호법」 제26조(업무위탁에 따른 개인정보의 처리제한)</td></tr>
<tr><td>벌금·과태료</td><td colspan="2">1천만원 이하 과태료</td></tr>
<tr><td>세부설명</td><td colspan="2">【설명】 개인정보 처리 위탁문서(계약서)에 포함되어야 할 내용
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

【참고】 업무위탁과 제3자 제공 비교
<table>
<tr><th>구분</th><th>업무위탁</th><th>제3자 제공</th></tr>
<tr><td>관련조항</td><td>「개인정보 보호법」 제26조</td><td>「개인정보 보호법」 제17조</td></tr>
<tr><td>예시</td><td>배송업무 위탁, TM 위탁 등</td><td>사업제휴, 개인정보 판매 등</td></tr>
<tr><td>이전목적</td><td>위탁자의 이익을 위해 처리</td><td>제3자의 이익을 위해 처리</td></tr>
<tr><td>예측가능성</td><td>정보주체가 사전 예측 가능
(정보주체의 신뢰 범위 내)</td><td>정보주체가 사전예측 곤란
(정보주체의 신뢰 범위 밖)</td></tr>
<tr><td>이전방법</td><td>원칙: 위탁사실 공개
예외: 위탁사실 고지(마케팅 업무 위탁)</td><td>제공목적 등 고지 후 정보주체 동의 획득</td></tr>
<tr><td>관리·감독책임</td><td>위탁자 책임</td><td>제공받는 자 책임</td></tr>
<tr><td>손해배상책임</td><td>위탁자 부담(사용자 책임)</td><td>제공받는 자 부담</td></tr>
</table></td></tr>
<tr><td>점검결과</td><td colspan="2">✓ (양 호) 점검기준 준수
✓ (개선필요) 점검기준 일부 준수
✓ (취 약) 점검기준 미준수
✓ (해당없음) 판단 기준에 따라 해당사항이 없는 경우</td></tr>
</table>

(표준 개인정보처리위탁 계약서)

※ 계약 체결 시, 관련 법 조항의 변경사항 유무 등 확인 필요

2.4.1

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(안)

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

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

제2조 (용어의 정의) 본 계약에서 별도로 정의되지 아니한 용어는「개인정보 보호법」, 같은 법 시행령 및 시행규칙,「개인정보의 안전성 확보조치 기준」(행정안전부 고시 제2019-47호) 및「표준 개인정보 보호지침」(행정안전부 고시 제2017-1호)에서 정의된 바에 따른다.

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

1. 개인정보의 암호화　　*2. 프로그램의 유지보수*

제4조 (재위탁 제한) ① "을"은 "갑"의 사전 승낙을 얻은 경우를 제외하고 "갑"과의 계약상의 권리와 의무의 전부 또는 일부를 제3자에게 양도하거나 재위탁할 수 없다.

② "을"이 다른 제3의 회사와 수탁계약을 할 경우에는 "을"은 해당 사실을 계약 체결 7일 이전에 "갑"에게 통보하고 협의하여야 한다.

제5조 (개인정보의 안전성 확보조치) "을"은「개인정보 보호법」제23조제2항 및 제24조제3항 및 제29조, 같은 법 시행령 제21조 및 제30조,「개인정보의 안전성 확보조치 기준」(행정안전부 고시 제2019-47호)에 따라 개인정보의 안전성 확보에 필요한 관리적·기술적 조치를 취하여야 한다.

제6조 (개인정보의 처리제한) ① "을"은 계약기간은 물론 계약 종료 후에도 위탁업무 수행 목적 범위를 넘어 개인정보를 이용하거나 이를 제3자에게 제공 또는 누설하여서는 안 된다.

1) 고객만족도 조사 업무, 회원가입 및 운영 업무, 사은품 배송을 위한 성명, 주소, 연락처 처리 등

② “을”은 계약이 해지되거나 또는 계약기간이 만료된 경우 위탁업무와 관련하여 보유하고 있는 개인정보를 「개인정보 보호법」 시행령 제16조 및 「개인정보의 안전성 확보조치 기준」(행정안전부 고시 제2019-47호)에 따라 즉시 파기하거나 “갑”에게 반납하여야 한다.

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

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

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

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

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

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

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

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

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

20 . . .

갑	을
○○시 ○○구 ○○로 ○○	○○시 ○○구 ○○로 ○○
성 명: (인)	성 명: (인)

2) 「개인정보 안전성 확보조치 기준 고시」(행정안전부 고시 제2019-47호) 및 「개인정보 보호법」 제26조에 따라 위탁자는 수탁자에 대해서 교육을 의무적으로 시행하여야 한다. 이때 수탁자는 개인정보를 취급하는 소속 직원으로 본다.

분 야	2. 개인정보의 처리 제한	
점검지표	2.4 업무위탁에 따른 개인정보의 처리제한	
점검항목	2.4.2 수탁업체에 대한 교육 및 처리현황 점검 등 관리 감독을 실시하고 있는가?	Seq: ⑱
판단기준 (해당여부)	☑ 위탁하는 업무가 없으면 해당 없음	
점검기준	☑ 수탁업체에 대한 개인정보보호 교육 실시 여부 ☑ 수탁업체가 위탁한 개인정보처리 업무를 적절하게 처리하고 있는지 점검·확인 여부	
증빙자료	수탁업체 대상 관리·감독 및 개인정보보호 교육 결과 등	
관련근거	「개인정보 보호법」 제26조(업무위탁에 따른 개인정보의 처리제한)	
벌금·과태료	없음	
세부설명	【설명】 요양기관에서 개인정보를 처리하는 업무를 위탁하는 경우 **수탁업체 교육** - 환자(정보주체)의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 수탁자를 교육 ※ 수탁업체를 대상으로 교육이 현실적으로 어려운 경우 수탁업체의 자체 개인정보보호 교육 실시 증빙서류를 받아 보관하는 것으로 대신할 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 개인정보보호 실태 점검표**"를 이용하여 기록·보관할 수 있음 - 수탁업체를 대상으로 직접 관리·감독이 어려운 경우 수탁업체 자체적으로 개인정보의 안전성 확보조치 등에 대한 점검 등을 실시하여 그 결과를 "**수탁업체 개인정보보호 실태 점검표**"를 제출 받아 보관하는 것으로 대신할 수 있음 【참고】 수탁자가 상시적으로 위탁업무를 처리하지 않는 경우, 계약서에 자체 교육 및 감독에 관한 사항을 명시하고 위탁업무 발생 시 보안서약서, 확인서 등 증빙자료를 확보해 놓을 수 있음	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

(수탁업체 개인정보보호 실태 점검표 예시)

2.4.2

수탁업체 개인정보보호 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*				

※『개인정보의 안전성 확보조치 기준(행정안전부고시 제2019-47호)』 참조

※ 위탁업무내용에 따라 점검항목 조정 가능 함

분 야	2. 개인정보의 처리 제한	
점검지표	2.4 업무위탁에 따른 개인정보의 처리제한	
점검항목	2.4.3 위탁에 관한 사실을 인터넷 홈페이지 또는 사보, 접수실, 대기실 등에 공개 하고 있는가?	Seq: ⑲
판단기준 (해당여부)	☑ 위탁하는 업무가 없으면 해당 없음	
점검기준	☑ 위탁에 관한 사실 공개(필수사항을 포함)여부 확인	
증빙자료	위탁에 관한 사실을 공개한 증빙자료(개인정보 처리방침 등)	
관련근거	「개인정보 보호법」 제26조(업무위탁에 따른 개인정보의 처리제한)	
벌금과태료	1천만원 이하 과태료	
세부설명	【설명】 요양기관(개인정보처리자)은 위탁하는 업무의 내용과 수탁자를 정보주체가 언제든지 쉽게 확인 할 수 있도록 공개해야 함 - **공개 필수사항(수탁기관명, 위탁업무내용)** - 공개 방법 ① 인터넷 홈페이지(운영 요양기관만 해당)공개내역 화면 ② 사업자의 보기 쉬운 장소인 접수실, 대기실 등에 게재 【참고】 개인정보 처리방침의 '위탁에 관한 사실' 항목에 포함하여 작성 후 공개도 가능함	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

분 야	2. 개인정보의 처리 제한	
점검지표	**2.5 개인정보 취급자에 대한 감독**	
점검항목	**2.5.1 개인정보취급자에 대한 보안 서약서를 제출토록 하였는가?**	**Seq: ⑳**
판단기준 (해당여부)	☑ 개인정보를 취급하는 직원 및 수탁업체 직원이 없는 경우(1인 운영 요양기관) 해당 없음	
점검기준	☑ 개인정보취급자로부터 보안서약서 수령 여부 확인	
증빙자료	개인정보취급자 보안서약서 등 관리·감독 증빙자료	
관련근거	「개인정보 보호법」 제28조(개인정보 취급자에 대한 감독)	
벌금·과태료	없음	
세부설명	【설명】 대표자(원장, 약국장)는 직원(개인정보취급자)에게 보안서약서를 제출하도록 하는 등 적절한 관리·감독을 해야 함 위탁업무를 직접 수행하는 수탁업체 담당자의 보안서약서를 제출받고 담당자의 변경이 발생하는 경우 수탁업체로부터 변경이력의 보고 및 보안서약서를 받아야 함 【참고】 표준개인정보보호지침 제15조(개인정보취급자에 대한 감독) ※ 개인정보취급자: 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 임직원(대진의(약사), 파견근로자, 시간제근로자 포함) 등을 말함	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

(보안서약서 예시)

2.5.1

보안 서약서

□ 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「개인정보보호법」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)

분 야	2. 개인정보의 처리 제한	
점검지표	2.5 개인정보 취급자에 대한 감독	
점검항목	2.5.2 개인정보취급자에 대한 정기적인 교육은 실시하고 있는가?	Seq: ㉑
판단기준 (해당여부)	☑ 필수사항	
점검기준	☑ 내부관리계획 또는 연간 개인정보보호 교육계획에 따라 교육 실시 여부 확인(연 1회 이상 교육 실시하여야 함)	
증빙자료	개인정보보호 교육 결과(교육수료증, 교육 참석 서명록 등)	
관련근거	「개인정보 보호법」 제28조(개인정보 취급자에 대한 감독), 제29조(안전조치 의무), 제31조(개인정보 보호책임자의 지정)	
벌금과태료	없음	
세부설명	【설명】 대표자(원장, 약국장)는 직원(개인정보취급자)을 대상으로 **매년 정기적으로 개인정보보호 교육을 실시**하여야 함 **※ 교육내용 및 방법은 요양기관 자체 내부관리계획(3.1.1 항목)에 따라 시행하여야 함** - 교육방법: 기관의 환경을 고려하여 집합교육, **인터넷 교육***, 외부 교육과정 참석, 전문 강사초빙 등 다양한 방법을 활용 가능 *** 요양기관업무포털(biz.hira.or.kr) 제공 동영상교육 참고** - 교육대상: 개인정보 및 관련설비(서버, PC, CCTV등)에 직·간접적으로 접근하는 내부직원 및 외주용역업체 직원 등 모든 인력포함 ※ 관련설비·장비가 위치한 장소에 접근할 수 있는 청소원, 경비원 등에게도 기본적인 정보보호 인식교육 수행	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

(개인정보보호 교육 서명록 예시)

2.5.2

개인정보보호 교육 서명록

○ 교육일자: *20XX년 XX월 XX일*
○ 교육장소: *대회의실*
○ 교육내용: *업무처리시 개인정보보호 준수사항*

연번	부서명	직급	성명	서명
1	*ㅇㅇ과*	*과장*	*ㅇㅇㅇ*	*ㅇㅇㅇ*
2	*ㅇㅇ과*	*대리*	*ㅇㅇㅇ*	*ㅇㅇㅇ*

※ 본 서식은 요양기관의 업무현황에 맞게 수정하여 사용할 수 있음

(개인정보보호 교육 수료증, 요양기관업무포털 biz.hira.or.kr 발급)

분 야	3. 개인정보의 안전한 관리	
점검지표	**3.1 내부관리 계획수립 시행**	
점검항목	**3.1.1 내부관리 계획을 수립하고 필수사항을 포함하고 있는가?**	**Seq: ㉒**
판단기준 (해당여부)	☑ 총 1만 명 미만의 환자(정보주체) 개인정보를 보유한 소상공인(상시근로자 수 5인 미만)의 경우 해당 없음	
점검기준	☑ 필수 사항을 포함한 내부관리계획(필수사항 ①~⑫) 수립 여부 확인	
증빙자료	내부관리계획서(필수 반영 사항 포함)	
관련근거	「개인정보 보호법」 제29조(안전조치 의무)	
벌금과태료	3천만원 이하 과태료	
세부설명	【설명】 요양기관(개인정보처리자)은 개인정보를 안전하게 처리하기 위하여 내부 의사결정절차를 통하여 내부기준을 수립하여 시행하여야 함 **- 내부관리계획 수립 시 필수 반영사항(①~⑫) 포함여부 확인** ① 개인정보 보호책임자의 지정에 관한 사항 ② 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항 ③ 개인정보취급자에 대한 교육에 관한 사항 ④ 접근 권한의 관리에 관한 사항 ⑤ 접근 통제에 관한 사항 ⑥ 개인정보의 암호화 조치에 관한 사항 ⑦ 접속기록 보관 및 점검에 관한 사항 ⑧ 악성프로그램 등 방지에 관한 사항 ⑨ 물리적 안전조치에 관한 사항 ⑩ 개인정보 보호조직에 관한 구성 및 운영에 관한 사항 ⑪ 개인정보 유출사고 대응 계획 수립·시행에 관한 사항 ⑫ 그 밖에 개인정보보호를 위하여 필요한 사항 요양기관(개인정보처리자)은 각 호의 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 함	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

(내부관리계획 예시)

※ (붉은색) 반드시 요양기관 환경에 맞게 수정 필요

3.1.1

개인정보 내부관리 계획

[*요양기관명*]

목 차

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(*인적사항신청서, 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. “개인정보”란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.
2. “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.
3. “정보주체”란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
4. “개인정보처리자”란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
5. “개인정보 보호책임자”란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지거나 업무처리를 최종적으로 결정하는 자로서, 법 제31조에 따른 지위에 해당하는 자를 말한다.
6. “개인정보 보호담당자”란 개인정보 보호책임자가 업무를 수행함에 있어 보조적인 역할을 하는 자를 말하며 개인정보 보호책임자가 일정 요건의 자격을 갖춘 이를 지정한다.
7. “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.
8. “개인정보처리시스템”이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다.

9. “영상정보처리기기”란 폐쇄회로텔레비전(CCTV), 네트워크카메라 등 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 일체의 장치를 말한다.
10. “개인영상정보”라 함은 영상정보처리기기에 의하여 촬영·처리되는 영상정보 중 개인의 초상, 행동 등 사생활과 관련된 영상으로서 해당 개인의 동일성 여부를 식별할 수 있는 정보를 말한다.
11. “영상정보처리기기 운영자”라 함은 개인정보 보호법 제25조제1항 각호에 따라 영상정보처리기기를 설치·운영하는 자를 말한다.
12. “영상정보 보호책임자”라 함은 개인영상정보의 처리에 관한 업무를 총괄해서 책임지는 자로서, 표준지침 제41조에 따라 영상정보처리기기 운영자가 지정한 자를 말한다.

제2장(내부관리계획의 수립 및 시행)

제4조(내부관리계획의 수립 및 승인)

1. 개인정보 보호책임자는 *[요양기관명] 고객 및 임직원*의 개인정보보호를 위한 전반적인 사항을 포함하여 내부관리계획을 수립하여야 한다.
2. 개인정보 보호책임자는 개인정보보호를 위한 내부관리계획의 수립 시 개인정보보호와 관련한 법령 및 관련 규정을 준수하도록 내부관리계획을 수립하여야 한다.
3. 개인정보 보호책임자는 개인정보 보호담당자가 수립한 내부관리계획의 타당성을 검토하여 개인정보보호를 위한 내부관리계획을 승인하여야 한다.
4. 개인정보 보호담당자는 개인정보보호 관련 법령의 제·개정 사항 등을 반영하기 위하여 매년 11월말까지 내부관리계획의 타당성과 개정 필요성을 검토하여야 한다.
5. 개인정보 보호담당자는 모든 항목의 타당성을 검토한 후 개정할 필요가 있다고 판단되는 경우 12월말까지 내부관리계획의 개정안을 작성하여 개인정보 보호책임자에게 보고하고 개인정보 보호책임자의 승인을 받아야 한다.

제5조(내부관리계획의 공표)

1. 개인정보 보호책임자는 전조에 따라 승인한 내부관리계획을 매년 1월말까지 *[요양기관명]* 전 임직원에게 공표한다.
2. 내부관리계획은 임직원이 언제든지 열람할 수 있는 방법으로 비치하여야 하며, 변경사항이 있는 경우에는 이를 공지하여야 한다.

제3장 개인정보 보호책임자의 의무와 책임

제6조(개인정보 보호책임자의 지정)

1. *[요양기관명]은* 개인정보보호법 시행령 제32조제2항에 따라 해당하는 지위에 있는 자를 개인정보 보호책임자로 임명한다.
   가. *[요양기관명]*의 행정사무를 총괄하는 사람 *[실장 OOO]*
   나. 개인정보와 관련하여 고객의 고충처리를 담당하는 부서의 장 *[실장 OOO]*

제7조(개인정보 보호책임자의 의무와 책임)

1 개인정보 보호책임자는 정보주체의 개인정보 보호를 위하여 다음 각 호의 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

2. 개인정보 보호책임자는 업무를 수행함에 있어서 필요한 경우 개인정보 처리 현황, 처리 체계 등에 대하여 수시로 조사하거나 관련 당사자로부터 보고를 받을 수 있다.

3. 개인정보 보호책임자는 개인정보 보호와 관련하여 이법 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 하며, 필요하면 *[요양기관명] 대표원장에게* 개선조치를 보고하여야 한다.

4. 개인정보 보호책임자는 연 1회 이상 내부관리계획에 따른 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 기술적·관리적 및 물리적 안전조치의 이행 여부를 점검·관리하여야 한다.

제8조(개인정보취급자의 범위 및 의무와 책임)

1. 개인정보취급자의 범위는 다음과 같다.
   가. *[요양기관명] 내 직원 또는 위탁업무를 담당하는 직원들로서* 정보주체의 개인정보를 처리하는 업무를 수행하는 자를 말하며, 정규직 이외에 임시직, 파견근로자, 시간제근로자 등 포함될 수 있다.
   나. 개인정보취급자의 의무와 책임
   (1). 내부관리계획의 준수 및 이행
   (2). 개인정보의 기술적·관리적 보호조치 기준 이행
   (3). 업무상 알게 된 개인정보를 제3자에게 제공하지 않음

제9조(개인정보보호 전담조직 구성 및 운영)

1. 개인정보보호 활동을 수행하고 관리하는 인력들에 대한 책임, 권한 및 역할을 정의하여야 한다.

   ○ 원장: 개인정보보호 총괄 담당

   ○ 사무장: 물리적 장소(차트실, 원장실, CCTV 등)보안 담당

   ○ 실장: 컴퓨터 백신 정기점검, 비밀번호 설정 등 기술적인 보안 담당

제4장 개인정보의 기술적 · 관리적 보호조치

제10조(개인정보취급자 접근권한 관리 및 인증)

1. 개인정보처리자는 개인정보처리시스템에 대한 접근권한을 업무수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.

   [청구 S/W 접속 시, 원장 계정 및 직원의 업무에 따라 다른 권한을 주어야 함]

2. 개인정보처리자는 휴직 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여야 하며, 또한 비밀유지의무 등에 대한 보안서약서를 받아야 한다.*[병원 입사 시 보안서약서를 작성하여 보관하고 있음. 내부 직원 퇴직 시, 개인정보처리시스템(청구 S/W 등) 계정을 삭제함]*

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

4. 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자 계정을 발급하는 경우, 개인정보취급자 별로 한 개의 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다. *[계정공유 금지 및 직원별 1인 1계정 사용]*

5. 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 가상사설망 또는 전용선 등 안전한 접속수단을 적용하여야 한다.

제11조(비밀번호 관리)

1. 개인정보처리자는 개인정보취급자 또는 정보주체가 생일, 주민등록번호, 전화번호 등 추측하기 쉬운 숫자나 개인관련 정보를 패스워드로 이용하지 않도록 비밀번호 작성규칙을 수립하고, 이를 적용 및 운용하여야 한다.*[특수문자, 영문, 숫자 모두 조합하여 8자이상 적용]*

2. 개인정보처리자는 비밀번호에 적정한 기간의 유효기간*(반기별 1회 이상)*을 설정하여야 한다.

제12조(접근통제)

1. 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 시스템을 설치·운영하여야 한다.

가. 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol)주소 등으로 제한하여 인가받지 않은 접근을 제한 *[백신 및 윈도우 방화벽을 이용하여 접근통제 설정]*

나. 개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지 *[접속기록 2년 이상 보관 및 분석]*

2. 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 업무용 컴퓨터에 조치를 취하여야 한다. *[P2P 프로그램 사용 금지 및 무선 LAN(Wifi) 비밀번호 설정]*

제13조(개인정보의 암호화)

1. 개인정보처리자는 주민등록번호, 비밀번호, 바이오정보에 대해서는 안전한 암호 알고리즘으로 암호화하여 저장하여야 한다. 단, 비밀번호를 저장하는 경우에는 복호화 되지 아니하도록 일방향 암호화하여 저장하여야 한다.
2. 개인정보처리자는 정보주체의 개인정보를 정보통신망을 통하여 송·수신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.
3. 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다
4. 개인정보처리자 또는 개인정보취급자는 정보주체의 개인정보를 업무용 컴퓨터(PC)에 저장할 때에는 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화 저장하여야 한다.

제14조(접속기록의 위·변조 방지)

1. 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 최소 2년 이상 보관하여야 한다. *[개인정보처리시스템(청구 S/W, CCTV, 등 접속 로그 2년 이상 보관]*
2. 개인정보처리자는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다. *[외장하드에 데이터 백업을 받고 있음]*
3. 개인정보를 다운로드한 것이 발견되었을 경우에는 그 사유를 반드시 확인하여야 한다.

제15조(보안프로그램 설치 및 운영)

1. 개인정보처리자는 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, 또는 일 1회 이상 업데이트를 적용하여야 한다.
3. 악성 프로그램관련 경보가 발령된 경우 또는 사용 중인 응용프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 적용하여야 한다.

제16조(물리적 접근제한 및 접근통제 방법)

1. 개인정보처리자는 *원장실[CCTV보관 PC, 메인 PC], 차트실 등* 개인정보를 보관하고 있는 물리적 보관 장소에는 이에 대한 출입통제 절차*[외부인 출입 시, 출입통제 관리대장을 작성한 후 출입]*를 수립·운영하여야 한다.
2. 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.
3. 개인정보처리자는 물리적 접근방지를 위한 별도의 보호시설에 출입하거나 개인정보를 열람하는 경우, 그 출입자에 대한 출입사실 및 열람 내용에 관한 관리대장을 작성하도록 하여야 한다.

제5장 개인정보보호 교육

제17조(개인정보보호 교육 계획의 수립)

1. 개인정보 보호책임자는 다음 각 호의 사항을 포함하는 연간 개인정보보호 교육계획을 매년 12월말까지 수립한다.
   가. 교육목적 및 대상 *[전 직원을 대상으로 개인정보보호 교육]*
   나. 교육내용 *[건강보험심사평가원(biz.hira.or.kr)의 개인정보보호 동영상교육 이수 등]*
   다. 교육 일정 및 방법 *[수시로 무료 온라인 개인정보보호 교육 이수]*
2. 개인정보 보호책임자는 수립한 개인정보보호 교육 계획을 실시한 이후에 교육의 성과와 개선 필요성을 검토하여 차년도 교육계획 수립에 반영하여야 한다.

제18조(개인정보보호 교육의 실시)

1. 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.
2. 교육 방법은 집체 교육뿐만 아니라, 인터넷 교육, 그룹웨어 교육 등 다양한 방법을 활용하여 실시하고, 필요한 경우 외부 전문기관이나 전문요원에 위탁하여 교육을 실시한다.
3. 개인정보보호에 대한 중요한 전파 사례가 있거나 개인정보보호 업무와 관련하여 변경된 사항이 있는 경우, 개인정보 보호책임자는 *직원 회의* 등을 통해 수시 교육을 실시할 수 있다.

제6장 개인정보 침해대응 및 피해구제

제19조(개인정보 유출사고 대응)

1. 개인정보가 해킹, 분실, 도난 등으로 내·외부자에 의하여 유출된 경우 아래와 같이 대응한다.

단계	상세 업무	비고
사고인지 및 긴급조치	○ 개인정보 유출사고 신고 접수 및 사고인지 ○ 피해 최소화를 위한 긴급조치 수행 ※ 유출된 개인정보 삭제조치 및 기술지원 요청	
↓ 정보주체 유출통지	○ 정보주체에게 개인정보 유출사실 통지(5일이내)	
↓ 개인정보 유출신고	○ 1천명 이상의 개인정보 유출시 행정안전부 또는 한국인터넷진흥원(privacy.go.kr)에 유출신고	
↓ 민원대응반 운영	○ 개인정보 유출사고 규모 및 성격에 따라 민원대응반 구성	
↓ 고객민원 대응	○ 2차 피해 방지를 위한 고객 민원 대응 및 고객 불안 해소 조치	
↓ 피해구제 절차	○ 개인정보 유출에 대한 피해구제 절차 안내	
↓ 보안기능 강화	○ 사고 원인 분석 및 보안 강화·기능 개선	
↓ 재발방지	○ 개인정보 유출사고 사례 전파 교육 및 개선 대책 시행	

제20조(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. 개인분쟁조정위원회: (국번없이)1336 [118] http://www.1336.or.kr
   나. 정보보호마크인증위원회: 02-580-0533~4 http://www.eprivacy.or.kr
   다. 대검찰청 사이버범죄수사단: 02-3480-3571 http://www.spo.go.kr
   라. 경찰청 사이버테러대응센터: 02-1566-0112 http://www.ctrc.go.kr

분 야	3. 개인정보의 안전한 관리	
점검지표	3.2 접근권한 관리 및 접근통제	
점검항목	3.2.1 개인정보처리시스템(전자차트, 청구S/W 등)에 대한 접근권한을 최소한의 범위로 업무담당자에 따라(1인 1계정) 차등 부여하였는가?	Seq: ㉓
판단기준 (해당여부)	☑ 개인정보처리시스템*을 사용하지 않는 경우 해당 없음 - 개인정보처리시스템: 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다. (전자차트, 청구S/W, 홈페이지 등)	
점검기준	☑ 업무담당자별 1인1계정 부여 (*계정공유금지) 여부 확인 ☑ 개인정보처리시스템 업무담당자별 접근권한 관리 여부 확인	
증빙자료	※ 동 항목은 별도의 증빙자료가 없어도 점검기준을 만족하는 경우에 점검결과를 양호로 선택하실 수 있습니다.	
관련근거	「개인정보 보호법」 제29조(안전조치 의무)	
벌금과태료	3천만원 이하 과태료	
세부설명	【설명】 요양기관 담당자(개인정보처리자)는 개인정보처리시스템에 대한 접근권한을 각 업무담당자 별 **1인 1계정**을 부여하여야 함 **환자(정보주체)의 개인정보가 1만 명 이상**인 경우 요양기관 담당자(개인정보처리자)는 개인정보처리시스템에 대한 **접근권한**을 업무 수행에 필요한 최소한의 범위로 업무담당자에 따라 **차등 부여**하여야 함 【참고】 - 접근권한: 열람(read), 기록(write), 실행(execution) 등 디렉토리 및 파일에 대해 사용자가 접근 및 수행할 수 있는 작업 권한 - 접근권한 부여기준과 권한 승인절차 확인 - 업무별 권한리스트와 부여한 업무담당자의 직무 확인	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

분 야	3. 개인정보의 안전한 관리	
점검지표	3.2 접근권한 관리 및 접근통제	
점검항목	3.2.2 개인정보처리시스템(전자차트, 청구S/W 등) 접근 권한의 부여·변경·말소 내역의 기록 관리를 최소 3년간 보관하고 있는가?	Seq: ㉔
판단기준 (해당여부)	☑ 개인정보처리시스템을 사용하지 않는 경우 해당 없음	
점검기준	☑ 업무별 접근권한관리 기록 보관(3년 이상) 여부 확인	
증빙자료	업무별 권한관리 기록	
관련근거	「개인정보 보호법」 제29조(안전조치 의무)	
벌금·과태료	3천만원 이하 과태료	
세부설명	【설명】 요양기관(개인정보처리자)은 권한 부여·변경 또는 말소에 대한 내역을 기록하고, 그 기록을 **최소 3년간** 보관하여야 함 요양기관(개인정보처리자)은 전보 또는 퇴직 등 인사이동이 발생하여 직원(개인정보취급자)이 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여야 함 【참고】 전산기능이 구현되어있지 않은 경우 상기 기능에 대해서 수탁업체에 기능개발 요청	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

(사용자 ID 관리대장 예시)

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*	*부서변경*	*○○○○ (○○○)*
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 수정 가능함

분 야	3. 개인정보의 안전한 관리	
점검지표	3.2 접근권한 관리 및 접근통제	
점검항목	3.2.3 안전한 비밀번호 작성규칙을 적용하고 있는가?	Seq: ㉕
판단기준 (해당여부)	☑ 업무용 PC, 모바일기기(스마트패드, 스마트폰 등)가 없는 경우 해당 없음	
점검기준	☑ 안전한 비밀번호 작성규칙(PC, 개인정보처리시스템 등) 준수 여부 확인	
증빙자료	※ 동 항목은 별도의 증빙자료가 없어도 점검기준을 준수하는 경우에 점검결과를 양호로 선택하실 수 있습니다.	
관련근거	「개인정보 보호법」 제29조(안전조치 의무)	
벌금과태료	3천만원 이하 과태료	
세부설명	【설명】 요양기관(개인정보처리자)은 직원(개인정보취급자) 또는 환자(정보주체)가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 함 【참고】 안전한 비밀번호 작성규칙 ① 비밀번호 최소길이 - 3가지 이상(영문 대·소문자, 숫자, 특수문자 등) 조합인 경우 8자리 - 2가지(영문 대·소문자, 숫자, 특수문자 등) 조합인 경우 10자리 ② 추측하기 어려운 비밀번호 사용 - 일련번호, 전화번호 등 쉬운 문자열이 포함되지 않도록 함 - 잘 알려진 단어, 키보드 상에 나란히 있는 문자열이 포함되지 않도록 함 - 사용자 ID와 동일한 비밀번호는 사용하지 않도록 함 ③ 비밀번호의 주기적인 변경 - 비밀번호는 최소 6개월마다 변경하여 동일한 비밀번호를 장기간 이용하지 않도록 관리 ④ 동일 비밀번호 사용 제한 - 2개의 비밀번호를 교대로 사용하지 않도록 함 ⑤ 비밀번호 설정·변경 시 자리수와 조합을 체크하여 비밀번호 작성규칙에 위배되는 경우, 법 위반을 알리고 작성규칙을 준수토록 함 - 고객 불만 등으로 그 적용이 어려운 경우에는 최소한 법 위반 경고창을 통해 '비밀번호 작성규칙'을 준수하도록 유도함 ※ 업무용 모바일 기기의 분실.도난 등으로 개인정보가 유출되지 않도록 비밀번호, 패턴, PIN 등 보호조치를 하여야 함	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

분 야	3. 개인정보의 안전한 관리	
점검지표	3.2 접근권한 관리 및 접근통제	
점검항목	3.2.4 개인정보처리시스템(전자차트, 청구S/W 등)에 대하여 불법적인 접근 및 침해사고를 방지하기 위한 접근통제시스템을 설치/운영하고 있는가?	Seq: ㉖
판단기준 (해당여부)	☑ 개인정보처리시스템을 사용하지 않는 경우 해당 없음	
점검기준	☑ (업무용 PC) 백신, 방화벽 기능을 가진 SW 설치 및 점검 여부 확인 ☑ (서버급 이상) 접근통제 관련 HW 및 SW 설치 및 운영 여부 확인	
증빙자료	※ 동 항목은 별도의 증빙자료가 없어도 점검기준을 준수하는 경우에 점검결과를 양호로 선택하실 수 있습니다.	
관련근거	「개인정보 보호법」 제29조(안전조치 의무)	
벌금과태료	3천만원 이하 과태료	
세부설명	【설명】 불법적인 접근 및 침해사고 방지를 위해 아래와 같은 방법을 하나 이상 적용 - 컴퓨터의 운영체제(윈도우 등)의 기본 기능을 이용하여 방화벽 운영 ※ 윈도우의 [설정] - [제어판] - [Windows방화벽]에서 '사용'을 클릭 - 보안프로그램(백신)의 방화벽 기능을 이용 - 보안업체 등에서 제공하는 보안 서비스(침입방지시스템 등)를 활용하여 방화벽 설치 【참고】 **접근통제시스템이란?** 정보통신망을 통한 개인정보처리시스템의 불법적 접근 및 침해사고 방지를 위해 비인가자의 접근을 차단할 수 있는 보안시스템을 말함 1) 침입차단시스템(Firewall) - 비인가 IP, port 차단 2) 침입방지시스템(IPS) - 시스템에서 지원하는 취약점 패턴에 대해서만 탐지 차단	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

분 야	3. 개인정보의 안전한 관리	
점검지표	3.2 접근권한 관리 및 접근통제	
점검항목	3.2.5 외부에서 정보통신망을 통한 접속 시 가상 사설망, 전용선 등 안전한 접속수단 혹은 안전한 인증수단을 제공하고 있는가?	Seq: ㉗
판단기준 (해당여부)	☑ 외부망과 연결되지 않은 서버만 운용 또는 서버 미운용 시 해당 없음	
점검기준	☑ 가상사설망(VPN: Virtual Private Network), 전용선 등의 안전한 접속수단 제공	
증빙자료	※ 동 항목은 별도의 증빙자료가 없어도 점검기준을 준수하는 경우에 점검결과를 양호로 선택하실 수 있습니다.	
관련근거	「개인정보 보호법」 제29조(안전조치 의무)	
벌금과태료	3천만원 이하 과태료	
세부설명	【설명】 외부망으로부터 개인정보처리시스템에 대한 접속은 **원칙적으로 차단**하여야 함. 다만 요양기관 직원(개인정보취급자)이 외부망을 통해 개인정보처리시스템에 접속이 필요한 경우에는 **가상사설망(VPN: Virtual Private Network)또는 전용선** 등의 안전한 접속수단을 적용하거나 안전한 **인증수단**(공인인증서, 일회용 비밀번호(OTP), 보안토큰 등)을 적용해야 함 【참고】 외부와 접속가능한 통신망 확인 후 VPN 또는 전용선 사용여부 확인 혹은 안전한 인증수단 사용여부 확인 - 가상사설망(VPN: Virtual Private Network)은 요양기관 담당자(개인정보처리자)가 기관 내의 개인정보처리시스템에 대해 원격으로 접속할 때 IPsec이나 SSL기반의 암호프로토콜을 사용한 터널링 기술을 통해 안전한 암호통신을 할 수 있도록 해주는 보안시스템을 의미한다. ※ 외부망과 연결된 서버 운용 시 전용선, VPN 외 IP, MAC, 공인인증서 등을 통해서 접속을 제한하여 처리가능	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

분 야	3. 개인정보의 안전한 관리	
점검지표	3.2 접근권한 관리 및 접근통제	
점검항목	3.2.6 P2P(peer to peer), 웹하드 등 비 인가프로그램의 접속을 차단하고 있는가?	Seq: ㉘
판단기준 (해당여부)	☑ PC가 없는 경우 해당 없음	
점검기준	(업무용 PC) ☑ 공유폴더 제거 및 비인가 프로그램 접속 차단여부 확인 (서버급 이상) ☑ 침입차단 시스템의 설치 및 운영여부 확인 ☑ 공유폴더 제거 여부 확인	
증빙자료	※ 동 항목은 별도의 증빙자료가 없어도 점검기준을 준수하는 경우에 점검결과를 양호로 선택하실 수 있습니다.	
관련근거	「개인정보 보호법」 제29조(안전조치 의무)	
벌금과태료	3천만원 이하 과태료	
세부설명	【설명】 요양기관 담당자(개인정보처리자)는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망(Wifi) 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리 시스템, 업무용 컴퓨터 및 모바일 기기 등에 조치를 하여야 함 - 기업용 백신SW 등 프로그램을 이용하여 접속 차단 가능함 ※ 방화벽(V3) 또는 브라우저(IE)등을 통해 유해 사이트 차단 가능 **- 차단이 힘든 경우 해당 비인가 프로그램을 삭제 조치하고 다시 설치되지 않도록 관리해야 함** - 윈도우계열 OS의 경우 "시작>제어판>성능 및 유지관리>관리도구>컴퓨터관리"에서 공유폴더가 있는지 확인 가능 ※ 공유폴더를 이용하여 업무를 진행해야 되는 경우, 공유폴더에 암호 설정 및 사용 후 공유폴더를 해제해야 함 - 공유기를 이용한 무선망을 사용하는 경우 안전한 비밀번호 적용 【참고】 **공개된 무선망(Wifi):** 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망 **P2P(peer to peer):** 인터넷으로 다른 사용자의 컴퓨터에 접속하여 각종 정보나 파일을 교환·공유 할 수 있게 해주는 서비스 **웹하드:** 개인이 기업형 웹하드 사이트 서버에 자료를 저장해두고 웹하드 업체는 돈을 받고 이 자료를 실시간으로 초고속 다운로드를 해주는 서비스	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

분 야	3. 개인정보의 안전한 관리	
점검지표	3.2 접근권한 관리 및 접근통제	
점검항목	3.2.7 인터넷 홈페이지의 개인정보 노출 방지를 위한 보안 조치를 실시하고 있는가?	Seq: ㉙
판단기준 (해당여부)	☑ 홈페이지를 보유하지 않은 기관은 해당사항 없음	
점검기준	☑ 홈페이지 개인정보 노출방지 점검 및 보완조치 여부 확인 ☑ 홈페이지 웹 취약점 점검 여부 확인	
증빙자료	홈페이지 개인정보 노출방지 점검, 웹 취약점 점검 수행 결과	
관련근거	「개인정보 보호법」 제29조(안전조치 의무)	
벌금과태료	3천만원 이하 과태료	
세부설명	【설명】 요양기관담당자(개인정보처리자)는 인터넷 홈페이지를 통해 개인정보가 유출되지 않도록 **연 1회 이상 홈페이지를 점검하는 것을 권장함** - 홈페이지 개인정보 노출 진단 모니터링 방법 **인터넷 홈페이지에서 고유식별정보**(주민등록번호, 여권번호, 운전면허번호, 외국인등록번호)**를 처리하고 환자(정보주체)의 개인정보가 1만 명 이상인** 경우, 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 **연 1회 이상 취약점을 점검하여야 함** - KISA 보호나라(www.boho.or.kr) 홈페이지를 통해 웹 취약점을 점검 가능	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

분 야	3. 개인정보의 안전한 관리	
점검지표	3.2 접근권한 관리 및 접근통제	
점검항목	3.2.8 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 접근을 제한하고 있는가?	Seq: ㉚
판단기준 (해당여부)	☑ 총 1만 명 미만의 환자(정보주체) 개인정보를 보유한 소상공인(상시근로자 수 5인 미만)의 경우 해당 없음	
점검기준	☑ 개인정보처리시스템(전자차트, 청구 S/W, 홈페이지 등)에 접속하는 계정 정보 또는 비밀번호를 일정 횟수 이상 잘못 입력 시 접근 제한 여부 확인	
증빙자료	※ 동 항목은 별도의 증빙자료가 없어도 점검기준을 준수하는 경우에 점검결과를 양호로 선택하실 수 있습니다.	
관련근거	「개인정보 보호법」 제29조(안전조치 의무)	
벌금과태료	3천만원 이하 과태료	
세부설명	【설명】 요양기관(개인정보처리자)은 개인정보처리시스템(전자차트, 청구 S/W, 홈페이지 등)에 권한 없는 자의 비정상적인 접근을 방지하기 위하여 계정 정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우에는 개인정보처리시스템에 접근을 제한하는 등 기술적 조치를 하여야 함 【참고】 비밀번호를 일정 횟수(예시: 5회) 잘못 입력한 경우 계정 잠금, 계정 해제 시 추가적인 인증수단(공인인증서, OTP 등)을 통하여 사용자 확인 후 계정 잠금 해제 등	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

분 야	3. 개인정보의 안전한 관리	
점검지표	3.2 접근권한 관리 및 접근통제	
점검항목	3.2.9 일정시간 이상 업무처리를 하지 않을 시 자동으로 시스템 접속이 차단되도록 하고 있는가?	Seq: ㉛
판단기준 (해당여부)	☑ 총 1만 명 미만의 환자(정보주체) 개인정보를 보유한 소상공인(상시근로자 수 5인 미만)의 경우 해당 없음	
점검기준	☑ 개인정보처리시스템(전자차트, 청구 S/W, 홈페이지 등)에서 일정시간 이상 업무처리를 하지 않을 시 자동으로 시스템 접속 차단 여부 확인	
증빙자료	※ 동 항목은 별도의 증빙자료가 없어도 점검기준을 준수하는 경우에 점검결과를 양호로 선택하실 수 있습니다.	
관련근거	「개인정보 보호법」 제29조(안전조치 의무)	
벌금과태료	3천만원 이하 과태료	
세부설명	【설명】 요양기관(개인정보처리자)은 개인정보가 권한이 없는 자에게 공개되거나 유출이 되지 않도록 일정시간 이상 개인정보처리시스템(전자차트, 청구 S/W, 홈페이지 등)에 업무처리를 하지 않는 경우에는 **자동으로 시스템 접속이 차단**되도록 하여야 함 예시) 개인정보처리시스템에 접속한 상태로 30분 이상 업무처리를 하지 않는 경우, 자동으로 로그아웃 됨 【참고】 개인정보처리시스템에 접속하는 업무용 컴퓨터 등에서 해당 개인정보처리시스템에 대한 접속의 차단을 의미, **업무용 컴퓨터의 화면보호기 등은 접속차단에 해당하지 않음** 일정시간 이상 업무처리를 하지 않아 개인정보처리시스템에 접속이 차단된 이후, **다시 접속하고자 할 때에도 최초의 로그인과 동일한 방법으로 접속하여야 함**	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

분 야	3. 개인정보의 안전한 관리	
점검지표	3.3 개인정보 암호화	
점검항목	3.3.1 고유식별정보, 비밀번호 및 바이오정보를 개인정보처리시스템(전자차트, 홈페이지, 청구S/W 등)에 저장 시 암호화 하고 있는가?	Seq: ㉜
판단기준 (해당여부)	☑ 개인정보처리시스템을 사용하지 않는 경우 해당 없음	
점검기준	☑ 개인정보처리시스템(전자차트, 홈페이지, 청구S/W 등)에 저장된 고유식별정보, 비밀번호 및 바이오정보의 암호화 적용여부 확인	
증빙자료	※ 동 항목은 별도의 증빙자료가 없어도 점검기준을 준수하는 경우에 점검결과를 양호로 선택하실 수 있습니다.	
관련근거	「개인정보 보호법」 제29조(안전조치 의무)	
벌금과태료	3천만원 이하 과태료	
세부설명	【설명】 고유식별정보, 비밀번호 및 바이오정보를 개인정보처리시스템(전자차트, 홈페이지, 청구S/W 등)에 저장 시 암호화 조치를 취해야 함 - 비밀번호는 일방향암호화* 하여야 함 * 일방향암호화: 저장된 값으로 원본값을 유추하거나 복호화 할 수 없도록 암호화 한 방법 - 바이오정보는 식별 및 인증 등의 고유기능으로 사용하는 경우에만 암호화 대상임(CT영상 등 의료행위 관련 바이오정보는 제외) 【참고】 건강보험심사평가원 제공 무료 암호화 모듈 활용 - 건강보험심사평가원에서는 요양기관이 보유한 진료정보를 보호하기 위해 암호화 모듈을 무료로 제공하고 있으며, 이를 통해 기술지원 및 개발비용 절감, 「개인정보 보호법」 준수 등의 효과를 도모 함	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

분 야	3. 개인정보의 안전한 관리	
점검지표	3.3 개인정보 암호화	
점검항목	3.3.2 고유식별정보, 비밀번호 및 바이오정보를 컴퓨터(업무용 PC) 및 모바일기기에 저장 시 암호화하고 있는가?	Seq: ㉝
판단기준 (해당여부)	☑ 업무용 PC가 없는 경우 해당 없음	
점검기준	☑ 업무용 PC 및 모바일기기에 저장된 고유식별정보, 비밀번호 및 바이오정보의 암호화 여부 확인	
증빙자료	※ 동 항목은 별도의 증빙자료가 없어도 점검기준을 준수하는 경우에 점검결과를 양호로 선택하실 수 있습니다.	
관련근거	「개인정보 보호법」 29조(안전조치 의무)	
벌금과태료	3천만원 이하 과태료	
세부설명	【설명】 업무용 컴퓨터 또는 모바일 기기에 고유식별정보, 비밀번호 및 바이오정보를 저장하여 관리하는 경우 안전한 암호화 알고리즘이 적용된 암호화 소프트웨어를 사용하여 암호화한 후에 저장하여야 함 - 업무용 PC 및 모바일기기에 문서파일(hwp, xls, txt 등) 형태로 고유식별정보, 비밀번호 및 바이오정보를 보관 시 아래와 같은 방법으로 암호화 할 수 있음 ▪ 문서편집기(한글, MS-Office 등)에서 제공하는 비밀번호 설정 기능 이용 ▪ 압축프로그램을 이용한 파일 압축 및 비밀번호 설정 ※ 비밀번호 설정 시 단순 숫자 또는 문자열 사용 금지 (3.2.3 항목의 안전한 비밀번호 작성규칙 준수 권장)	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

분 야	3. 개인정보의 안전한 관리	
점검지표	3.3 개인정보 암호화	
점검항목	3.3.3 고유식별정보, 비밀번호 및 바이오정보를 정보통신망을 통하여 송·수신하거나 보조저장매체를 통하여 전달 시 암호화하고 있는가?	Seq: ㉞
판단기준 (해당여부)	☑ 업무용 PC가 없는 경우 해당 없음	
점검기준	☑ 고유식별정보, 비밀번호 및 바이오정보를 정보통신망(이메일, 메신저 등)을 통하여 송·수신하거나 보조저장매체 등을 통해 전달하는 경우 이를 암호화하는지 여부 확인	
증빙자료	※ 동 항목은 별도의 증빙자료가 없어도 점검기준을 준수하는 경우에 점검결과를 양호로 선택하실 수 있습니다.	
관련근거	「개인정보 보호법」 제29조(안전조치 의무)	
벌금·과태료	3천만원 이하 과태료	
세부설명	【설명】 고유식별정보, 비밀번호 및 바이오정보를 정보통신망을 통하여 송·수신하거나 보조저장매체 등을 통해 전달하는 경우 암호화 하여야 함 예시) 요양기관이 급여비용 청구를 위해 건강보험심사평가원 진료비 청구포털시스템을 이용하는 경우 암호화 및 안전한 송·수신 기능 제공 개인정보가 포함된 문서파일(hwp, xls, txt 등)은 문서편집기 및 압축프로그램에서 제공하는 비밀번호 설정 기능을 통하여 암호화 후 송·수신 가능함 ※ 비밀번호 설정 시 단순 숫자 또는 문자열 사용 금지 (3.2.3 항목의 안전한 비밀번호 작성규칙 준수 권장) 홈페이지에서 개인정보를 수집하는 기관의 경우 SSL/TLS 등의 통신 암호화를 적용하여야 함 ☞ wire shark 프로그램을 통해 전송되는 패킷의 암호화 검사 시 암호화 하지 않은 사례 있음	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

<table>
<tr><td>분 야</td><td colspan="2">3. 개인정보의 안전한 관리</td></tr>
<tr><td>점검지표</td><td colspan="2">3.3 개인정보 암호화</td></tr>
<tr><td>점검항목</td><td>3.3.4 고유식별정보, 비밀번호 및 바이오정보를 암호화하여 저장 시 안전한 암호 알고리즘 사용을 하였는가?</td><td>Seq: ㉟</td></tr>
<tr><td>판단기준
(해당여부)</td><td colspan="2">☑ 개인정보처리시스템이 없는 경우 해당 없음</td></tr>
<tr><td>점검기준</td><td colspan="2">☑ 암호화 시 안전한 암호 알고리즘을 사용 여부 확인</td></tr>
<tr><td>증빙자료</td><td colspan="2">※ 동 항목은 별도의 증빙자료가 없어도 점검기준을 준수하는 경우에 점검결과를 양호로 선택하실 수 있습니다.</td></tr>
<tr><td>관련근거</td><td colspan="2">「개인정보 보호법」 제29조(안전조치 의무)</td></tr>
<tr><td>벌금과태료</td><td colspan="2">3천만원 이하 과태료</td></tr>
<tr><td>세부설명</td><td colspan="2">【설명】 개인정보처리시스템에 고유식별정보, 비밀번호, 바이오정보를 암호화하여 저장 시, 안전한 암호알고리즘을 사용해야함

【참고】 안전한 암호알고리즘, 암호화 방식 등은 "개인정보 암호화 조치 안내서" 참조
※ 개인정보보호 종합지원포털(http://www.privacy.go.kr)에서 다운로드 가능

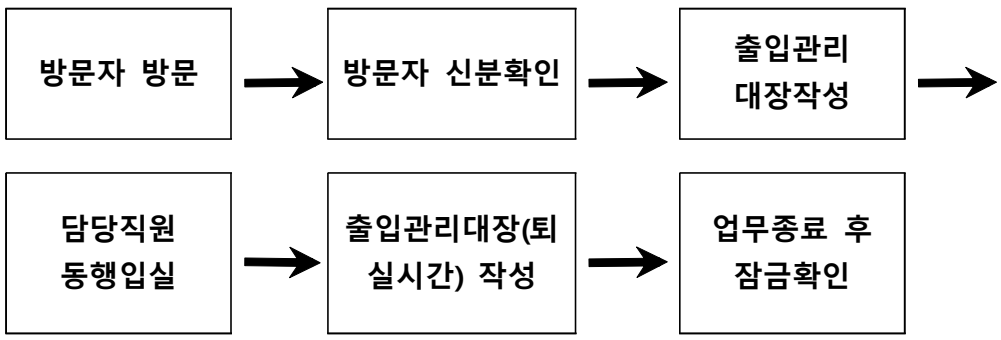
※ 안전한 암호알고리즘을 사용하더라도 암호화 키가 잘못 관리되어 유·노출 되는 경우에는 암호화된 정보들이 유·노출될 수 있으므로 이를 안전하게 관리하여야 함
<table>
<tr><th>구분</th><th>공공기관</th><th>민간 부문
(법인·단체·개인)</th></tr>
<tr><td>대칭키 암호 알고리즘</td><td>SEED, LEA, HIGHT, ARIA-128/192/256</td><td>ARIA-128/192/256, SEED AES-128/192/256, Blowfish, Camellia-128/192/256, MISTYI, KASUMI, 등</td></tr>
<tr><td>공개키 암호 알고리즘</td><td>RSAES-OAEP</td><td>RSA, RSAES-OAEP, RSAES-PKCSI 등</td></tr>
<tr><td>일방향 암호 알고리즘</td><td>SHA-224/256/384/512</td><td>SHA-224/256/384/512 Whirlpool 등</td></tr>
</table>
☞ 안전하지 않은 알고리즘(MD5, SHA-1, 자체 함수제작 등) 및 양방향 암호화 방식으로 암호화한 사례 있음</td></tr>
<tr><td>점검결과</td><td colspan="2">✓ (양 호) 점검기준 준수
✓ (개선필요) 점검기준 일부 준수
✓ (취 약) 점검기준 미준수
✓ (해당없음) 판단 기준에 따라 해당사항이 없는 경우</td></tr>
</table>

분 야	3. 개인정보의 안전한 관리	
점검지표	3.3 개인정보 암호화	
점검항목	3.3.5 고유식별정보를 인터넷과 내부망의 중간지점(DMZ)에 저장 시 암호화하고 있는가?	Seq: ㊱
판단기준 (해당여부)	☑ 업무용 PC가 없는 경우 해당 없음	
점검기준	☑ 고유식별정보를 인터넷 구간 및 인터넷 구간과 내부망의 중간지점(DMZ)에 저장하는 경우 암호화하여 저장하는지 확인	
증빙자료	※ 동 항목은 별도의 증빙자료가 없어도 점검기준을 준수하는 경우에 점검결과를 양호로 선택하실 수 있습니다	
관련근거	「개인정보 보호법」 제29조(안전조치 의무)	
벌금과태료	3천만원 이하 과태료	
세부설명	【설명】 고유식별정보를 인터넷에 접근가능한 PC혹은 서버에 저장하는 경우(인터넷 구간 및 인터넷 구간과 내부망의 중간지점(DMZ)에 저장하는 경우) 암호화 하여 저장하는지 확인 【참고】 **DMZ**: 내부망과 인터넷 구간 사이에 위치한 중간 지점으로 침입차단시스템 등으로 접근제한 등을 수행하지만, 외부망에서 직접 접근이 가능한 영역을 말함 **내부망**: 물리적 망분리, 접근통제시스템 등에 의해 인터넷 구간에서 접근이 통제 또는 차단되는 구간을 말함	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

분 야	3. 개인정보의 안전한 관리	
점검지표	3.4 접속기록 보관	
점검항목	3.4.1 개인정보취급자의 접속기록을 최소 2년 이상 보관하여 관리하고 있는가?	Seq: ㊲
판단기준 (해당여부)	☑ 개인정보처리시스템이 없는 경우 해당 없음	
점검기준	☑ 개인정보취급자의 접속기록을 최소 2년 이상 보관 및 관리여부 확인	
증빙자료	※ 동 항목은 별도의 증빙자료가 없어도 점검기준을 준수하는 경우에 점검결과를 양호로 선택하실 수 있습니다.	
관련근거	「개인정보 보호법」 제29조(안전조치 의무)	
벌금·과태료	3천만원 이하 과태료	
세부설명	【설명】 개인정보처리시스템(전자차트, 청구S/W 등)에 접속한 기록이 위·변조 및 도난, 분실되지 않도록 접속기록*을 **최소 2년 이상 보관·관리**하여야 함 * 접속기록: 개인정보취급자등이 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 개인정보취급자 등의 계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 전자적으로 기록한 것을 말함 개인정보처리시스템을 위탁·운영하는 경우 수탁업체에 2년 이상 접속기록 보관 여부를 확인하여야 함 ※ 해당 기능이 불가능한 개인정보처리시스템인 경우, 수탁업체에 기능 추가를 요청하여야 함 요양기관 담당자(개인정보처리자)는 개인정보의 유출·변조·훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 **1회 이상 점검**하여야 함 이와 함께, 개인정보를 다운로드한 것이 발견되었을 경우에는 내부관리 계획으로 정하는 바에 따라 그 사유를 반드시 확인 ※ **접속기록의 필수 항목(5개)**: ID, 일자 및 시간, 접속자 IP주소, 처리한 정보주체 정보(개인정보취급자가 누구의 개인정보를 처리하였는지를 알 수 있는 성명, ID 등), 수행업무(열람, 수정, 삭제, 인쇄, 입력 등)	
	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

분 야	3. 개인정보의 안전한 관리	
점검지표	3.4 접속기록 보관	
점검항목	3.4.2 접속기록의 위·변조 및 도난, 분실되지 않도록 접속 기록을 안전하게 보관하고 있는가?	Seq: ㊳
판단기준 (해당여부)	☑ 개인정보처리시스템이 없는 경우 해당 없음	
점검기준	☑ 개인정보처리시스템(전자차트, 청구S/W 등)에 접속한 기록을 위·변조 및 도난, 분실되지 않도록 안전하게 보관하는지 여부	
증빙자료	※ 동 항목은 별도의 증빙자료가 없어도 점검기준을 준수하는 경우에 점검결과를 양호로 선택하실 수 있습니다.	
관련근거	「개인정보 보호법」 제29조(안전조치 의무)	
벌금·과태료	3천만원 이하 과태료	
세부설명	【설명】 대표자(원장, 약국장)은 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 함 【참고】 1. 접속기록 위·변조 방지 방법 - 접속기록을 백업하여 개인정보처리시스템 이외의 별도의 저장매체(USB, 외장하드, CD, DVD 등)에 보관 예시) 개인정보처리시스템(전자 차트, 청구 S/W 등)의 데이터 및 접속기록을 일괄 백업하여 보조저장매체(USB, 외장하드 등)에 보관 2. 접속기록을 안전하게 보관하는 방법 - 별도 지정된 장소(통제구역), 금고 또는 잠금 장치가 있는 캐비넷(보관함) 등에 보관	
	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

분 야	3. 개인정보의 안전한 관리	
점검지표	3.5 보안프로그램 설치운영	
점검항목	3.5.1 개인정보처리시스템이 설치된 업무용 PC에 백신 프로그램 등의 보안 프로그램의 설치 및 업데이트, 악성프로그램 삭제 등 지속적으로 관리하고 있는가?	Seq: ㊴
판단기준 (해당여부)	☑ PC를 보유하지 않는 경우 해당 없음	
점검기준	☑ 최신 보안 프로그램 설치 여부 확인 - 자동업데이트 혹은 일 1회 이상의 업데이트 실시 ☑ 발견된 악성프로그램 등에 대한 대응 조치여부 확인	
증빙자료	※ 동 항목은 별도의 증빙자료가 없어도 점검기준을 준수하는 경우에 점검결과를 양호로 선택하실 수 있습니다.	
관련근거	「개인정보 보호법」 제29조(안전조치 의무)	
벌금과태료	3천만원 이하 과태료	
세부설명	【설명】 요양기관(개인정보처리자)은 악성프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 함 - 업무용 PC에는 개인용 백신S/W가 아닌 기업용 백신S/W를 사용하여야 함 - 기업용 백신S/W가 없는 경우, 건강보험심사평가원 제공 DUR 모듈에 포함된 백신S/W(AhnLab Online Security)를 사용 가능 - 백신S/W는 항상 활성화 시켜두고, 월 1회 이상 정기적으로 검사하는 것을 권장 보안 프로그램의 자동 업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지하여야 함 - 보안 프로그램 등을 통하여 발견된 바이러스, 트로이목마 등의 악성프로그램 등에 대해 삭제, 치료 등의 대응 조치를 취하여야 함 사용 중인 응용 프로그램(한컴 오피스, MS 오피스 등)이나 운영체제 소프트웨어(Windows 7, 10 등)의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시하여야 함	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

분 야	3. 개인정보의 안전한 관리	
점검지표	3.6 물리적 접근방지	
점검항목	3.6.1 전산실, 자료보관실 등 물리적 보관 장소에 대한 출입 통제절차를 수립하여 운영하고 있는가?	Seq: ㊵
판단기준 (해당여부)	☑ 별도의 물리적 보관 장소를 가지고 있지 않은 경우 해당 없음	
점검기준	☑ 물리적 보관장소에 대한 출입통제 절차 수립 여부 확인 ☑ 출입관리 대장을 작성·관리여부 확인	
증빙자료	전산실·자료보관실 출입통제 절차(절차가 반영된 규정, 계획), 출입통제 관리대장	
관련근거	「개인정보 보호법」 제29조(안전조치 의무)	
벌금·과태료	3천만원 이하 과태료	
세부설명	【설명】 요양기관(개인정보처리자)은 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 함 **※ 출입통제절차 예시**  【참고】 출입 통제방법 - 통제구역 설정, 통제구역 잠금장치 및 지정된 자만 출입, 출입자 명부 작성 등	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

(출입통제 절차 수립 예시)

3.6.1

방문자 신분확인

⬇

출입관리대장 작성
(방문자명 및 소속, 입실시간, 방문목적)

⬇

담당직원 동행 입실

⬇

출입관리대장 작성
(퇴실시간)

⬇

업무종료 후 잠금 확인

(출입관리대장 예시)

3.6.1

출 입 관 리 대 장(예시)

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

※ 위의 서식을 참고하여 요양기관의 환경에 맞게 수정 가능함

분 야	3. 개인정보의 안전한 관리	
점검지표	3.6 물리적 접근방지	
점검항목	3.6.2 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하고 있는가?	Seq: ㊶
판단기준 (해당여부)	☑ 필수사항	
점검기준	☑ 개인정보가 포함된 서류, 보조저장매체를 별도 지정된 통제구역, 금고, 잠금장치가 있는 보관함에 보관 여부 확인	
증빙자료	※ 동 항목은 별도의 증빙자료가 없어도 점검기준을 준수하는 경우에 점검결과를 양호로 선택하실 수 있습니다.	
관련근거	「개인정보 보호법」 제29조(안전조치 의무)	
벌금과태료	3천만원 이하 과태료	
세부설명	【설명】 요양기관(개인정보처리자)은 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 함 - 개인정보가 포함된 서류, 보조저장매체 등의 보관 시, 별도 보관 장소가 없는 경우나 임시로 보관이 필요한 경우에는 잠금장치가 있는 보관시설(캐비닛, 금고 등)에 보관하여야 함 ☞ 개인정보가 포함된 서류(진료기록부, 처방전 등)을 안전한 장소에 보관하지 않고 책상 등 공개된 장소에 방치하는 사례 있음	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

분 야	3. 개인정보의 안전한 관리	
점검지표	3.7 개인정보 처리방침의 수립 및 공개	
점검항목	3.7.1 개인정보 처리방침을 수립하고 있는가?	Seq: ㊷
판단기준 (해당여부)	☑ 필수사항	
점검기준	☑ 필수항목(8개)을 포함한 개인정보 처리방침 수립 여부	
증빙자료	개인정보 처리방침	
관련근거	「개인정보 보호법」 제30조(개인정보 처리방침의 수립 및 공개)	
벌금과태료	1천만원 이하 과태료	
세부설명	【설명】 다음 각 호의 사항이 포함된 개인정보 처리방침을 정하여야 함 (필수 8항목) ① 개인정보의 처리목적 ② 개인정보의 처리 및 보유기간 ③ 개인정보의 제3자 제공에 관한사항(해당되는 경우에만 정한다) ④ 개인정보처리의 위탁에 관한사항(해당되는 경우에만 정한다) ⑤ 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한사항 ⑥ 처리하는 개인정보의 항목 ⑦ 개인정보의 파기에 관한사항 ⑧ 개인정보 보호책임자에 관한사항 ⑨ 개인정보 처리방침의 변경에 관한 사항 ⑩ 시행령 제30조제1항에 따른 개인정보의 안전성 확보조치에 관한 사항 【참고】 개인정보보호 종합포털(www.privacy.go.kr)의 '개인정보 처리방침 만들기' 활용방법 참고	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

(개인정보 처리방침 예시)

3.7.1

【 개인정보 처리방침 】

OO요양기관은(**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 알려드립니다.

이 개인정보 처리방침의 순서는 다음과 같습니다.

1. 수집하는 개인정보의 항목 및 수집방법

A는 *OO(업무내용)*를 위해 필요한 *OO(처방전, 진료정보 등)*과 건강보험급여 청구에 필요한 최소한의 개인정보만을 수집합니다.

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

2. 개인정보의 수집 및 이용목적

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

3. 개인정보의 보유 및 이용기간 및 파기절차 및 파기방법

의료법, 약사법, 건강보험법에서 정한 보유기간 동안 개인정보를 보유하며 그 이후는 지체 없이 파기합니다.

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

4. 이용자 및 법정대리인의 권리와 그 행사방법

이용자 및 법정대리인은 개인정보와 관련하여 인터넷, 전화, 서면 등을 이용하여 *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.

5. 개인정보의 제3자 제공

*A*는 건강보험심사평가원에 요양급여비용 청구를 위해 진료기록을 제출합니다.

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

6. 개인정보 처리의 위탁

개인정보를 정보시스템을 통해 관리하기 위해 다음의 회사에 개인정보를 위탁하고 있습니다.

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

- 폐기: 업체명(연락처) 기입

- CCTV: 업체명(연락처) 기입

7. 개인정보 보호책임자

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

8. 개인정보의 안전성 확보조치

*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 사용자 비밀번호를 정기적으로 갱신하여 안전하게 관리합니다.

9. 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.

공고일자: 20XX년 XX월 XX일

시행일자: 20XX년 XX월 XX일

<참고> 제정일자/공고일자/시행일자: 2012년 3월 30일 이후 일자로 기입

※ 본 서식은 요양기관의 업무현황에 맞게 수정하여 사용할 수 있음

분 야	3. 개인정보의 안전한 관리	
점검지표	3.7 개인정보 처리방침의 수립 및 공개	
점검항목	3.7.2 개인정보 처리방침을 홈페이지 또는 보기 쉬운 장소(접수대, 대기실 등)에 공개하고 있는가?	Seq: ㊸
판단기준 (해당여부)	☑ 필수 사항	
점검기준	☑ 개인정보 처리방침 공개여부 확인	
증빙자료	개인정보 처리방침 공개 사실을 확인할 수 있는 자료	
관련근거	「개인정보 보호법」 제30조(개인정보 처리방침의 수립 및 공개)	
벌금과태료	1천만원 이하 과태료	
세부설명	【설명】 개인정보 처리방침은 인터넷 홈페이지, 대기실 등을 통하여 환자(정보주체)가 언제든지 쉽게 확인할 수 있도록 공개하여야 함 개인정보 처리방침을 변경하는 경우에는 변경 및 시행시기, 변경된 내용을 인터넷 홈페이지 등을 통해 지속적으로 공개하여야 하며, 변경된 내용은 정보주체가 쉽게 확인할 수 있도록 변경 전·후를 비교하여 공개하여야 함 【참고】 홈페이지에 공개할 경우에는 "개인정보 처리방침"이라는 명칭을 사용하되, 글자 크기나 색상 등을 활용하여 다른 고지사항과 구분함으로써 정보주체가 쉽게 확인할 수 있도록 하여야 함	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

분 야	3. 개인정보의 안전한 관리	
점검지표	3.8 개인정보 보호책임자의 지정	
점검항목	3.8.1 개인정보 보호책임자가 지정되고 그 역할이 정의되어 있는가?	Seq: ㊹
판단기준 (해당여부)	☑ 필수 사항	
점검기준	☑ 개인정보 보호책임자가 자격요건에 맞게 문서로 지정되었는지 여부	
증빙자료	개인정보 보호책임자 지정 및 역할 확인이 가능한 문서(다음 중 택일 하여 증빙) - 내부관리계획, 업무 분장표, 직제표, 개인정보 처리방침 등	
관련근거	「개인정보 보호법」 제31조(개인정보 보호책임자의 지정)	
벌금과태료	1천만원 이하 과태료	
세부설명	【설명】 대표자(원장·약국장)은 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 지정하여야 함 또한, 적절한 책임·권한·역할을 아래와 같은 **문서를 통하여 정의**하여야 함 - 내부관리계획, 업무 분장표, 직제표, 개인정보 처리방침 등 ❍ **개인정보 보호책임자의 지정요건** 가. 사업주 또는 대표자 나. 정보주체의 개인정보 보호업무를 위해 조직된 부서의 장 또는 개인정보보호에 관한 소양이 있는 사람 ❍ **개인정보 보호책임자는 다음 각 호의 업무를 수행함** ① 개인정보보호 계획의 수립 및 시행 ② 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선 ③ 개인정보 처리와 관련한 불만의 처리 및 피해구제 ④ 개인정보 유출 및 오용.남용방지를 위한 내부통제시스템의 구축 ⑤ 개인정보 보호 교육 계획의 수립 및 시행 ⑥ 개인정보 파일의 보호 및 관리·감독 ⑦ 그 밖에 개인정보의 적절한 처리를 위하여 대통령령으로 정한 업무 - 개인정보 처리방침의 수립.변경 및 시행 - 개인정보 보호 관련 자료의 관리 - 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기 ❍ **기타 개인정보 보호책임자의 활동(권장)** - 개인정보보호 전담조직 구성 및 전담인력 확보 - 개인정보보호 활동을 수행하는데 필요한 예산 확보 및 반영 (교육비·출장비, 진료차트S/W 등 도입·운영, 백신S/W 등 예산)	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

분 야	3. 개인정보의 안전한 관리	
점검지표	3.8 개인정보 보호책임자의 지정	
점검항목	3.8.2 개인정보 보호책임자는 개인정보보호 교육을 이수하고 관리·감독을 수행하고 있는가?	Seq: ㊺
판단기준 (해당여부)	☑ 필수사항	
점검기준	☑ 개인정보 보호책임자의 교육이수 여부 확인 ☑ 관리·감독 활동 수행여부 확인	
증빙자료	1. 개인정보 보호책임자 교육 이수 실적 - 교육 참석확인증, 수료증 등 2. 개인정보 보호책임자 관리·감독 및 제도개선 활동 실적	
관련근거	「개인정보 보호법」 제31조(개인정보 보호책임자의 지정)	
벌금과태료	없음	
세부설명	【설명】 개인정보 보호책임자 역할 개인정보 보호책임자는 기관(사업자)의 개인정보보호 총괄 업무를 수행할 수 있어야 함 【참고】 동법 시행령 제32조 제1항(개인정보 보호책임자의 업무 및 지정요건 등) **개인정보 보호책임자 교육이수** - 기관의 환경을 고려하여 집합교육, 인터넷 교육, 외부교육과정 참석, 전문 강사초빙 등 다양한 방법을 활용하여 교육 이수 ex) 요양기관업무포털(biz.hira.or.kr) 또는 개인정보보호 종합포털(www.privacy.go.kr) 등의 교육이수 **개인정보 보호책임자 관리·감독 활동(예시)** 개인정보 정기점검 체크리스트 - 각종 관리대장 기록·관리 여부 - 개인정보처리시스템 접속기록 점검 - 운영체제, 백신, 문서편집 프로그램 최신 보안 패치 적용 - 직원변경에 따른 ID, 보안서약서 관리 등	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

(개인정보 정기점검 체크리스트 예시)

3.8.2

개인정보 정기점검 체크리스트

○ 점 검 자: _____

○ 점검일자: *20XX년 XX월 XX일(매월 1회 점검)*

연번	점검사항	점검결과			점검주기
		양호	취약	해당 없음	
1	*출입통제 관리대장 기록·관리 여부*	*○*			*매월*
2	*개인정보처리시스템 접근기록 관리(정상) 여부*			*○*	*매월*
3	*백신 프로그램 정기점검 및 최신 업데이트 여부*	*○*			*매월*
4	*물리적 접근 방지 및 잠금장치 적용 여부*	*○*			*매월*
5	*비밀번호 작성규칙 준수 여부(최소 6개월마다 변경)*		*○*		*매월*
6	*직원변경에 따른 ID 및 권한 부여/변경/말소 관리*		*○*		*반기*
7	*직원변경에 따른 보안서약서 관리*	*○*			*매월*

[요양기관명] 개인정보 보호책임자: _____(인)

※ 위의 내용은 요양기관의 환경에 맞게 수정하여 사용 가능

분 야	3. 개인정보의 안전한 관리	
점검지표	3.9 개인정보 유출방지 등	
점검항목	3.9.1 개인정보 유·노출 등 침해사고 발생 시 대응절차를 숙지하고 있는가?	Seq: ㊻
판단기준 (해당여부)	☑ 필수사항	
점검기준	☑ 침해사고 대응절차 숙지여부 확인	
증빙자료	※ 동 항목은 별도의 증빙자료가 없어도 점검기준을 준수하는 경우에 점검결과를 양호로 선택하실 수 있습니다	
관련근거	「개인정보 보호법」 제34조(개인정보 유출통지 등)	
벌금과태료	3천만원 이하 과태료	
세부설명	【설명】 개인정보 유·노출 및 침해사고를 통하여 발생할 수 있는 사회적, 경제적 피해 등 2차 피해를 예방하기 위하여 개인정보 침해사고 대응 범위, 절차, 신고방법 등 침해사고 대응절차를 숙지해야 함 【참고】 요양기관(개인정보처리자)은 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이(5일 이내) 환자(정보주체)에게 통보하여야 함 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 ※ 통보 방법으로는 서면, 이메일, SMS 통보 등의 방법을 이용 **1천명 이상의 환자(정보주체)의 개인정보가 유출된 경우** 유출통지 결과를 신고해야 함 - 행정안전부 또는 전문기관(한국인터넷진흥원)에 신고해야 함 - 추가적으로 홈페이지 혹은 대기실 등 원내 보기 쉬운 장소에 7일 이상 게시하여야 함	
점검결과	✓ **(양 호)** 점검기준 준수 ✓ **(개선필요)** 점검기준 일부 준수 ✓ **(취 약)** 점검기준 미준수 ✓ **(해당없음)** 판단 기준에 따라 해당사항이 없는 경우	

(개인정보 유출 시 필수 조치요령)

3.9.1

개인정보 유출 사고 발생 시 이것만은 꼭 조치하세요!

1

유출된 정보주체 개개인에게 지체 없이 통지

⇨ **「개인정보 보호법」 제34조 제1항**

✓ 시 한: 유출되었음을 알게 되었을 경우 지체 없이(5일 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 제8호(**3천만원 이하의 과태료**)
정보주체에게 같은 항 각 호의 사항을 알리지 아니한 자

2

피해 최소화를 위한 대책 마련 및 필요한 조치 실시

⇨ **「개인정보 보호법」 제34조 제2항**

✓ 접속경로 차단, 취약점 점검·보완, 유출된 개인정보의 삭제 등 피해를 최소화하기 위해 필요한 긴급조치 이행
✓ 긴급조치 이행 등에 어려움이 있는 경우 전문기관에 기술지원 요청

* 피해 최소화 대책을 마련하지 않거나 필요한 긴급 조치를 하지 않은 경우: **시정명령**

3

1천명 이상 유출된 경우 유출 통지 결과를 신고

⇨ **「개인정보 보호법」 제34조 제3항**

✓ 1천명 이상 개인정보가 유출된 경우 유출 통지 및 조치 결과를 지체 없이 행정안전부 또는 전문기관(한국인터넷진흥원, www.privacy.go.kr)에 신고

* 「개인정보 보호법」 제75조 제2항 제9호(**3천만원 이하의 과태료**)
조치결과를 신고하지 아니한 자(행정안전부 또는 전문기관에 통지 결과 등을 신고하지 않은 경우)

4

1천명 이상 유출된 경우에는 추가적으로 홈페이지에 공지

⇨ **「개인정보 보호법 시행령」 제40조 제3항**

✓ 1천명 이상 개인정보가 유출된 경우 개별 통지와 함께 유출된 사실을 인터넷 홈페이지에 7일 이상 게재

* 홈페이지 등에 공지하지 않거나 7일 미만 게재하는 경우: **시정명령**

[별표] **개인정보처리자 유형 및 개인정보 보유량에 따른 안전조치 기준**

유형	적용대상	안전조치 기준
유형1 (완화)	▪ 1만명 미만의 정보주체에 관한 개인정보를 보유한 소상공인, 단체, 개인	▪ 제5조: 제2항부터 제5항까지 ▪ 제6조: 제1항, 제3항, 제6항 및 제7항 ▪ 제7조: 제1항부터 제5항까지, 제7항 ▪ 제8조, 제9조, 제10조, 제11조, 제13조
유형2 (표준)	▪ 100만명 미만의 정보주체에 관한 개인정보를 보유한 중소기업 ▪ 10만명 미만의 정보주체에 관한 개인정보를 보유한 대기업, 중견기업, 공공기관 ▪ 1만명 이상의 정보주체에 관한 개인정보를 보유한 소상공인, 단체, 개인	▪ 제4조: 제1항제1호부터 제11호까지 및 제15호, 제3항부터 제4항까지 ▪ 제5조 ▪ 제6조: 제1항부터 제7항까지 ▪ 제7조: 제1항부터 제5항까지, 제7항 ▪ 제8조, 제9조, 제10조, 제11조, 제13조
유형3 (강화)	▪ 10만명 이상의 정보주체에 관한 개인정보를 보유한 대기업, 중견기업, 공공기관 ▪ 100만명 이상의 정보주체에 관한 개인정보를 보유한 중소기업, 단체	▪ 제4조부터 제13조까지

내부관리계획에 포함되어야 하는 필수 사항

내부관리계획 포함 사항		유형1 (완화)	유형2 (표준)	유형3 (강화)
항	호			
① 개인정보처리자는 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 다음 각 호의 사항을 포함하는 내부 관리계획을 수립·시행하여야 한다.	1. 개인정보 보호책임자의 지정에 관한 사항	-	O	O
	2. 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사한	-	O	O
	3. 개인정보취급자에 대한 교육에 관한 사항	-	O	O
	4. 접근권한의 관리에 관한 사항	-	O	O
	5. 접근 통제에 관한 사항	-	O	O
	6. 개인정보의 암호화 조치에 관한 사항	-	O	O
	7. 접속기록 보관 및 점검에 관한 사항	-	O	O
	8. 악성프로그램 등 방지에 관한 사항	-	O	O
	9. 물리적 안전조치에 관한 사항	-	O	O
	10. 개인정보 보호조직에 관한 구성 및 운영에 관한 사항	-	O	O
	11. 개인정보 유출사고 대응 계획 수립·시행에 관한 사항	-	O	O

	12. 위험도 분석 및 대응방안 마련에 관한 사항	-	-	O
	13. 재해 및 재난 대비 개인정보처리시스템의 물리적 안전조치에 관한 사항	-	-	O
	14. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항	-	-	O
	15. 그 밖에 개인정보 보호를 위하여 필요한 사항	-	O	O
② [별표]의 유형1에 해당하는 개인정보처리자는 제1항에 따른 내부 관리계획을 수립하지 아니할 수 있고, [별표]의 유형2에 해당하는 개인정보처리자는 제1항제12호부터 제14호까지를 내부 관리계획에 포함하지 아니할 수 있다.				
③ [별표]의 유형1에 해당하는 개인정보처리자는 제1항에 따른 내부 관리계획을 수립하지 아니할 수 있고, [별표]의 유형2에 해당하는 개인정보처리자는 제1항제12호부터 제14호까지를 내부 관리계획에 포함하지 아니할 수 있다.		-	O	O
④ 개인정보 보호책임자는 연 1회 이상으로 내부 관리계획의 이행 실태를 점검·관리 하여야 한다.		-	O	O

▶ 내부관리계획 수립의무 위반 시, 3천만원 이하 과태료 부과(법 제75조제2항제6호)

▶ 위의 각 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부 관리계획을 수정하여 시행하고, 그 수정이력을 관리해야 함

▶ 개인정보 보호책임자는 연 1회 이상 내부관리계획의 이행 실태를 점검·관리하여야 함