개인정보보호
자율점검 참고자료
(의료기관)

2017. 5.

사단법인
대한병원협회
Korean Hospital Association

분 야	1. 개인정보의 처리(수집 · 이용 · 제공 등)		
점검지표	1.1 개인정보의 수집 · 이용		
점검항목	1.1.1 진료목적 외로 서면가입(오프라인)·홈페이지 (온라인) 등을 통한 회원 가입 시 동의는 받고 있는가?		Seq: 1
판단기준 (해당여부)	※ 서면 및 홈페이지 등을 통한 회원가입(개인정보수집)을 하지 않는 경우 해당 없음		
점검기준	※ 필수항목(4개)를 정보주체(환자)에게 고지하고 동의를 받아야 한다. 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		
증빙자료	회원가입신청서(고지내용 ①~④ 포함된 서면 또는 홈페이지 등의 회원가입신청서)		
관련근거	개인정보보호법 제15조(개인정보의 수집·이용)	행정자치부 점검항목	1-1, 1-2, 1-3, 6-1, 7-1
벌금과태료	3천만 원 이하 과태료		
세부설명	【설명】 서면(오프라인) 또는 홈페이지(온라인)등을 통해 정보주체(환자)의 개인정보를 수집·이용하는 경우 개인정보처리자(의료기관 담당자)는 필수항목 4가지를 정보주체(환자)에게 고지하고 동의를 받아야 한다. - 회원가입이 필요한 홈페이지를 운영하거나, 별도의 서비스(홍보, 마케팅, 상담 등)를 제공하는 경우 - 고객관리를 위한 개인정보는 별도의 동의 필요 - 홈페이지 회원 개인정보 수집 시, 정보주체의 동의 필요 - 홈페이지 회원정보로 주민등록번호는 수집하지 않도록 해야 함 (주민등록번호를 사용하지 아니하고도 회원가입 할 수 있는 방법을 제공) 【참고】 최소 개인정보(필수정보)와 그 외의 개인정보(선택정보 : 홍보, 상담, 마케팅 등)를 구분하여 정보주체(환자)가 명확하게 인지할 수 있도록 알리고 회원가입 신청 서식에 개인정보 수집·이용에 관한 명시적 '동의' 표시(체크) 여부 확인		
점검결과 선택방법	① **(양호)** 점검기준 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 진료목적외 회원가입을 하지 않음(개인정보 수집을 안 함)		

분 야	1. 개인정보의 처리(수집 · 이용 · 제공 등)		
점검지표	1.1 개인정보의 수집 · 이용		
점검항목	1.1.2 각종 게시판, 기타 개인정보 수집 시 동의는 받고 있는가?		Seq: 2
판단기준 (해당여부)	※ 서면 및 홈페이지 등을 통한 회원가입(개인정보수집)을 하지 않는 경우 해당 없음 - 의료법 제22조, 같은 법 시행규칙 제14조(진료기록부 등의 기재사항)에 의해 **진료를 목적으로 수집**하는 필요한 최소한의 개인정보는 동의 받지 않아도 됨		
점검기준	※ 필수항목(4개)을 정보주체(환자)에게 고지하고 동의를 받아야 한다. 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		
증빙자료	개인정보처리동의서(고지내용①~④이 포함된 서면 또는 홈페이지 등의 개인정보처리동의서)		
관련근거	개인정보보호법 제15조(개인정보의 수집·이용)	**행정자치부 점검항목**	1-1, 1-2, 1-3, 6-1
벌금과태료	3천만 원 이하 과태료		
세부설명	【설명】 홈페이지 운영 시 각종 게시판을 통해 개인정보를 수집하는 경우와 회원 가입이 아닌 형태의 모든 개인정보를 수집하는 서식에 개인정보 수집·이용에 관한 명시적 '동의' 표시(체크) 여부 확인 - 진료목적으로 수집가능한 개인정보는 **성명, 주민번호, 전화번호, 주소** 등 【참고】 홈페이지 회원가입은 대부분 동의를 받고 있으나, 게시판은 동의 받지 않는 사례 다수 있음 - 홈페이지를 운영하는 의료기관에서 홈페이지 내 게시판(건의사항, 상담, 자유게시판 등)을 통해 개인정보를 수집하는 경우, 개인정보 수집·이용에 관한사항을 알려주고 동의를 받아야 함		
점검결과 선택방법	① **(양호)** 점검기준 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 회원가입을 하지 않음(개인정보 수집을 안 함)		

분 야	1. 개인정보의 처리(수집 · 이용 · 제공 등)		
점검지표	1.2 개인정보의 수집 제한		
점검항목	1.2.1 목적에 필요한 최소한의 개인정보 수집하고 있는가?		Seq: 3
판단기준 (해당여부)	※ 서면 및 홈페이지 등을 통한 회원가입, 별도의 서비스(홍보, 마케팅, 상담) 제공을 목적으로 개인정보 수집을 하지 않는 경우 해당 없음		
점검기준	1. 목적달성을 위한 최소한의 개인정보만 수집 2. 선택정보 제공 미동의시에도 서비스 제공 3. 최소한의 정보 외의 개인정보 수집에는 동의하지 아니할 수 있다는 고지		
증빙자료	회원가입신청서(고지내용 ①~④이 포함된 서면 또는 홈페이지 등의 회원가입신청서)		
관련근거	개인정보보호법 제16조(개인정보의 수집 제한)	행정자치부 점검항목	2-1
벌금과태료	3천만 원 이하 과태료		
세부설명	【설명】 개인정보를 필요 이상으로 수집·저장하고 있으면 해킹 등에 의하여 언제든지 개인정보가 유출될 위험이 있고, 개인정보처리자(의료기관 담당자)에 의하여 남용될 우려가 있기 때문에 목적에 필요한 범위 내에서 최소한의 개인정보만을 수집하여야 함 또한, 필요 최소한의 정보 외의 개인정보 수집(선택정보)에 동의하지 아니한다는 이유로 정보주체(환자)에게 재화 또는 서비스 제공을 거부해서는 안 됨(회원 가입도 포함) - 서면(오프라인) 또는 홈페이지(온라인)등에서 개인정보를 수집하는 경우, 목적 달성을 위해 반드시 수집하여야 하는 최소한의 개인정보인지 여부 확인 - 필수정보는 아니나, 추가적인 서비스 제공 등을 위해 필요한 선택정보로 수집하는 경우에도 목적 달성을 위한 최소한의 정보인지 여부를 확인 - 정보주체(환자)의 동의를 받아 개인정보를 수집하는 경우라도 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 아니할 수 있다는 사실을 구체적으로 알리고 수집하는지 확인 - 전화를 통하여 개인정보를 수집할 때에는 녹취사실을 정보주체(환자)에게 알려야 하며 해당녹취파일에 대하여 안전성 확보조치를 해야 함 【참고】 최소한의 개인정보 수집 여부에 대한 입증 책임은 개인정보처리자(의료기관 담당자)가 부담		
점검결과 선택방법	① **(양호)** 점검기준 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 회원가입을 하지 않음(개인정보 수집을 안 함)		

분 야	1. 개인정보의 처리(수집 · 이용 · 제공 등)		
점검지표	1.2 개인정보의 수집 제한		
점검항목	1.2.2 최소한 정보 외의 개인정보 수집에 대한 미 동의를 이유로 재화 또는 서비스 제공 거부 하고 있지는 않는가?		Seq: 4
판단기준 (해당여부)	※ 서면 및 홈페이지 등을 통한 회원가입(개인정보수집)을 하지 않는 경우 해당 없음		
점검기준	※ 필수정보 외 개인정보 수집 미동의시에도 회원가입 등 기본적인 서비스 제공		
증빙자료	회원가입신청서(고지내용 ①~④이 포함된 서면 또는 홈페이지 등의 회원가입신청서)		
관련근거	개인정보보호법 제16조(개인정보의 수집 제한)	**행정자치부 점검항목**	2-2, 6-2, 6-3, 6-4
벌금과태료	3천만 원 이하 과태료		
세부설명	【설명】 최소한의 정보(필수정보) 외의 개인정보 수집에 동의하지 않아도 회원 가입(홈페이지, 서면 등) 또는 기본적인 서비스 제공이 가능한지 여부 확인 특히, 홈페이지 회원 가입 시 필수정보가 아닌, 선택정보로 되어 있는 개인정보 미 입력 시 회원가입 진행을 하지 못하는 경우 확인 - 고객관리를 위한 개인정보는 별도의 동의 필요 - 홈페이지 회원 개인정보 수집 시, 정보주체의 동의 필요 - 홈페이지 회원정보로 주민등록번호는 수집하지 않도록 해야 함 (주민등록번호를 사용하지 아니하고도 회원가입할 수 있는 방법을 제공) 【참고】 홈페이지에서 선택정보이나 동의 체크하지 않으면 다음으로 넘어가지 않은 사례가 있음 예) 홈페이지 회원가입 시 선택정보임에도 불구하고 미동의 시 회원가입이 되지 않는 경우		
점검결과 선택방법	① **(양호)** 점검기준 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 회원가입을 하지 않음(개인정보 수집을 안 함)		

분 야	1. 개인정보의 처리(수집 · 이용 · 제공 등)		
점검지표	1.2 개인정보의 수집 제한		
점검항목	1.2.3 만 14세 미만 아동의 개인정보를 처리 시, 법정대리인의 동의 여부		Seq: 5
판단기준 (해당여부)	14세 미만 아동의 개인정보를 처리 시, 법정대리인의 동의 여부 확인		
점검기준	※ 개인정보파일의 정보주체들 중 만 14세 미만의 아동이 있을 경우, 해당 아동으로부터 개인정보를 수집 시 법정대리인으로부터 동의를 받았는지 확인		
증빙자료	법정 대리인의 동의 자료		
관련근거	개인정보보호법 제22조(개인정보의 수집 제한)	행정자치부 점검항목	6-5
벌금과태료	3천만 원 이하 과태료		
세부설명	【설명】 개인정보처리자는 만 14세 미만 아동의 법정대리인의 동의를 받기 위하여 해당 아동으로부터 직접 법정대리인의 성명 · 연락처에 관한 정보를 수집할 수 있음		
점검결과 선택방법	① **(양호)** 점검기준 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 회원가입을 하지 않음(개인정보 수집을 안 함)		

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 정보주체(환자)의 별도 동의는 받고 있는가?**		**Seq: 6**
판단기준 (해당여부)	※ 제3자 정보제공 및 목적 외 이용 사실이 없는 경우 해당사항 없음 ※ "제3자" 란? ☞ 정보주체(환자)또는 그의 법정대리인으로부터 개인정보를 수집·보유한 해당 기관을 제외한 모든 자(수탁자는 제외)		
점검기준	※ 제3자 제공을 위한 동의사항(①~⑤)을 고지하고 동의 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		
증빙자료	제3자 제공 동의서(필수고지내용 ①~⑤이 포함된 동의서) - 환자의 진료기록은 의료법에서 정한 위임장 등 관련서류를 첨부한 경우에만 제공 가능		
관련근거	개인정보보호법 제17조(개인정보의 제공), 제18조(개인정보의 목적 외 이용·제공 제한)	**행정자치부 점검항목**	3-1, 3-2, 3-3, 4-1, 4-2, 4-3, 6-1, 7-1
벌금과태료	5년 이하 징역 또는 5천만 원 이하 벌금		
세부설명	【설명】 개인정보를 수집 목적을 넘어 이용하거나 제공하는 경우, 다른 개인정보의 처리에 대한 동의와 분리해서 목적 외 이용·제공에 대한 별도의 동의를 받아야 함 - 법률에서 정한 개인정보 수집목적 범위 내에서 제3자 제공이 가능한 경우에는 별도 고지 후 동의 받을 필요 없음 · 감염병의 예방 및 관리에 관한 법률 제16조(감염병 표본감시 등) · 생명윤리 및 안전에 관한 법률 제18조(개인정보의 제공) · 응급의료에 관한 법률 제11조(응급환자의 이송) · 의료법 제21조(기록 열람 등) · 후천성면역결핍증 예방법 제5조(의사 또는 의료기관 등의 신고) 【참고】 - 제3자 제공 동의 시 ⑤번에 대한 고지 없이 동의 받는 사례 있음 - "개인정보보호 가이드라인 <2015.02>" 內 열람 또는 사본의 교부 등 허용사유 참고		
점검결과 선택방법	① **(양호)** 점검기준 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 제3자 정보제공 및 목적 외 이용 사실이 없음		

분 야	1. 개인정보의 처리(수집 · 이용 · 제공 등)		
점검지표	1.3 개인정보의 제공		
점검항목	**1.3.2 정보주체(환자)에게 사전에 "제3자 개인정보 제공 및 목적 외 이용 관련 사항을 동의 받고 있는가?**		**Seq: 7**
판단기준 (해당여부)	※ 제3자 정보제공 및 목적 외 이용 사실이 없는 경우 해당사항 없음 ※ "제3자" 란? ☞ 정보주체(환자)와 그의 법정대리인으로부터 개인정보를 수집·보유한 해당 기관을 제외한 모든 자(수탁자는 제외)		
점검기준	※ 제3자에게 개인정보 제공 및 목적 외 이용 시 정보주체에게 통보함		
증빙자료	1. 서면으로 고지한 경우 관련 문서 2. 서면, 홈페이지, 이메일, 접수실 게시 등 고지 사실을 확인할 수 있는 증빙자료		
관련근거	개인정보보호법 제17조(개인정보의 제공)	**행정자치부 점검항목**	3-1, 3-2, 3-3
벌금과태료	3천만 원 이하 과태료		
세부설명	【설명】 제3자에게 개인정보 제공 및 목적 외 이용 시 점검항목 1.3.1에서 별도 동의를 받았더라도 정보주체(환자)에게 사실을 통보하여야 함 - 법률에서 정한 개인정보 수집목적 범위 내에서 제3자 제공이 가능한 경우에는 별도 고지 후 동의 받을 필요 없음 【예시】 **<정보주체에게 알려야 할 사항>** 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 【참고】 서면, 홈페이지 공고, 이메일, 접수실 게시 등 다양한 방법으로 통지		
점검결과 선택방법	① **(양호)** 점검기준 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 제3자 정보제공 및 목적 외 이용 사실이 없음		

분 야	1. 개인정보의 처리(수집 · 이용 · 제공 등)		
점검지표	1.4 개인정보 이용 · 제공 제한		
점검항목	1.4.1 개인정보를 목적 외로 이용하거나 제3자에게 제공하는 경우, 해당 내용을 기록하고 관리하는가? (공공의료기관)		Seq: 8
판단기준 (해당여부)	※ 제3자 정보제공 및 목적 외 이용 사실이 없는 경우 해당사항 없음 ※ "제3자" 란? ☞ 정보주체(환자)또는 그의 법정대리인으로부터 개인정보를 수집·보유한 해당 기관을 제외한 모든 자(수탁자는 제외)		
점검기준	※ 필수기재사항 8항목이 기재된 "개인정보 목적 외 이용 및 제3자 제공 대장" 비치(관련 문서 보관)		
증빙자료	개인정보 목적 외 이용 및 제3자 제공 대장(필수기재사항 8항목 포함)		
관련근거	개인정보보호법 제18조(개인정보의 목적 외 이용·제공 제한)	행정자치부 점검항목	4-1, 4-2, 4-3
벌금과태료	5년 이하 징역 또는 5천만 원 이하 벌금, 3천만 원 이하 과태료		
세부설명	【설명】 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우에는 아래의 내용을 "개인정보의 목적 외 이용 및 제3자 제공 대장"에 기록하고 관리하여야 한다. (개인정보보호법 시행령 제15조, 시행규칙 제3조) **< 필수 기재사항 8항목 >** ① 이용하거나 제공하는 개인정보 또는 개인정보파일의 명칭 ② 이용기관 또는 제공받는 기관의 명칭 ③ 이용 목적 또는 제공받는 목적 ④ 이용 또는 제공의 법적 근거 ⑤ 이용하거나 제공하는 개인정보의 항목 ⑥ 이용 또는 제공의 날짜, 주기 또는 기간 ⑦ 이용하거나 제공하는 형태 ⑧ 법률에 따라 목적 등을 제한하거나 필요한 조치를 마련할 것을 요청한 경우에는 그 내용(문서) ※ 법률의 규정에 따라 환자정보 제공 가능 : 국민건강보험공단, 건강보험심사평가원, 법원, 국민연금공단, 보험회사(자보), 근로복지공단(산재)등의 경우 【참고】 "개인정보보호 가이드라인 <2015.2>" 內 열람 또는 사본의 교부 등 허용 사유 참고		
점검결과 선택방법	① **(양호)** 점검기준 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 개인정보를 목적 외로 이용하거나 제3자에게 제공하지 않음		

분 야	1. 개인정보의 처리(수집 · 이용 · 제공 등)		
점검지표	1.5 개인정보 파기		
점검항목	**1.5.1 진료목적으로 수집한 진료정보 보유기간 경과, 처리목적(제공받는 경우 제공받는 목적) 달성 후 지체 없이 개인정보를 파기하고 관리대장을 작성하여 관리하고 있는가?**		**Seq: 9**
판단기준(해당여부)	※ 의료법 시행규칙 제15조(진료에 관한 기록의 보존)에서 정한 보존기간이 경과했는지의 여부(환자명부 : 5년, 진료기록부 : 10년, 처방전 : 2년, 수술기록 : 10년, 검사소견기록 : 5년, 방사선 사진 및 그 소견서 : 5년, 간호기록부 : 5년, 조산기록부 : 5년, 진단서 등의 부본 : 3년) ※ 다만, 의료기관은 계속적인 진료를 위하여 필요한 경우에는 매년 1회 이상 보존기간 연장여부 혹은 파기여부를 결정할 수 있음		
점검기준	1. 처리목적을 달성한 개인정보를 지체 없이 파기 2. 개인정보 파기결과를 파기관리대장에 기록		
증빙자료	1. 개인정보파일 파기 요청서 2. 개인정보파일 파기 관리대장 3. 파기 사실 확인서(위탁) 또는 증빙서류(파기현장사진 등)		
관련근거	개인정보보호법 제21조(개인정보의 파기)	**행정자치부 점검항목**	5-1
벌금과태료	3천만 원 이하 과태료		
세부설명	【설명】 개인정보처리자(의료기관 담당자)는 보유기간의 경과 및 개인정보의 처리목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이(5일 이내) 그 개인정보를 파기하도록 하고 있다. - 개인정보파일 전체가 보유 목적 상실 등으로 파기하는 경우 1. "개인정보파일 파기요청서"를 작성하여 개인정보보호책임자의 승인을 받고 파기를 실행한다. 2. 개인정보파일 파기결과를 개인정보파일 파기 관리대장에 기록한다. 【참고】 - 표준개인정보보호지침 제11조 제1항 및 2항, 제56조 4항 - 개인정보파일을 연장하여 보존하는 경우 "개인정보보호_가이드라인<2015.2>" 內 개인정보의 파기 참고 ※ 서면이나 홈페이지를 통해 수집한 정보도 처리목적을 달성한 경우에는 그 정보를 파기하여야 한다.		
점검결과 선택방법	① **(양호)** 점검기준 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 진료를 하지 않는 의료기관		

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: 10
판단기준 (해당여부)	※ 의료법 시행규칙 제15조(진료에 관한 기록의 보존)에서 정한 보존기간이 경과했는지의 여부(환자명부 : 5년, 진료기록부 : 10년, 처방전 : 2년, 수술기록 : 10년, 검사소견기록 : 5년, 방사선 사진 및 그 소견서 : 5년, 간호기록부 : 5년, 조산기록부 : 5년, 진단서 등의 부본 : 3년) ※ 다만, 의료기관은 계속적인 진료를 위하여 필요한 경우에는 매년 1회 이상 보존기간 연장여부 혹은 파기여부를 결정할 수 있음		
점검기준	1. 개인정보의 파기 시 복원 불가능한 방법으로 파기 2. 파기 결과 증빙서류 보관		
증빙자료	※ 동 항목은 별도의 증빙자료가 없어도 점검기준을 만족하는 경우에 점검 결과를 양호로 선택하실 수 있습니다.		
관련근거	개인정보보호법 제21조(개인정보의 파기)	행정자치부 점검항목	5-1
벌금과태료	3천만원 이하 과태료		
세부설명	【설명】 개인정보(파일)의 당초 수집목적이 달성되었거나, 보유기간이 경과되어 파기 시 복원이 불가능한 방법으로 영구 삭제하여야 한다. - 개인정보의 '복원이 불가능한 방법' 이란 사회통념상 현재의 기술수준에서 적절한 비용이 소요되는 방법을 말한다. · 전자적 파일 : 청구S/W 파기기능을 이용하여 파기 · 별도저장매체 : 하드디스크, USB, CD · 파기 방법 : 천공, 소각, 파쇄 등 【참고】 표준개인정보보호지침 제10조 제2항 - 개인정보취급자는 종이에 출력된 개인정보는 분쇄기로 분쇄하거나 소각을 통하여 파기하고 전자적 파일 형태의 정보는 기록을 재생할 수 없는 기술적 방법을 사용하여 파기한다. ※ (권고)보존기간이 도래하지 않은 경우 파기계획 수립		
점검결과 선택방법	① **(양호)** 점검기준 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 파기대상 개인정보 없음		

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: 11
판단기준 (해당여부)	※ 개인정보가 포함된 임시파일 및 출력자료가 없으면 해당 없음		
점검기준	1. 임시파일 및 출력자료는 사용 후 즉시 파기 2. 업무 PC내에 개인정보가 포함된 자료가 없어야함		
증빙자료	※ 동 항목은 별도의 증빙자료가 없어도 점검기준을 만족하는 경우에 점검 결과를 양호로 선택하실 수 있습니다.		
관련근거	개인정보보호법 제21조(개인정보의 파기)	행정자치부 점검항목	5-1
벌금과태료	3천만 원 이하 과태료		
세부설명	【설명】 업무 수행 상 보존 필요성은 없으나, 임시적으로 생성된 파일이나 출력 자료를 사용 후 즉시 파기하는지 여부 확인 - 예) 개인정보가 포함된 파일, 서류, 환자사진 등 · 문서파일(한글문서, 워드, 엑셀, 환자사진 등) · 출력자료 : 진료기록부 사본, 처방전 등 【참고】 표준개인정보보호지침 제10조 제1항		
점검결과 선택방법	① **(양호)** 점검기준 모두 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 진료를 하지 않는 의료기관		

분 야	1. 개인정보의 처리(수집 · 이용 · 제공 등)		
점검지표	1.5 개인정보의 파기		
점검항목	1.5.4 타 법령에 따라 보존하는 경우 개인정보를 별도로 분리보관 하고 있는가?		Seq: 12
판단기준 (해당여부)	※ 타 법령에 근거하여 개인정보의 전부 또는 일부를 보유할 필요가 없는 경우 해당 없음		
점검기준	1. 법령에 따라 개인정보를 별도로 분리 보관 2. 개인정보 관리대장을 작성		
증빙자료	개인정보 관리대장		
관련근거	개인정보보호법 제21조(개인정보의 파기)	행정자치부 점검항목	5-2
벌금과태료	1천만 원 이하 과태료		
세부설명	【설명】 개인정보의 수집목적이 달성된 경우에도 타 법령에 근거하여 개인정보를 전부 또는 일부 보유한다면 보유 근거법령 및 보유기간 등을 정보주체에게 명확하게 공개하고, 그 개인정보를 별도의 DB 등에 분리하여 보관하여야 함 개인정보를 이용, 제공, 파기, 열람하는 경우 개인정보 관리대장을 작성하여 보관하여야 함 【참고】 접근권한은 소송 담당자 등 필수요원으로 접근권한을 엄격히 제한 필요 - 법령에 따라 분리 보관한다는 의미는 소송, 민원 등 특정한 상황이 아니면 접근할 필요가 없다는 것이다. ※ 법원·경찰 등에서 법률에 의해서 보존요청이 올 경우 요청기간에 따라 보존하여야함 - 해당 기관 관련 법률(형사소송법, 민사소송법, 의료법 등) - 다른 법령에 따라 보존하는 개인정보 Data Base 중, 파기 여부 확인 예) 필드에 삭제 표기의 플래그 형태로 남기는 사례 확인 등 - 진료기록의 보존기간(의료법 시행규칙 제15조) · 진료기록부 : 10년 · 간호기록부 : 5년 · 처방전 : 2년(요양급여비용을 청구한 처방전은 3년)		
점검결과 선택방법	① **(양호)** 점검기준 모두 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 법령에 따라 분리 보관할 개인정보가 없음		

분 야	2. 개인정보의 처리 제한		
점검지표	2.1 민감정보의 처리제한		
점검항목	**2.1.1 사상, 정치, 건강 등 민감정보의 동의에 의한 수집 및 제공 시 개인정보 수집 동의와 별도로 구분하여 동의 받고 있는가?**		**Seq: 13**
판단기준 (해당여부)	※ 민감정보를 수집하지 않는 경우 해당 없음 민감정보 : 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 유전정보, 범죄경력자료 등		
점검기준	※ 민감정보 수집 시 별도동의를 받아야 함		
증빙자료	민감정보 수집 동의서		
관련근거	개인정보보호법 제23조(민간정보의 처리 제한)	**행정자치부 점검항목**	7-1, 6-1
벌금과태료	5년 이하 징역 또는 5천만 원 이하 벌금		
세부설명	【설명】 개인정보보호법 제23조에서 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보(민감정보)는 처리하지 못하게 되어있다. - 다음사항에 해당하는 경우에는 처리 가능 1. 정보주체에게 개인정보보호법 제15조제2항 각 호(점검항목 1.1.1의 필수고지사항①~④) 또는 제17조제2항 각 호(점검항목 1.3.1의 필수고지사항①~⑤)의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우 2. 법령에서 민감정보의 처리를 요구하거나 허용하는 경우 ※ 진료목적으로 수집하는 경우 별도 동의 불필요 (진료목적의 범위 : 진료신청, 진단, 검사, 치료, 수납 등) 개인정보보호법 제18조 2항에서 목적 외 이용 및 제3자 제공 시, 제23조에서 민감정보의 수집 시, 제24조에서 고유식별 정보의 수집 시, 별도 동의를 받도록 하고 있다. 또한 재화나 서비스를 홍보하거나 판매를 권유하기 위하여 개인정보의 처리에 대한 동의를 받으려는 때는 정보주체가 이를 명확하게 인지할 수 있도록 알리고 동의를 받아야 한다.		
점검결과 선택방법	① **(양호)** 점검기준 모두 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 민감정보 수집을 하지 않음		

분 야	2. 개인정보의 처리 제한		
점검지표	2.2 고유식별정보의 처리제한		
점검항목	2.2.1 관련법령에 의거하여 고유식별정보를 수집하고 안전하게 처리하고 있는가?		Seq: 14
판단기준 (해당여부)	※ 고유식별정보를 수집하지 않는 경우 해당 없음 (고유식별정보: 주민번호, 여권번호, 운전면허번호, 외국인등록번호)		
점검기준	1. 관련법령에 의거하여 고유식별 정보를 수집 2. 고유식별정보 암호화 등 안전성 확보조치 수행		
증빙자료	※ 동 항목은 별도의 증빙자료가 없어도 점검기준을 만족하는 경우에 점검결과를 양호로 선택하실 수 있습니다.		
관련근거	개인정보보호법 제24조(고유식별정보의 처리 제한), 제24조의 2(주민등록번호 처리의 제한)	행정자치부 점검항목	8-1, 9-1, 7-1
벌금과태료	5년 이하의 징역 또는 5천만 원 이하의 벌금, 3천만 원 이하의 과태료		
세부설명	【설명】 개인정보보호법 제24조의 2에서 법령에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우에 한하여 처리가능 - 다음사항에 해당하는 경우에는 처리 가능 1. 법령에서 구체적으로 주민등록번호의 처리를 요구하거나 허용하는 경우 2. 정보주체(환자) 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우 개인정보처리자는 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 않게 암호화 조치를 통하여 안전하게 보관하여야 함 ※ 기 보유 주민번호 중 법령상 근거가 없는 경우 법 시행 후 2년 이내 파기('16.8.6) - 의료법 및 약사법에 근거하여 받은 사항은 해당 없음 ※ 주민번호 유출 등이 발생한 경우 안전성 확보조치를 하지 않았을 시 최대 5억 원 이하 과징금 부과징수 【참고】 개인정보의 안전성 확보조치 기준(행정자치부고시 제2014-7호)		
점검결과 선택방법	① **(양호)** 점검기준 모두 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 고유식별정보를 수집하지 않는 경우 해당 없음		

분 야	2. 개인정보의 처리 제한		
점검지표	2.2 고유식별정보의 처리제한		
점검항목	2.2.2 주민등록번호 외 회원가입 방법 제공 여부		Seq: 15
판단기준 (해당여부)	주민등록번호 외 회원가입 방법 제공하는가?		
점검기준	※ 공공기관 및 공공기관 외의 인터넷 홈페이지를 운영하는 자로 전년말 기준 직전 3개월간 인터넷 홈페이지를 이용자 수가 하루 평균 1만명이상인 경우 - 인터넷 홈페이지를 통하여 회원으로 가입할 경우 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법		
증빙자료	주민등록번회 외 회원가입 방법 증비자료		
관련근거	개인정보보호법 제24조의 2(주민등록번호 처리의 제한)	행정자치부 점검항목	9-2
벌금과태료	3천만 원 이하 과태료		
세부설명	【설명】(예 : I-PIN, 공인인증서, 휴대전화 인증 등)을 제공하고 있는지 확인정보의 안전성 확보조치 기준(행정자치부고시 제2014-7호)		
점검결과 선택방법	① **(양호)** 점검기준 모두 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 홈페이지 이용자 수 하루 평균 1만명 미만인 경우		

<table>
<tr><td>분 야</td><td colspan="3">2. 개인정보의 처리 제한</td></tr>
<tr><td>점검지표</td><td colspan="3">2.2 주민등록번호 처리의 제한</td></tr>
<tr><td>점검항목</td><td colspan="2">2.2.3 주민등록번호를 저장하는 경우 암호화 하였는가?
(100만명 이상의 주민등록번호를 저장하는 경우에는 ‘17.12.31까지 암호화 예정인가?)</td><td>Seq: 16</td></tr>
<tr><td>판단기준
(해당여부)
점검기준</td><td colspan="3">주민등록번호를 안전한 알고리즘을 사용하여 암호화하여 저장 하였는가?</td></tr>
<tr><td>증빙자료</td><td colspan="3">암호화 조치 여부 확인 자료</td></tr>
<tr><td>관련근거</td><td>개인정보보호법
제24조의2(주민등록번호 처리의 제한 등)</td><td>행정자치부
점검항목</td><td></td></tr>
<tr><td>벌금과태료</td><td colspan="3">5천만원 이하 과태료</td></tr>
<tr><td>세부설명</td><td colspan="3">「개인정보 보호법」제24조의2 제2항

제24조의2(주민등록번호 처리의 제한)
② 개인정보처리자는 제24조제3항에도 불구하고 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다. 이 경우 암호화 적용 대상 및 대상별 적용 시기 등에 관하여 필요한 사항은 개인정보의 처리 규모와 유출 시 영향 등을 고려하여 대통령령으로 정한다.

「개인정보 보호법 시행령」제21조의2

제21조의2(주민등록번호 암호화 적용 대상 등)
① 법 제24조의2제2항에 따라 암호화 조치를 하여야 하는 암호화 적용 대상은 주민등록번호를 전자적인 방법으로 보관하는 개인정보처리자로 한다.
② 제1항의 개인정보처리자에 대한 암호화 적용 시기는 다음 각 호와 같다.
1. 100만명 미만의 정보주체에 관한 주민등록번호를 보관하는 개인정보처리자: 2017년 1월 1일
2. 100만명 이상의 정보주체에 관한 주민등록번호를 보관하는 개인정보처리자: 2018년 1월 1일
③ 행정자치부장관은 기술적·경제적 타당성 등을 고려하여 제1항에 따른 암호화 조치의 세부적인 사항을 정하여 고시할 수 있다.</td></tr>
</table>

암호화 적용 기준 요약표

<table>
<tr><th colspan="4">구분</th><th>암호화기준</th></tr>
<tr><td>정보통신망, 보조저장매체를 통한 송신 시</td><td colspan="3">비밀번호, 바이오정보, 고유식별정보</td><td>암호화 송신</td></tr>
<tr><td rowspan="5">개인정보처리 시스템에 저장 시</td><td colspan="3">비밀번호</td><td>일방향(해쉬 함수) 암호화 저장</td></tr>
<tr><td colspan="3">바이오정보</td><td>암호화 저장</td></tr>
<tr><td rowspan="3">고유식별정보</td><td colspan="2">주민등록번호</td><td>암호화 저장
※ 암호화 저장 시기 개인정보보호법 시행령 제21조의2 참고</td></tr>
<tr><td rowspan="2">여권번호, 외국인 등록번호, 운전면허 번호</td><td>인터넷 구간, 인터넷 구간과 내부망의 중간 지점(DMZ)</td><td>암호화 저장</td></tr>
<tr><td>내부망에 저장</td><td>암호화 저장 또는 다음 항목에 따라 암호화 적용 여부·적용범위를 정하여 시행
① 개인정보 영향평가 대상이 되는 공공기관의 경우, 그 개인정보 영향평가의 결과
② 암호화 미적용시 위험도 분석에 따른 결과</td></tr>
<tr><td>업무용 컴퓨터, 모바일 기기에 저장시</td><td colspan="3">비밀번호, 바이오정보, 고유식별정보</td><td>암호화 저장
※ 비밀번호는 일방향 암호화 저장</td></tr>
</table>

점검결과 선택방법	① **(양호)** 점검기준 모두 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 주민등록번호를 수집하지 않는 경우.

<table>
<tr><td>분 야</td><td colspan="3">2. 개인정보의 처리제한</td></tr>
<tr><td>점검지표</td><td colspan="3">2.3 영상정보처리기기 설치운영 제한</td></tr>
<tr><td>점검항목</td><td colspan="2">2.3.1 영상정보처리기기(CCTV) 운영·관리방침을 수립하고 있는가?</td><td>Seq: 17</td></tr>
<tr><td>판단기준
(해당여부)</td><td colspan="3">※ 영상정보처리기기(CCTV)가 없는 경우는 해당 없음</td></tr>
<tr><td>점검기준</td><td colspan="3">1. 영상정보처리기기(CCTV) 운영·관리방침 수립
2. 영상정보처리기기(CCTV) 운영·관리방침 공개</td></tr>
<tr><td>증빙자료</td><td colspan="3">영상정보처리기기(CCTV) 운영 · 관리 방침(필수 기재사항 ①~⑧ 포함하여 수립)</td></tr>
<tr><td>관련근거</td><td>개인정보보호법
제25조(영상정보처리기기의 설치운영 제한),
시행령 제25조(영상정보처리기기의 운영관리 방침)</td><td>행정자치부
점검항목</td><td>없음
(개인정보 점검
대상항목이 아님)</td></tr>
<tr><td>벌금과태료</td><td colspan="3"></td></tr>
<tr><td>세부설명</td><td colspan="3">【설명】 영상정보처리기기(CCTV) 운영자는 아래 내용이 포함된 영상정보처리기기(CCTV) 운영 · 관리방침을 마련하고, 이를 공개하여야 한다.(법 제25조 제7항, 시행령 제25조)

<영상정보처리기기(CCTV) 운영·관리 방침에 포함되어야 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 (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 개인정보처리방침과 동일하게 인터넷 홈페이지 또는 보기 쉬운 장소(접수대 등)에 게시하여야 한다.
※ 개인정보처리방침에 포함하여 게시해도 됨

【참고】 영상정보처리기기 운영 · 관리 방침은 영상정보처리기기(CCTV)의 운영책임기관 에서 수립하여 관리(예. 영상정보처리기기(CCTV)의 관리를 위탁 운영하는 경우라도 위탁자가 운영·관리 방침 수립 및 관리)</td></tr>
<tr><td>점검결과
선택방법</td><td colspan="3">① (양호) 점검기준 모두 준수
② (개선필요) 점검기준 준수 미흡
③ (취약) 점검기준 미준수
④ (해당없음) 영상정보처리기기(CCTV)가 없음</td></tr>
</table>

분 야	2. 개인정보의 처리제한		
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: 18**
판단기준 (해당여부)	※ 영상정보처리기기(CCTV)가 없는 경우는 해당 없음		
점검기준	※ 안내판 설치(필수 기재사항 ①~④ 포함)		
증빙자료	※ 동 항목은 별도의 증빙자료가 없어도 점검기준을 만족하는 경우에 점검결과를 양호로 선택하실 수 있습니다.		
관련근거	개인정보보호법 제25조(영상정보처리기기의 설치운영 제한)	**행정자치부 점검항목**	없음 (개인정보 점검 대상항목이 아님)
벌금과태료	1천만 원 이하 과태료		
세부설명	【설명】 의료기관이 공개된 장소에 영상정보처리기기(CCTV)를 설치·운영하는 경우 정보주체(환자)가 쉽게 인식할 수 있도록 안내판을 설치하여야 한다. 【참고】 안내판에 필수기재 하여야 할 사항 ① 설치 목적 및 장소 ② 촬영 범위 및 시간 ③ 관리책임자의 성명(또는 직책) 및 연락처 ④ (영상정보 처리기기CCTV) 설치·운영을 위탁한 경우) 수탁 관리자 성명(또는 직책)·업체명 및 연락처 ※ 의료기관의 진료실, 처치실, 수술실, 입원실, 행정사무실, 의무기록실, 전산소 등 출입에 제한이 있는 공간에 영상정보처리기기를 설치하여 개인영상 등을 수집하고자 하는 경우에는 정보주체의 수집·이용 동의를 받아야 함		
점검결과 선택방법	① **(양호)** 점검기준 모두 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 영상정보처리기기(CCTV)가 없으면 해당 없음		

분 야	2. 개인정보의 처리제한		
점검지표	2.3 영상정보처리기기 설치운영 제한		
점검항목	2.3.3 영상정보처리기기(CCTV)에 대한 이용 · 제공 · 열람 · 파기 내역을 기록하고 관리 하는가?		Seq: 19
판단기준 (해당여부)	※ 영상정보처리기기(CCTV)가 없는 경우는 해당 없음		
점검기준	※ 개인영상정보 관리대장 작성		
증빙자료	개인영상정보 관리대장		
관련근거	개인정보보호법 제25조(영상정보처리기기의 설치운영 제한)	행정자치부 점검항목	없음 (개인정보 점검 대상항목이 아님)
벌금과태료			
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 한다. - **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 함 - **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 【참고】 표준 개인정보 보호지침 제45조, 46조, 48조		
점검결과 선택방법	① **(양호)** 점검기준 모두 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 영상정보처리기기(CCTV)가 없으면 해당 없음		

분 야	2. 개인정보의 처리제한		
점검지표	2.3 영상정보처리기기의 설치운영 제한		
점검항목	2.3.4 영상정보처리기기(CCTV)가 분실·도난·유출·변조 또는 훼손 되지 아니하도록 안전성 확보조치를 하고 있는가?		Seq: 20
판단기준 (해당여부)	※ 영상정보처리기기(CCTV)가 없는 경우는 해당 없음		
점검기준	1. (점검항목 3.1.1)내부관리계획수립 (안전성 확보조치 사항 포함) ※ 소상공인의 경우 해당 없음 2. 영상정보처리기기(CCTV)보관 시설 마련 및 잠금장치 설치 3. 영상정보처리기기(CCTV)에 대한 접근통제		
증빙자료	1. 내부관리계획(안정성 확보조치 사항이 포함되어야 함) 2. 영상정보처리기기(CCTV) 접근통제 및 잠금장치 여부 ※ 동 항목은 별도의 증빙자료가 없어도 점검기준을 준수하는 경우에 점검결과를 양호로 선택하실 수 있습니다.		
관련근거	개인정보보호법 제25조(영상정보처리기기의 설치운영 제한)	행정자치부 점검항목	없음 (개인정보 점검 대상항목이 아님)
벌금과태료	2년 이하 징역 또는 2천만 원 이하 벌금, 3천만 원 이하의 과태료		
세부설명	【설명】 영상정보처리기기(CCTV)의 분실·도난·유출·변조 또는 훼손되지 않도록 개인영상정보의 안전성을 확보하고 조치하여야 한다. - 영상정보처리기기(CCTV)의 안전한 처리를 위한 내부 관리계획의 수립 및 시행(소상공인은 내부 관리계획을 수립하지 않아도 무방) · 소상공인 : 직원 수가 5인 미만인 기관 - 영상정보처리기기(CCTV)의 안전한 물리적 보관을 위한 보관시설 마련 또는 잠금장치 설치 - 영상정보처리기기(CCTV)에 대한 접근 통제 및 접근 권한의 제한		
점검결과 선택방법	① **(양호)** 점검기준 모두 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 영상정보처리기기(CCTV)가 없는 경우		

분 야	2. 개인정보의 처리제한		
점검지표	2.4 업무위탁에 따른 개인정보의 처리제한		
점검항목	2.4.1 위탁 계약 시 문서(계약서)에 의한 계약을 하였는가?		Seq: 21
판단기준 (해당여부)	※ 위탁하는 업무가 없으면 해당 없음 - 진료신청서 처리사무, 진료비 수납사무, 연말정산 사무, 각종 증명서 발급 사무 등 개인정보 처리업무 위탁 - 진료정보 위·수탁 업무 · 전자차트 및 청구S/W 등의 유지보수, 혈액검사, CCTV 운영, 홈페이지 운영, 처방전 보관/폐기 등		
점검기준	※ 보안요구사항이 포함된 위탁사업자별 계약서		
증빙자료	위탁사업자별 계약서(기재항목 ①~⑦이 포함된 위·수탁 계약서, 협약서, 특약서 등)		
관련근거	개인정보보호법 제26조(업무위탁에 따른 개인정보의 처리제한)	행정자치부 점검항목	10-1
벌금과태료	1천만 원 이하 과태료		
세부설명	【설명】 개인정보 처리 위탁문서(계약서)에 포함되어야 할 내용(개인정보보호법 제26조, 표준 개인정보 처리지침 제19조~20조) 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】 <법 제26조(업무위탁에 따른 개인정보의 처리 제한), 시행령 제28조(개인정보의 처리 업무 위탁 시 조치)> ※ 단순한 시스템 유지보수 등 직접적으로 개인정보를 처리하지 않더라도 수탁업체에서 관리자 권한 등을 통해 개인정보에 접근할 수 있는 업무는 개인정보 위탁업무로 보아야 함 ※ (점검항목 3.1.1)내부관리계획 또는 (점검항목 3.7.1)개인정보보호 처리방침 등에 수탁업체 관리·감독 및 교육계획 포함 여부 확인		
점검결과 선택방법	① **(양호)** 점검기준 모두 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 위탁하는 업무가 없음		

분 야	2. 개인정보의 처리제한		
점검지표	2.4 업무위탁에 따른 개인정보의 처리제한		
점검항목	2.4.2 수탁업체에 대한 교육 및 처리현황 점검 등 관리 감독을 실시하고 있는가?		Seq: 22
판단기준 (해당여부)	※ 위탁하는 업무가 없으면 해당 없음		
점검기준	1. 수탁업체에 대한 개인정보보호 교육을 실시하여야 한다. 2. 위탁한 개인정보처리 업무에 대해 수탁업체가 적절하게 처리하고 있는지를 점검·확인 하여야 한다.		
증빙자료	수탁업체 대상 관리·감독 및 개인정보보호 교육 결과		
관련근거	개인정보보호법 제26조(업무위탁에 따른 개인정보의 처리제한)	**행정자치부 점검항목**	없음 (권고사항)
벌금과태료	없음		
세부설명	【설명】 요양기관에서 개인정보를 처리하는 업무(전자차트 및 청구SW 유지보수, 혈액검사, 홈페이지 운영, CCTV운영 등)를 위탁하는 경우 **수탁업체 교육** - 정보주체(환자)의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 수탁자를 교육 ※ (점검항목 3.1.2)연간 개인정보보호 교육 계획에 따라 교육시행 ※ 수탁업체를 대상 교육이 현실적으로 어려운 경우 수탁업체의 자체 개인정보보호교육 이수 증빙서류 제출받아 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**"을 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**"을 제출 받아 보관하는 것으로 대신할 수 있음 【참고】 수탁자 선정 시 인력, 물적 시설, 재정능력, 기술력, 책임능력 등을 고려 (*손해배상책임에 대해 수탁자는 위탁기관의 직원으로 봄)		
점검결과 선택방법	① **(양호)** 점검기준 모두 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 위탁하는 업무가 없음		

분 야	2. 개인정보의 처리제한		
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: 23
판단기준 (해당여부)	※ 위탁하는 업무가 없으면 해당 없음 - 진료정보 위·수탁 업무 · 전자차트 및 청구S/W 등의 유지보수, 혈액검사, CCTV 운영, 홈페이지 운영, 처방전 보관/폐기 등		
점검기준	※ 위탁에 관한 사실을 공개(필수사항을 포함)		
증빙자료	다음중 하나의 증빙자료만 있어도 됨 ① 인터넷 홈페이지(운영 의료기관만 해당)공개내역 화면 ② 관보나 일반 일간 · 주간신문 또는 인터넷신문에 게재 ③ 환자에게 배포하는 각종 소식지(간행물, 소식지, 홍보지 또는 청구서)에 포함하여 연 2회 이상 발행 ④ 사업자의 보기 쉬운 장소인 접수실, 대기실 등에 게재 ⑤ 계약서 등에 실어 발급하는 방법		
관련근거	개인정보보호법 제26조(업무위탁에 따른 개인정보의 처리제한)	행정자치부 점검항목	10-2
벌금과태료	1천만 원 이하 과태료		
세부설명	【설명】 개인정보처리자(의료기관 담당자)는 위탁하는 업무의 내용과 수탁자를 정보주체가 언제든지 쉽게 확인 할 수 있도록 공개해야 한다. (개인정보보호법 시행령 제28조) - 공개 필수사항(위탁기관명, 위탁업무내용, 위탁기간) - 개인정보 처리 수탁자 담당자 연락처, 수탁자의 관리 현황 점검 결과 등 개인정보 처리 위탁에 관한 사항 ※ 표준 개인정보 보호지침 제19조(개인정보 처리방침의 기재사항) 제6호 참조		
점검결과 선택방법	① **(양호)** 점검기준 모두 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 위탁하는 업무가 없음		

분 야	2. 개인정보의 처리제한		
점검지표	2.5 개인정보 취급자에 대한 감독		
점검항목	2.5.1 개인정보취급자에 대한 보안 서약서를 제출토록 하였는가?		Seq: 24
판단기준 (해당여부)	※ 개인정보를 취급하는 직원(1인 운영 요양기관은 해당 없음) 및 수탁업체 직원이 없는 경우 해당 없음		
점검기준	1. 개인정보취급자로부터 보안서약서 수령 2. 수탁업체 담당직원으로부터 보안서약서 수령		
증빙자료	개인정보취급자 보안서약서(수탁업체 직원 포함)		
관련근거	개인정보보호법 제28조(개인정보 취급자에 대한 감독)	행정자치부 점검항목	없음 (권고사항)
벌금과태료	없음		
세부설명	【설명】 - 대표자(원장, 약국장)는 개인정보를 취급하는 직원에게 보안서약서를 제출하도록 하는 등 적절한 관리· 감독을 해야 함 - 직원의 인사이동 등에 따라 개인정보취급자의 업무가 변경되는 경우에는 지체 없이 개인정보에 대한 접근권한을 변경 또는 말소해야 함 - 수탁업무 계약서 작성 시 보안서약서를 같이 받으며 담당자의 변경이 발생하는 경우 수탁업체로부터 변경이력의 보고 및 보안서약서를 받아야 함 【참고】 표준개인정보보호지침 제18조(개인정보취급자에 대한 감독) ※ 개인정보취급자 : 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 임직원(대진의(약사), 파견근로자, 시간제근로자 포함) 등을 말함		
점검결과 선택방법	① **(양호)** 점검기준 모두 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 개인정보취급자(직원 및 수탁업체 직원)가 없는 경우		

분 야	2. 개인정보의 처리제한		
점검지표	2.5 개인정보 취급자에 대한 감독		
점검항목	2.5.2 개인정보취급자에 대한 정기적인 교육은 실시하고 있는가?		Seq: 25
판단기준 (해당여부)	※ 개인정보취급자에게 연1회 이상 개인정보보호 교육(사내교육, 외부교육, 위탁교육, 온라인교육)을 실시했는지 여부		
점검기준	점검기준 3.1.2의 연간 개인정보보호계획에 따라 교육시행 또는 자체 일정에 맞춰 교육시행		
증빙자료	개인정보보호 교육 결과[교육수료증, 사내교육(문서 및 교육 참석 서명록)]		
관련근거	개인정보보호법 제28조(개인정보 취급자에 대한 감독), 제29조(안전조치 의무), 제31조(개인정보 보호책임자의 지정)	**행정자치부 점검항목**	없음 (권고사항)
벌금과태료	없음		
세부설명	【설명】 대표자(원장, 약국장)는 취급자(직원)를 대상으로 매년 정기적으로 개인정보보호 교육을 실시하여야 한다. - 개인정보취급자가 개인정보를 훼손·침해·누설 할 경우에는 중벌에 처해지므로, 교육 시 이러한 점을 인식시키기 위해 노력해야하며, 개인정보 이용·제공 절차, 취급 시 주의사항, 침해사고 대응절차 등에 대해 교육 - 교육방법 : 기관의 환경을 고려하여 집합교육, 인터넷 교육, 외부교육과정 참석, 전문 강사초빙 등 다양한 방법을 활용 ※ Ex) 개인정보보호종합포털(www.privacy.go.kr) 등의 교육이수 - 교육대상 : 개인정보 및 관련설비(서버, PC, CCTV등)에 직간접적으로 접근하는 내부직원 및 외주용역업체 직원등 모든 인력포함 ※ 관련설비·장비가 위치한 장소에 접근할 수 있는 청소원, 경비원 등에게도 기본적인 정보보호 인식교육 수행 ※ 교육내용 및 방법에 관한 사항은 점검항목3.1.2의 점검지표의 이행으로 수립된 내부계획에 따라 시행 【참고】 교육 실적 확인 - 참석확인증, 수료증, 참석자 서명 등 포함 및 참석을 확인할 수 있는 증빙서류 - 대표자(원장, 약국장) 교육 참석 및 전달교육 여부		
점검결과 선택방법	① **(양호)** 점검기준 모두 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 개인정보취급자(직원 및 수탁업체 직원)가 없는 경우 해당 없음		

분 야	3. 개인정보의 안전한 관리		
점검지표	3.1 내부관리 계획수립 시행		
점검항목	3.1.1 내부관리 계획을 수립하고 필수사항을 포함하고 있는가?		Seq: 26
판단기준 (해당여부)	※ 소상공인(직원 수 5인 미만)에 해당하면 해당 없음		
점검기준	※ 내부관리계획을 수립(필수사항 ①~④포함)		
증빙자료	내부관리계획서(필수 반영 사항 포함)		
관련근거	개인정보보호법 제29조(안전조치 의무)	행정자치부 점검항목	11-1-1
벌금과태료	3천만 원 이하 과태료		
세부설명	【설명】 개인정보처리자(의료기관 담당자)가 개인정보를 안전하게 처리하기 위하여 내부 의사결정절차를 통하여 내부기준을 수립하여 시행하여야 함 - 내부관리계획 수립 시 필수 반영사항(①~⑤) 포함여부 확인 ① 개인정보 보호책임자의 지정에 관한 사항 ② 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항 ③ 개인정보의 안전성 확보에 필요한 조치에 관한 사항 ④ 개인정보취급자에 대한 교육에 관한 사항 ⑤ 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항 ⑥ 그밖에 개인정보 보호를 위하여 필요한 사항(예:개인정조파일 보유기간 등) 개인정보처리자(의료기관 담당자)는 각호의 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 함 【참고】 - 개인정보처리자 : 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말함 - 개인정보책임자 : 개인정보의 처리에 관한 업무를 총괄해서 책임지는 자 - 개인정보취급자 : 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 임직원(대진의(약사), 파견근로자, 시간제근로자 포함) 등을 말함		
점검결과 선택방법	① **(양호)** 점검기준 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 기준 [별표] 유형1		

분 야	3. 개인정보의 안전한 관리		
점검지표	3.1 내부관리 계획수립 시행		
점검항목	3.1.2 연간 개인정보보호 교육계획이 수립되어 있는가?		Seq: 27
판단기준 (해당여부)	※ 연간 개인정보보호 교육계획 수립 여부		
점검기준	※ 교육대상 및 목적에 따른 개인정보보호 교육계획을 수립		
증빙자료	개인정보보호 교육 계획 - 교육의 목적, 대상, 교육 내용, 일정 및 방법 등을 포함하여 수립		
관련근거	개인정보보호법 제29조(안전조치 의무)	행정자치부 점검항목	11-1-2
벌금과태료	1천만 원 이하 과태료		
세부설명	【설명】 개인정보보호 교육의 목적은 안전하게 개인정보가 관리될 수 있도록 개인정보 보호에 대한 인식을 제고시키고 개인정보보호 대책의 필요성을 이해시키는 것이다. 교육대상(일반직원, 개인정보취급자·담당자 등) 및 목적에 따라 교육내용을 차별화하고 일정 및 방법 등 구체적 사항을 명시해야 함 내부관리계획 또는 "○○년 개인정보보호 교육 계획(안)"과 같은 문서를 통해 관리하여야 함 - **교육대상** : 개인정보 및 관련설비(서버, PC, CCTV등)에 직·간접적으로 접근하는 내부직원 및 외주용역 업체 직원등 모든 인력포함 - **교육내용** : 개인정보보호의 중요성, 기관의 개인정보보호정책·지침·위험관리, 기술적·관리적 보호조치 기준 이행, 개인정보보호 업무의 절차·책임 등, 개인정보 취급관련 주의사항, 개인정보 침해 사고 대응절차 등 - **교육방법** : 기관의 환경을 고려하여 집합교육, 인터넷 교육, 외부 교육과정 참석, 전문 강사초빙 등 다양한 방법을 활용 - **수립시기** : 전년도말 혹은 당해 1/4분기 이내에 수립을 권장		
점검결과 선택방법	① **(양호)** 점검기준 모두 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 기준 [별표] 유형1		

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: 28
판단기준 (해당여부)	※ 개인정보처리시스템을 사용하지 않는 경우 해당 없음		
점검기준	1. 개인정보처리시스템 업무담당자별 접근권한 관리 2. 업무별 권한 관리대장 작성 및 관리 3. 업무담당자별 1인1계정 부여 (*계정공유금지)		
증빙자료	업무별 권한관리 대장		
관련근거	개인정보보호법 제29조(안전조치 의무)	행정자치부 점검항목	11-2-1, 11-2-4
벌금과태료	3천만원 이하 과태료		
세부설명	【설명】 개인정보처리자(의료기관 담당자)는 개인정보처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 업무담당자에 따라 차등 부여하여야 함 - 접근권한 : 판독(read), 기록(write), 실행(execution) 등 디렉토리 및 파일에 대해 사용자가 접근 및 수행할 수 있는 작업 권한 【참고】 업무담당자 별 1인 1계정 부여 여부 확인 접근권한 부여기준과 권한 승인절차 확인 업무별 권한리스트와 부여한 업무담당자의 직무 확인 - 개인정보처리시스템 : 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다. ※ 개인정보처리시스템 별로 접근권한자, 접근권한 부여기준, 권한승인절차, 접근권한 관리자 및 승인권자에 대한 내용이 포함 ※ 접근권한 차등부여를 확인할 수 있는 증빙자료(화면, 대장 등)		
점검결과 선택방법	① **(양호)** 점검기준 모두 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 기준 [별표] 유형1, 전자차트, 청구SW를 사용하지 않는 경우에는 해당 없음		

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 보관하는 절차를 마련하고 이를 실행하고 있는가?**		**Seq: 29**
판단기준 (해당여부)	※ 개인정보처리시스템을 사용하지 않는 경우 해당 없음		
점검기준	※ 업무별 접근권한관리 기록 보관(3년 이상)		
증빙자료	1. 업무별 권한관리(부여, 변경, 말소내역 포함) 대장 2. 위탁할 경우 증빙자료를 요청하여 보관		
관련근거	개인정보보호법 제29조(안전조치 의무)	**행정자치부 점검항목**	11-2-2, 11-2-3
벌금과태료	3천만 원 이하 과태료		
세부설명	【설명】 개인정보처리자(의료기관 담당자)는 개인정보의 안전성 확보조치 기준(제5조 제1항 및 제2항)에 의한 권한 부여·변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다. 【참고】 개인정보처리자(의료기관 담당자)는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자(의료기관 담당자)가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여야 한다. - 접근권한의 부여, 변경, 말소 관리대장 점검 및 DB접속권한 리스트 출력 요청 후 3년 간 보관 여부 확인 - 전산기능이 구현되어있지 않은 경우 상기기능에 대해서 위탁업체에 기능개발 요청 ※ 개인정보의 안전성 확보조치 기준(행정자치부고시 제2016-35호)		
점검결과 선택방법	① **(양호)** 점검기준 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 전자차트, 청구SW 등 개인정보처리시스템을 사용하지 않는 경우에는 해당 없음		

분 야	3. 개인정보의 안전한 관리		
점검지표	3.2 접근권한 관리 및 접근통제		
점검항목	3.2.3 안전한 비밀번호 작성규칙을 적용하고 있는가?		Seq: 30
판단기준 (해당여부)	※ PC가 없는 경우 해당 없음		
점검기준	※ 안전한 비밀번호 작성규칙(PC, 개인정보처리시스템, 홈페이지등) 준수		
증빙자료	※ 동 항목은 별도의 증빙자료가 없어도 점검기준을 준수하는 경우에 점검 결과를 양호로 선택하실 수 있습니다.		
관련근거	개인정보보호법 제29조(안전조치 의무)	행정자치부 점검항목	11-2-5
벌금과태료	3천만 원 이하 과태료		
세부설명	【설명】 개인정보처리자(의료기관 담당자)는 개인정보취급자(의료기관 담당자) 또는 정보주체(환자)가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야한다. 【참고】 안전한 비밀번호 작성규칙 ① 비밀번호 최소길이 - 비밀번호가 3가지 이상(영대문자, 숫자, 영소문자, 특수문자 등) 조합인 경우 8자리 - 비밀번호가 2가지 이상(영대문자, 숫자, 영소문자, 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 및 동일한 비밀번호 사용 제한 - 비밀번호를 최소 6개월마다 변경하여 동일한 비밀번호를 장기간 이용하지 않도록 관리 - 2개의 비밀번호를 교대로 사용하지 않도록 함 ④ 비밀번호 설정·변경할 때 입력 값의 자리수와 조합을 체크하여 안전한 비밀번호 작성규칙에 위배되는 경우, 법 위반을 알리고 작성규칙을 준수하도록 함 - 고객 불만 등으로 그 적용이 어려운 경우에는 최소한 법 위반 경고창을 통해 '비밀번호 작성규칙'을 준수하도록 유도함		
점검결과 선택방법	① **(양호)** 점검기준 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** PC가 없는 경우 해당 없음		

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: 31**
판단기준 (해당여부)	※ 개인정보시스템을 사용하지 않는 경우 해당 없음		
점검기준	1. (서버급 이상) 접근통제시스템 관련 HW 및 SW 설치 및 운영 2. (그 외 업무용 PC등) 백신, 방화벽 기능을 가진 SW(V3, 알약 등) 설치 및 점검		
증빙자료	※ 동 항목은 별도의 증빙자료가 없어도 점검기준을 준수하는 경우에 점검결과를 양호로 선택하실 수 있습니다.		
관련근거	개인정보보호법 제29조(안전조치 의무)	**행정자치부 점검항목**	11-2-6
벌금과태료	3천만 원 이하 과태료		
세부설명	**※ 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 3) 웹방화벽 (WAF) - http(80)프로토콜 기반으로 하는 취약점 공격만 탐지 및 차단 【설명】 1. 개인정보처리시스템에 대한 접속권한을 IP(Internet Protocol) 주소 등으로 제한하여 인가받지 않은 접근을 제한하여야 함 2. 개인정보처리시스템에 접속한 IP주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지하여야 함 3. 개인정보처리자(의료기관담당자)는 별도의 개인정보처리시스템을 이용하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 접근통제 기능을 이용할 수 있음 4. 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 함		
점검결과 선택방법	① **(양호)** 점검기준 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 개인정보처리시스템을 사용하지 않는 경우 해당 없음		

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 접속수단을 제공하고 있는가?		Seq: 32
판단기준 (해당여부)	※ 외부망과 연결되지 않은 서버만 운용 또는 서버 미운용 시 해당 없음		
점검기준	※ 가상사설망(VPN : Virtual Private Network) 또는 전용선 등의 안전한 접속 수단 제공		
증빙자료	※ 동 항목은 별도의 증빙자료가 없어도 점검기준을 준수하는 경우에 점검결과를 양호로 선택하실 수 있습니다.		
관련근거	개인정보보호법 제29조(안전조치 의무)	행정자치부 점검항목	11-2-7
벌금과태료	3천만원 이하 과태료		
세부설명	【설명】 - 외부망으로부터 개인정보처리시스템에 대한 접속은 원칙적으로 차단하여야 한다. 다만 개인정보처리자(의료기관 담당자)가 외부망을 통해 개인정보처리시스템에 접속이 필요한 경우에는 가상사설망(VPN : Virtual Private Network)또는 전용선 등의 안전한 접속수단을 적용하여야 한다. 【참고】 외부와 접속가능한 통신망 확인 후 VPN 또는 전용선 사용여부 확인 - **정보통신망:『전기통신기본법』제2조제2호에 따른 전기통신설비를** 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다. - 가상사설망(VPN : Virtual Private Network)은 개인정보취급자(의료기관담당자)가 사업장내의 개인정보처리시스템에 대해 원격으로 접속할 때 IPsec이나 SSL기반의암호프로토콜을 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 선택방법	① **(양호)** 점검기준 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 기준 [별표] 유형1, 외부망과 연결되지 않은 서버만 운용 또는 서버 미운용 시 해당 없음		

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: 33
판단기준 (해당여부)	※ PC가 없는 경우 해당 없음		
점검기준	(서버급 이상) 1. 침입차단 시스템의 설치 및 운영 2. 공유폴더 제거 (그 외 업무용 PC등) 1. 공유폴더 제거 및 비인가 프로그램 접속 차단		
증빙자료	침입차단시스템의 운영실적(탐지 및 차단정책 적용) ※ 자체서버를 보유하지 않은 경우에 한하여 동 항목은 별도의 증빙자료가 없어도 점검기준을 준수하는 경우에 점검결과를 양호로 선택하실 수 있습니다.		
관련근거	개인정보보호법 제29조(안전조치 의무)	행정자치부 점검항목	11-2-9
벌금과태료	3천만 원 이하 과태료		
세부설명	【설명】 개인정보처리자(의료기관 담당자)는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터 및 모바일 기기 등에 조치를 하여야 함 - **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 - **공개된 무선망 :** 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다. ※ 방화벽(V3) 또는 브라우저(IE)등을 통해 유해 사이트 차단 가능 【참고】 **(서버급이상)** · (점검항목 3.2.4) 점검항목의 침입차단시스템의 운영실적 보유 **(그 외 업무PC등)** PC만 사용하는 소규모 의료기관 · (공유폴더제거) 윈도우즈의 경우 "시작>제어판>성능 및 유지관리>관리도구>컴퓨터관리"의 공유폴더가 있는지 확인 ※ 보안취약 유해 사이트 : 메신저, P2P, 웹하드 등 ※ 비업무사이트 : 음란, 도박, 게임, 채팅, 증권 등		
점검결과 선택방법	① **(양호)** 점검기준 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** PC가 없는 경우 해당 없음		

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: 34
판단기준 (해당여부)	※ 홈페이지를 보유하지 않은 기관은 해당사항 없음		
점검기준	※ 홈페이지 개인정보 노출방지 점검 및 보완조치		
증빙자료	홈페이지 개인정보 노출방지 점검(웹 취약점 점검) 수행 및 결과		
관련근거	개인정보보호법 제29조(안전조치 의무)	행정자치부 점검항목	11-2-10
벌금과태료	3천만 원 이하 과태료		
세부설명	【설명】 고유식별정보(주민번호, 여권번호, 운전면허번호, 외국인등록번호)를 처리하는 개인정보처리자(의료기관담당자)는 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하여야 한다. 【참고】 홈페이지 개인정보 노출 진단 모니터링 방법(홈페이지 보유) 상용 개인정보 노출 진단 S/W를 이용하여 개인정보 노출 여부 모니터링 ※ 한국인터넷진흥원 원격취약점 점검서비스(www.kcert.or.kr)를 통해서도 웹 공격에 대한 취약점을 점검가능 ※ **웹 취약점 :** 고유식별정보등에 대한 보호를 제대로 하지 않으면 해커들에게 신분 도용 또는 다른 범죄를 수행하게 하기 위한 데이터로 제공될 수 있기 때문에 암호화와 같은 보호조치 또는 민감데이터의 노출 차단이 필요		
점검결과 선택방법	① **(양호)** 점검기준 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 기준 [별표] 유형1, 페이지를 보유하지 않은 경우 해당 없음		

분 야	3. 개인정보의 안전한 관리		
점검지표	3.2 접근권한 관리 및 접근통제		
점검항목	3.2.8 업무용 모바일 기기에 비밀번호 설정 여부		Seq: 35
판단기준 (해당여부)	업무용 모바일 기기 비밀번호 설정 되어 있는지 확인		
점검기준	※ 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치*를 하여야 함		
증빙자료	※ 동 항목은 별도의 증빙자료가 없어도 점검기준을 준수하는 경우에 점검결과를 양호로 선택하실 수 있습니다.		
관련근거	개인정보보호법 제29조(안전조치 의무)	행정자치부 점검항목	11-2-11
벌금과태료	3천만 원 이하 과태료		
세부설명	【설명】 * 비밀번호, 패턴, PIN 등을 이용한 화면잠금, 디바이스 암호화, USIM 카드 잠금 설정, 원격 잠금 및 데이터 삭제 등 ※ 업무용 모바일 기기의 분실에 따라 개인정보 유출되는 사례 있음		
점검결과 선택방법	① **(양호)** 점검기준 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 모바일기기가 없는 경우 해당 없음		

분 야	3. 개인정보의 안전한 관리		
점검지표	3.3 개인정보 암호화		
점검항목	3.3.1 비밀번호 및 바이오정보의 저장 시 암호화하고 있는가?		Seq: 36
판단기준 (해당여부)	비밀번호 및 바이오정보를 저장 시 암호화하는지 확인		
점검기준	※ 비밀번호 및 바이오정보의 암호화 처리 ※ 단, 비밀번호의 경우 일방향 암호화		
증빙자료	※ 동 항목은 별도의 증빙자료가 없어도 점검기준을 준수하는 경우에 점검결과를 양호로 선택하실 수 있습니다.		
관련근거	개인정보보호법 제29조(안전조치 의무)	행정자치부 점검항목	11-3-2
벌금과태료	3천만 원 이하 과태료		
세부설명	【설명】 비밀번호 및 바이오정보*를 저장 시 암호화하는지 확인 * 실별 및 인증 등의 고유기능에 사용되는 경우로 한정되며 콜센터 등 일반 민원 상담시 저장되는 음석기록이나 일반 사진 정보는 암호화 대상에서 제외 【참고】 - 바이오정보 : 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보 - 비밀번호 : 개인정보처리시스템, 업무용 컴퓨터 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 말함 ※ 개인을 식별하는 용도로 사용하는 바이오 정보는 암호화 대상에 해당 (지문, 얼굴, 홍채, 정맥, 음석, 필적 등) ※ CT영상 등 의료행위 관련 바이오정보는 암호화 대상에서 제외됨 ※ 개인정보처리자(요양기관 담당자)는 비밀번호를 암호화하여 저장하되 복호화 되지 아니하도록 일방향 암호화하여 저장하여야 함		
점검결과 선택방법	① **(양호)** 점검기준 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 개인정보를 보유하지 않은 경우는 해당 없음		

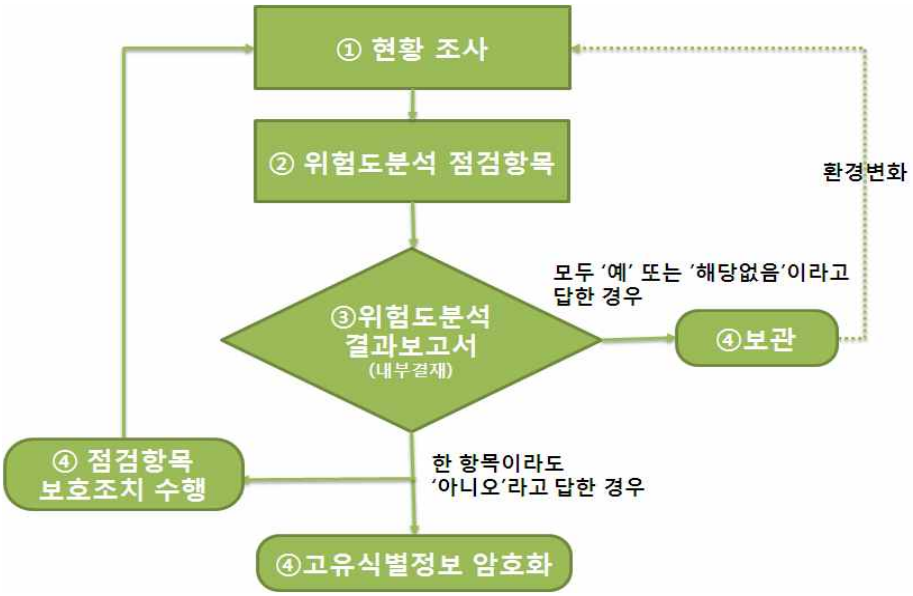
<table>
<tr><td>분 야</td><td colspan="3">3. 개인정보의 안전한 관리</td></tr>
<tr><td>점검지표</td><td colspan="3">3.3 개인정보 암호화</td></tr>
<tr><td>점검항목</td><td colspan="2">3.3.2 고유식별정보를 내부망에 저장 시 암호화 조치 또는 그에 상응하는 조치 적용 여부</td><td>Seq: 37</td></tr>
<tr><td>판단기준
(해당여부)
점검기준</td><td colspan="3">내부망에 고유식별정보를 저장하는 경우에는 암호화의 적용여부 및 적용 범위를 정하여 시행하고 있는지 확인</td></tr>
<tr><td>증빙자료</td><td colspan="3">암호화 조치 여부 확인 자료</td></tr>
<tr><td>관련근거</td><td>개인정보보호법
제29조(안전조치 의무)</td><td>행정자치부
점검항목</td><td>11-3-4</td></tr>
<tr><td>벌금과태료</td><td colspan="3">3천만 원 이하 과태료</td></tr>
<tr><td>세부설명</td><td colspan="3">【설명】 - 영향평가 대상이 되는 공공기관의 경우 개인정보영향평가의 결과에 따라 암호화 적용여부 및 범위를 정할 수 있음
- 영향평가 대상이 되는 공공기관의 경우를 제외하고는 위험도 분석에 따른 결과에 따라 암호화 적용여부 및 범위를 정함

< 개인정보 영향평가의 대상 >

① 구축·운용 또는 변경하려는 개인정보파일로서 5만명 이상의 정보주체에 관한 법 제23조에 따른 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일
② 구축·운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축·운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일
③ 구축·운용 또는 변경하려는 개인정보파일로서 100만명 이상의 정보주체에 관한 개인정보파일
④ 법 제33조 제1항에 따른 개인정보영향평가를 받은 후에 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하려는 경우 그 개인정보파일</td></tr>
</table>

< 위험도 분석 절차 및 내용 >

① 위험도 분석을 위해 개인정보 파일 및 고유식별정보 보유 여부 등 현황조사
② 개인정보 파일단위별로 위험도 분석 항목별 점검을 수행
③ 위험도 분석 결과보고서를 작성하여 내부결재 후 보관
④ 점검 결과에 따라 고유식별정보 암호화 등을 수행



구 분	점 검 항 목
DB 및 Application 기반	12. 상시적으로 네트워크를 통한 비인가자의 DB 접근을 통제하고 있습니까?
	13. DB서버 내에 불필요한 서비스 포트를 차단하고 있습니까?
	14. 상시적으로 DB 접속자 및 개인정보취급자의 접속기록을 남기고 있습니까?
	15. DB 접속기록을 주기적으로 모니터링하여 통제하고 있습니까?
	16. DB서버에 접속하는 관리자 PC가 인터넷 접속되는 내부망의 네트워크와 분리되어 있습니까?
	17. 개인정보취급자의 역할에 따라 DB 접근권한을 차등화하여 부여하고 있습니까?
	18. 개인정보취급자의 전보, 이직, 퇴사 등 인사이동 발생 시 지체 없이 DB 접근권한을 변경하고 있습니까?
	19. DB접속자 및 개인정보취급자의 DB 로그인 비밀번호를 최소 3개월마다 변경하고 있습니까?

		20. DB접속자 및 개인정보취급자의 비밀번호 입력 시 5회 이상 연속 입력오류가 발생한 경우 계정 잠금 등 접근을 제한하고 있습니까?
		21. DB 및 DB접속 어플리케이션 서버에 대한 물리적 접근을 인가된 자로 한정하고 있습니까?
		22. DB 및 DB접속 어플리케이션 서버에서 보조기억매체(USB 등) 사용 시 관리자 승인 후 사용하고 있습니까?
		23. DB서버 및 DB접속 어플리케이션 서버에 접속하는 모든 개인정보 취급자의 단말기(PC, 노트북 등)의 운영체제 보안패치를 제조사 공지 후 지체 없이 수행하고 있습니까?
		24. HDD등 DB 저장매체의 불용 처리 시(폐기, 양여, 교체 등) 저장매체에 저장된 개인정보는 모두 파기하고 있습니까?
	웹(Web) 기반 ※웹사이트 운영시	25. 신규 웹 취약점 및 알려진 주요 웹(Web) 취약점 진단/보완을 년1회 이상 실시하거나, 상시적으로 비인가자에 의한 웹서버 접근, 홈페이지 위·변조 등을 자동으로 차단할 수 있는 보호 조치를 하고 있습니까?
		26. 웹서버 프로그램과 운영체제 보안패치를 제조사 공지 후 지체 없이 수행하고 있습니까?
점검결과 선택방법	① **(양호)** 점검기준 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)**	

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 암호하고 있는가?**		**Seq: 38**
판단기준 (해당여부) 점검기준	고유식별정보, 비밀번호 및 바이오정보를 정보통신망을 통하여 내·외부로 송·수신하거나 보조저장매체 등을 통해 전달하는 경우에 이를 암호화하는지 확인		
증빙자료	고육식별정보, 비밀번호 등 에 대한 암호화 여부 확인 자료		
관련근거	개인정보보호법 제29조(안전조치 의무)	**행정자치부 점검항목**	11-3-1
벌금과태료	3천만 원 이하 과태료		
세부설명	【설명】 고유식별정보, 비밀번호 및 바이오정보를 정보통신망을 통하여 내·외부로 송·수신하거나 보조저장매체 등을 통해 전달하는 경우에 이를 암호화하는지 확인 【참고】 비밀번호와 바이오정보는 반드시 암호화해야 함 ※ wire shark 등 프로그램을 통해 전송되는 패킷의 암호화 검사 시 암호화하지 않은 사례 있음		
점검결과 선택방법	① **(양호)** 점검기준 모두 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 개인정보처리시스템이 없거나 보조저장 매체를 통해서 송·수신하지 않는 경우 해당 없음		

분 야	3. 개인정보의 안전한 관리		
점검지표	3.3 개인정보 암호화		
점검항목	3.3.4 고유식별정보, 비밀번호 및 바이오정보를 암호화하여 저장 시 안전한 암호알고리즘 사용 여부 확인		Seq: 39
판단기준 (해당여부)	개인정보처리시스템에 고유식별정보, 비밀번호, 바이오정보를 암호화하여 저장 시, 안전한 암호알고리즘을 사용해야함		
점검기준	안전한 암호 알고리즘 확인		
증빙자료	안전한 암호 알고리즘 확인 자료		
관련근거	개인정보보호법 제29조(안전조치 의무)	행정자치부 점검항목	11-3-5
벌금과태료	3천만 원 이하 과태료		
세부설명	【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		
점검결과 선택방법	① **(양호)** 점검기준 모두 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)**		

분 야	3. 개인정보의 안전한 관리		
점검지표	3.3 개인정보 암호화		
점검항목	3.3.5 고유식별정보의 인터넷과 내부망의 중간지점(DMZ) 저장시 암호화하고 있는가?		Seq: 40
판단기준 (해당여부) 점검기준	고유식고유식별정보를 인터넷 구간 및 인터넷 구간과 내부망의 중간지점(DMZ)에 저장하는 경우 암호화하여 저장하는지 확인 저장하는 경우 암호화하여 저장하는지 확인		
증빙자료	DMZ 저장시 암호화 여부 확인 자료		
관련근거	개인정보보호법 제29조(안전조치 의무)	행정자치부 점검항목	11-3-3
벌금과태료	3천만 원 이하 과태료		
세부설명	【설명】 고유식별정보를 인터넷 구간 및 인터넷 구간과 내부망의 중간지점(DMZ)에 저장하는 경우 암호화하여 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 선택방법	① **(양호)** 점검기준 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 인터넷 구간(DMZ 포함) 등에 있는 고유식별정보가 없음		

분 야	3. 개인정보의 안전한 관리		
점검지표	3.3 개인정보 암호화		
점검항목	3.3.6 고유식병정보를 업무용 컴퓨터 또는 모바일 기기에 저장시 안전한 암호화 알고리즘 사용 여부 확인		Seq: 41
판단기준 (해당여부)	고유식별정보를 업무용 컴퓨터 또는 모바일 기기에 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용		
점검기준			
증빙자료			
관련근거	개인정보보호법 제29조(안전조치 의무)	행정자치부 점검항목	11-3-6
벌금과태료	3천만 원 이하 과태료		
세부설명	【설명】고유식별정보를 업무용 컴퓨터 또는 모바일 기기에 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용 ※ 안전한 암호알고리즘, 암호화 방식 등은 "개인정보 암호화 조치 안내서" 참조 ※ 개인정보보호 종합지원포털(http://www.privacy.go.kr)에서 다운로드 가능 ☞ 안전하지 않은 알고리즘(MD5, SHA-1, 자체 함수제작 등) 및 양방향 암호화 방식으로 암호화한 사례 있음		
점검결과 선택방법	① **(양호)** 점검기준 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)**		

분 야	3. 개인정보의 안전한 관리		
점검지표	3.4 접속기록 보관		
점검항목	3.4.1 개인정보취급자의 접속기록을 최소 6개월 이상 보관하여 관리하고 있는가?		Seq: 42
판단기준 (해당여부)	※ 개인정보처리시스템이 없는 경우 해당 없음		
점검기준	※ 개인정보취급자의 접속기록을 최소 6개월 이상 보관 및 관리		
증빙자료	※ 접속기록 보관 및 백업에 관한 정책 또는 관리규정 - 위탁운영을 하는 경우 : 해당업체에 확인 후 증빙자료 제출 요구		
관련근거	개인정보보호법 제29조(안전조치 의무)	행정자치부 점검항목	11-4-1, 11-4-2, 11-4-3
벌금과태료	3천만 원 이하 과태료		
세부설명	【설명】 1. 개인정보처리시스템(전자차트, 청구S/W 등)에 접속한 기록이 위·변조 및 도난, 분실되지 않도록 접속한 기록을 최소 6개월 이상 보관·관리하여야 한다. - 접속기록 : 개인정보취급자등이 개인정보처리시스템에 접속하여 수행한 업무내역에 대하여 식별자, 접속일시, 접속자를 알 수 있는 정보, 수행업무 등 접속한 사실을 전자적으로 기록한 것을 말함 2. 개인정보처리시스템을 위탁·운영하는 경우 업체에 6개월 이상 보관되고 있는지 업체에 증빙 자료를 받아야 함 3. 개인정보처리자(의료기관 담당자)는 개인정보의 유출·변조·훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 반기별로 1회 이상 점검하여야 함 ※ **접속기록의 항목(4개)** : ID, 날짜 및 시간, 접속자 IP주소, 수행업무 (열람, 수정, 삭제, 인쇄, 입력 등)		
점검결과 선택방법	① **(양호)** 점검기준 모두 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 개인정보처리시스템이 없는 경우 해당 없음		

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: 43
판단기준 (해당여부)	※ 개인정보처리시스템이 없는 경우 해당 없음		
점검기준	※ 개인정보처리시스템(전자차트, 청구S/W 등)에 접속한 기록은 위·변조 및 도난, 분실되지 않도록 안전하게 보관해야 한다.		
증빙자료	접속기록 보관 및 백업에 관한 정책 또는 관리규정		
관련근거	개인정보보호법 제29조(안전조치 의무)	행정자치부 점검항목	11-4-4
벌금과태료	3천만 원 이하 과태료		
세부설명	【설명】 대표자(원장, 약국장)은 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 함 【참고】 개인정보의 안전성 확보조치 기준고시 제8조 1. 접속기록 위·변조 방지 방법 - 접속기록을 백업하여 개인정보처리시스템 이외의 보조저장매체나 별도의 저장장치에 보관(CD, DVD, 등과 같은 덮어쓰기 방지 매체 사용 권장) 2. 접속기록을 안전하게 보관하는 방법 - 별도 지정된 장소(통제구역), 금고 또는 잠금 장치가 있는 캐비넷(보관함) 등에 보관 3. 개인정보처리시스템을 자체 개발·운영하는 경우 해당 시스템의 접속기록을 위와 같은 위·변조 방지 방법으로 저장하고 안전하게 보관 4. 개인정보처리시스템을 위탁 운영하는 경우 해당업체에 관련 증빙자료(접속기록을 별도의 보조저장매체나 저장장치에 분리 보관 여부)를 요청하여 확인		
점검결과 선택방법	① **(양호)** 점검기준 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 개인정보처리시스템이 없는 경우 해당 없음		

분 야	3. 개인정보의 안전한 관리		
점검지표	3.5 보안프로그램 설치운영		
점검항목	**3.5.1 개인정보처리시스템이 설치된 업무용 PC에 백신 프로그램 등의 최신 보안 프로그램을 설치하여 관리하고 있는가?**		**Seq: 44**
판단기준 (해당여부)	※ PC를 보유하지 않는 경우 해당 없음		
점검기준	※ 최신 보안 프로그램 설치		
증빙자료	※ 동 항목은 별도의 증빙자료가 없어도 점검기준을 준수하는 경우에 점검결과를 양호로 선택하실 수 있습니다.		
관련근거	개인정보보호법 제29조(안전조치 의무)	**행정자치부 점검항목**	11-5-1
벌금과태료	3천만 원 이하 과태료		
세부설명	【설명】 개인정보처리자(의료기관 담당자)는 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 ※ 심평원 DUR 프로그램을 업무용 PC에 상시 실행시켜두는 것으로 백신을 설치한 것으로 할 수 있음 【참고】 개인정보의 안전성 확보조치 기준 제9조(악성프로그램 등 방지) - **보안 프로그램** : 인정된 사용자만이 단말기나 기타 주변기기를 통해서 파일에 접근할 수 있도록 조정하는 프로그램 - **백신 소프트웨어** : 컴퓨터 바이러스 프로그램을 찾아내고 손상된 파일을 치료하는 소프트웨어 - **악성 프로그램** : 컴퓨터바이러스와 달리 다른 파일을 감염시키지는 않지만, 악의적인 용도로 사용될 수 있는 유해 프로그램, 트로이목마, 스파이웨어, 원격관리 프로그램, 해킹툴, 악성 자바스크립트 등이 해당 ※ 백신S/W는 항상 활성화 시켜두고, 월 1회 이상의 정기적 검사를 하는 것을 권장		
점검결과 선택방법	① **(양호)** 점검기준 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** PC를 보유하지 않는 경우 해당 없음		

분 야	3. 개인정보의 안전한 관리		
점검지표	3.5 보안프로그램 설치운영		
점검항목	3.5.2 보안프로그램을 정기적(일 1회 이상)으로 업데이트 하는가?		Seq: 45
판단기준 (해당여부)	※ PC를 보유하지 않는 경우 해당 없음		
점검기준	※ 보안프로그램의 최신 상태 유지 - 자동업데이트 기능 혹은 일 1회 이상의 업데이트 실시		
증빙자료	※ 동 항목은 별도의 증빙자료가 없어도 점검기준을 준수하는 경우에 점검결과를 양호로 선택하실 수 있습니다		
관련근거	개인정보보호법 제29조(안전조치 의무)	행정자치부 점검항목	11-5-2
벌금과태료	3천만 원 이하 과태료		
세부설명	【설명】 개인정보의 안전성 확보조치 기준 제9조(악성프로그램 등 방지) 1. (업무용 PC) 보안 프로그램의 자동 업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지하여야 함 2. (서버용 보안프로그램) 최신업데이트가 있는 경우 USB 또는 업데이트 서버를 활용하여 최신업데이트 상태 유지 3. 악성프로그램관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시하여야 함 【참고】 보안프로그램의 자동업데이트 기능을 설정하거나 일 1회 이상 업데이트를 통해 최신상태를 유지하고 있는지 확인 - 보안프로그램의 환경설정 또는 업데이트 설정에서 자동업데이트 기능 설정		
점검결과 선택방법	① **(양호)** 점검기준 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** PC를 보유하지 않는 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: 46
판단기준 (해당여부)	※ 진료를 하지 않거나 홈페이지 등을 통해 개인정보를 수집하지 않는 경우 해당 없음		
점검기준	1. 출입통제 절차를 수립 2. 절차에 따라 출입관리 대장을 작성		
증빙자료	전산실 • 자료보관실 출입통제 절차(절차가 반영된 규정, 계획), 출입통제 관리대장		
관련근거	개인정보보호법 제29조(안전조치 의무)	행정자치부 점검항목	11-6-1
벌금과태료	3천만원 이하 과태료		
세부설명	【설명】 개인정보처리자는 전산실, 원무실, 의무기록실 및 그밖의 문서보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다. **※ 출입통제절차 예시** 방문자 방문 → 방문자 신분확인 → 출입관리 대장작성 → 담당직원 동행입실 → 출입관리대장(퇴실시간) 작성 → 업무종료 후 잠금확인 【참고】 출입 통제절차 - 통제구역 설정, 통제구역 시건장치 또는 지정된 자만 출입 가능 여부, 출입자 명부 작성 여부 등		
점검결과 선택방법	① **(양호)** 점검기준 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 개인정보를 보관하지 않는 경우 해당 없음		

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: 47
판단기준 (해당여부)	※ 진료를 하지 않거나 홈페이지 등을 통해 개인정보를 수집하지 않는 경우 해당 없음		
점검기준	※ 개인정보가 포함된 서류, 보조저장매체는 사람이 쉽게 접근할 수 없는 곳에 보관하여야한다. - 별도 지정된 통제구역, 금고, 잠금장치가 있는 보관함에 보관		
증빙자료	1. 개인정보 내부관리계획 및 안전한 보관 절차가 반영된 규정 또는 계획서 2. 잠금장치가 설치된 장소 사진 등		
관련근거	개인정보보호법 제29조(안전조치 의무)	행정자치부 점검항목	11-6-2
벌금과태료	3천만 원 이하 과태료		
세부설명	【설명】 1. 개인정보처리자(의료기관 담당자)는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 함 2. 개인정보처리자(의료기관 담당자)는 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하여야 함 다만 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있음		
점검결과 선택방법	① **(양호)** 점검기준 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 개인정보를 보관하지 않는 경우 해당 없음		

분 야	3. 개인정보의 안전한 관리		
점검지표	3.7 개인정보 처리방침의 수립 및 공개		
점검항목	3.7.1 개인정보처리방침을 수립하고 있는가?		Seq: 48
판단기준 (해당여부)	※ 필수사항		
점검기준	※ 개인정보 처리방침 수립		
증빙자료	※ 개인정보처리방침 수립을 확인할 수 있는 자료		
관련근거	개인정보보호법 제30조(개인정보 처리방침의 수립 및 공개)	행정자치부 점검항목	12-1, 12-2
벌금과태료	1천만 원 이하 과태료		
세부설명	【설명】 표준 개인정보 보호지침 제37조에 따르면 다음 각 호의 사항이 포함된 개인정보처리방침을 정하여야 한다.(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 정보주체의 권리 · 의무 및 그 행사방법에 관한사항 ⑥ 처리하는 개인정보의 항목 ⑦ 개인정보의 파기에 관한사항 ⑧ 개인정보보호 책임자에 관한사항 ⑨ 개인정보 처리방침의 변경에 관한 사항 ⑩ 시행령 제30조제1항에 따른 개인정보의 안전성 확보조치에 관한 사항 【참고】 개인정보 처리방침의 작성지침(행자부 고시 참조)		
점검결과 선택방법	① **(양호)** 점검기준 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 진료를 하지 않는 기관으로 개인정보를 전혀 수집하지 않는 경우 해당 없음		

분 야	3. 개인정보의 안전한 관리		
점검지표	3.7 개인정보 처리방침의 수립 및 공개		
점검항목	3.7.2 개인정보처리방침을 홈페이지 또는 보기 쉬운 장소(접수대, 대기실 등)에 공개하고 있는가?		Seq: 49
판단기준 (해당여부)	※ 필수 사항		
점검기준	※ 개인정보 처리방침 공개		
증빙자료	다음중 하나의 증빙자료만 있어도 됨 ① 홈페이지(운영 의료기관만 해당)공개내역 화면 또는 URL ② 접수실, 대기실 등에 게재 ③ 해당 공개 방법을 확인할 수 있는 자료		
관련근거	개인정보보호법 제30조(개인정보 처리방침의 수립 및 공개)	행정자치부 점검항목	12-3
벌금과태료	1천만 원 이하 과태료		
세부설명	【설명】 개인정보보호법 시행령 제31조 - 개인정보처리방침은 정보주체(환자)가 언제든지 쉽게 확인할 수 있도록 인터넷 홈페이지 등을 통해 공개하여야 함 - 홈페이지에 공개 할 수 없는 경우에는 다음의 방법 가운데 하나 이상의 방법으로 공개하여야 함. 또한, 이 경우에도 "개인정보처리방침"이라는 명칭을 사용하되, 글자 크기나 색상 등을 활용하여 다른 고지사항과 구분함으로써 정보주체가 쉽게 확인할 수 있도록 하여야 함 ① 개인정보처리자의 사업장등의 보기 쉬운 장소에 게시하는 방법 ② 관보(개인정보처리자가 공공기관인 경우만 해당한다)나 개인정보처리자의 사업장등이 있는 시·도 이상의 지역을 주된 보급지역으로 하는 「신문 등의 진흥에 관한 법률」 제2조제1호가목·다목 및 같은 조 제2호에 따른 일반일간신문, 일반주간신문 또는 인터넷신문에 싣는 방법 ③ 같은 제목으로 연 2회 이상 발행하여 정보주체에게 배포하는 간행물·소식지·홍보지 또는 청구서 등에 지속적으로 싣는 방법 ④ 재화나 용역을 제공하기 위하여 개인정보처리자와 정보주체가 작성한 계약서 등에 실어 정보주체에게 발급하는 방법 【참고】 행정자치부 개인정보보호 지침 Ⅲ-2 개인정보처리방침 공개 참조 개인정보처리방침을 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 한다.		
점검결과 선택방법	① **(양호)** 점검기준 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 선택 불가		

분 야	3. 개인정보의 안전한 관리		
점검지표	3.8 개인정보보호책임자의 지정		
점검항목	3.8.1 개인정보보호책임자가 지정되고 그 역할이 정의되어 있는가?		Seq: 50
판단기준 (해당여부)	※ 필수 사항		
점검기준	1. 개인정보보호책임자가 자격요건에 맞게 지정 2. 개인정보보호책임자의 역할 정의		
증빙자료	개인정보보호책임자 지정 및 역할 확인이 가능한 문서 (다음 중 택일 하여 증빙) - 내부관리계획, 업무 분장표, 직제표, 개인정보처리방침 등		
관련근거	개인정보보호법 제31조(개인정보보호 책임자의 지정)	행정자치부 점검항목	13-1
벌금과태료	1천만 원 이하 과태료		
세부설명	【설명】 대표자(원장)은 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보보호책임자를 지정하여야 함 또한, 적절한 책임·권한·역할을 정의하여야 함 - **개인정보보호책임자의 지정요건** 가. 사업주 또는 대표자 나. 임원(임원이 없는 경우에는 개인정보 처리 관련 업무를 담당하는 부서의 장) ※ 사업주 또는 대표자가 아닌 경우에는, 인사 발령 등 공식적인 지정 절차 필요 【참고】 **< 개인정보 보호책임자의 업무 >** ① 개인정보 보호 계획의 수립 및 시행 ② 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선 ③ 개인정보 처리와 관련한 불만의 처리 및 피해 구제 ④ 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축 ⑤ 개인정보 보호 교육 계획의 수립 및 시행 ⑥ 개인정보파일의 보호 및 관리·감독 ⑦ 개인정보 처리방침 수립·변경 및 시행 ⑧ 개인정보 보호 관련 자료의 관리 ⑨ 처리목적이 달성되거나 보유기간이 경과한 개인정보 파기 ⑩ 개인정보침해 관련 민원의 접수·처리 ⑪ 개인정보취급자가 등록 또는 변경등록 신청한 개인정보파일의 등록 또는 변경등록 사항의 적정성에 대한 판단 및 행정자치부 등록 ⑫ 그 밖에 개인정보 보호를 위하여 필요한 업무		
점검결과 선택방법	① **(양호)** 점검기준 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 선택불가		

분 야	3. 개인정보의 안전한 관리		
점검지표	3.8 개인정보 보호책임자의 지정		
점검항목	3.8.2 개인정보보호 전담조직과 적정인력을 운영하고 있는가?		Seq: 51
판단기준 (해당여부)	※ 진료를 하지 않거나 홈페이지 등을 통해 개인정보를 수집하지 않는 경우 해당 없음		
점검기준	1. 개인정보보호 전담조직 구성 및 운영 2. 개인정보보호 담당자 지정 ※ 소규모 의원, 약국의 경우 2번 항목만 준수해도 양호로 인정		
증빙자료	1. 업무분장표 또는 인사명령 등 조직 구성과 구성원 역할 확인이 가능한 문서 2. 개인정보보호 담당자가 명시되어 있는 개인정보처리방침 등		
관련근거	개인정보보호법 제31조(개인정보보호 책임자의 지정)	행정자치부 점검항목	없음 (권고사항)
벌금과태료	없음		
세부설명	【설명】 개인정보보호 활동을 수행하고 관리하는 인력들에 대한 책임, 권한 및 역할을 정의하여야 한다. **개인정보보호 업무를 총괄하여 수행할 수 있는 조직을 지정·운영**하여 개인정보보호에 관한 예산 및 인력을 운영할 수 있도록 개인정보보호 업무담당자에게 책임과 권한을 부여한다. ※ 소규모 의원, 약국의 경우 현실적으로 전담조직 마련이 어려우므로 담당자 지정만으로 운영 【예시】 개인정보보호 전담팀(총괄)을 구성하여 정책을 일관성 있게 추진·수행하며, 업무별로(홈페이지분야, DB분야, 민원분야 등) 담당자를 지정·운영 【참고】 개인정보보호 전담조직 구성 및 전담인력 확보 - 전담인력 : 개인정보보호 업무만을 전담하는 인력 - 담당인력 : 타 업무와 개인정보보호 업무를 병행하는 인력		
점검결과 선택방법	① **(양호)** 점검기준 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 진료를 하지 않거나 홈페이지 등을 통해 개인정보를 수집하지 않는 경우 해당 없음		

<table>
<tr><td>분 야</td><td colspan="3">3. 개인정보의 안전한 관리</td></tr>
<tr><td>점검지표</td><td colspan="3">3.8 개인정보 보호책임자의 지정</td></tr>
<tr><td>점검항목</td><td colspan="2">3.8.3 개인정보보호책임자는 교육 및 관리·감독 등 역할을 수행하고 있는가?</td><td>Seq: 52</td></tr>
<tr><td>판단기준
(해당여부)
점검기준</td><td colspan="3">1. 개인정보보호책임자의 교육이수
2. 관리·감독 활동 수행</td></tr>
<tr><td>증빙자료</td><td colspan="3">1. 개인정보 보호책임자 교육 이수 실적
- 교육 참석확인증, 수료증 등
2. 개인정보 보호책임자 관리·감독 및 제도개선 활동 실적</td></tr>
<tr><td>관련근거</td><td>개인정보보호법
제31조(개인정보보호 책임자의 지정)</td><td>행정자치부
점검항목</td><td>없음
(권고사항)</td></tr>
<tr><td>벌금과태료</td><td colspan="3">없음</td></tr>
<tr><td>세부설명</td><td colspan="3">【설명】 개인정보 보호책임자 역할
개인정보보호 책임자는 기관(사업자)의 개인정보보호 총괄 업무를 수행할 수 있도록 분야별 전문기술 교육뿐만 아니라 개인정보 보호 관련 법률 및 제도, 사내 규정 등 알고 있어야 한다.

【참고】 동법 시행령 제32조 제1항(개인정보 보호책임자의 업무 및 지정요건 등)
개인정보보호책임자 교육이수
- 기관의 환경을 고려하여 집합교육, 인터넷 교육, 외부교육과정 참석, 전문 강사초빙 등 다양한 방법을 활용
ex) 개인정보보호종합포털(www.privacy.go.kr) 등의 교육이수
· 일반직원 대상 직장교육의 단순 참석은 인정하지 않음
개인정보 보호책임자 관리·감독
- 보호책임자 주관 개인정보 처리실태 점검, 개인정보파일 점검, 개인정보처리시스템 점검 활동 등
- 주민번호 미 수집 관련 서식개선, 개인정보보호 관련 회의 주재 등의 개선 활동</td></tr>
<tr><td>점검결과
선택방법</td><td colspan="3">① (양호) 점검기준 준수
② (개선필요) 점검기준 준수 미흡
③ (취약) 점검기준 미준수
④ (해당없음) 선택불가</td></tr>
</table>

<table>
<tr><td>분 야</td><td colspan="3">3. 개인정보의 안전한 관리</td></tr>
<tr><td>점검지표</td><td colspan="3">3.8 개인정보 보호책임자의 지정</td></tr>
<tr><td>점검항목</td><td colspan="2">3.8.4 개인정보보호 활동을 수행하는데 필요한 예산을 반영하고 있는가?</td><td>Seq: 53</td></tr>
<tr><td>판단기준
(해당여부)</td><td colspan="3">※ 진료를 하지 않는 의료기관 중 개인정보를 수집 하지 않는 경우 해당없음</td></tr>
<tr><td>점검기준</td><td colspan="3">※ 개인정보보호 예산 반영 권장항목에 따른 예산 반영</td></tr>
<tr><td>증빙자료</td><td colspan="3">1. 당해 연도 개인정보보호 예산 편성 내역
2. 개인정보보호 관련 예산집행 증빙 자료</td></tr>
<tr><td>관련근거</td><td>개인정보보호법
제31조(개인정보보호 책임자의 지정)</td><td>행정자치부
점검항목</td><td>없음
(권고사항)</td></tr>
<tr><td>벌금과태료</td><td colspan="3">없음</td></tr>
<tr><td>세부설명</td><td colspan="3">【설명】 개인정보보호 활동을 수행하는데 필요한 예산을 적절하게 반영하여 지속적인 개인정보보호 업무를 추진하도록 한다.
별도의 전산시스템(서버급)구축한 의료기관의 경우
- 개인정보보호 교육 및 관리 감독
- 개인정보가 유출하지 않도록 보안시스템 등에 예산을 반영하여 개인정보보호 활동 수행
별도의 전산시스템(서버급)구축하지 못한 의료기관의 경우
- 소속기관의 상황에 따라 예산 수립여부를 결정할 수 있음
※ 단, 백신프로그램 설치 및 개인정보보호 교육은 필수 시행

【참고】 개인정보보호 예산 반영 필수항목
1. 개인정보보호 교육·홍보 예산
- 집합교육, 인터넷 및 그룹웨어 교육
- 외부 전문기관 및 전문 강사 초빙교육비
2. 관리·감독, 컨설팅, 모니터링 예산
- 운영시설, 위탁업체 등에 대한 관리·감독 수행
- 개인정보처리시스템 모니터링 비용
3. 보안시스템(F/W, IDS, IPS, UTM 등) 도입·운영 예산
- 개인정보보호를 위한 시스템(H/W·S/W) 개발, 도입·교체, 운영, 유지보수비
4. 백신S/W 도입·운영 예산
- 업무용 PC, 서버 등에 설치·운영하는 백신S/W 관련 도입·운영 비용</td></tr>
<tr><td>점검결과
선택방법</td><td colspan="3">① (양호) 점검기준 준수
② (개선필요) 점검기준 준수 미흡
③ (취약) 점검기준 미준수
④ (해당없음) 진료를 하지 않는 의료기관 중 개인정보를 수집 하지 않는 경우 해당 없음</td></tr>
</table>

분 야	3. 개인정보의 안전한 관리		
점검지표	3.9 개인정보 유출방지 등		
점검항목	3.9.1 개인정보 노출방지를 위한 모니터링 및 정기점검을 실시하고 있는가?		Seq: 54
판단기준 (해당여부)	※ 진료를 하지 않는 요양기관 중 개인정보를 수집 하지 않는 경우 해당 없음		
점검기준	1. 개인정보 노출방지 2. 취약점 정기적 점검 ※ 홈페이지 개인정보 노출진단, PC점검, 보안진단의 날 운영 등		
증빙자료	1. 홈페이지 개인정보 노출방지 점검, 웹 취약점 점검 등 수행 결과 2. 업무용 PC에 대한 개인정보 노출방지 점검 활동 수행 결과		
관련근거	개인정보보호법 제29조(안전조치 의무)	행정자치부 점검항목	없음 (권고사항)
벌금과태료	없음		
세부설명	【설명】 홈페이지를 통해 개인정보가 노출되는 것을 막기 위해 노출방지 시스템을 구축하여 운영하거나 기관 내 홈페이지들에 대하여 개인정보 노출여부 및 취약점 점검 등을 정기적으로 실시하여 개인정보 노출을 예방하여야 한다. 또한, 점검결과 노출이 발견되었거나 취약점이 발견된 경우에는 후속 조치를 수행하여 위협을 제거하여야 한다. **홈페이지 개인정보 노출 진단 모니터링 방법(홈페이지 보유)** - 상용 개인정보 노출 진단 S/W(또는 심평원 제공 무료 홈페이지 개인정보 노출 진단 서비스)를 이용하여 개인정보 노출 여부 모니터링 【참고】 컴퓨터(PC)에 개인정보 노출방지 점검 항목 - 바이러스 백신 프로그램 설치 및 실행 - 운영체제, MS 오피스 최신 보안 패치 - 로그인 패스워드(9자리 이상) 설정 - 화면 보호기 설정 등 ※ 위의 항목은 예시이며 의료기관 환경에 따라 가감하여 사용 ※ 월 1회 이상 정기점검을 권장		
점검결과 선택방법	① **(양호)** 점검기준 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 진료를 하지 않는 의료기관 중 개인정보를 수집 하지 않는 경우 해당 없음		

분 야	3. 개인정보의 안전한 관리		
점검지표	3.9 개인정보 유출방지 등		
점검항목	3.9.2 개인정보 유·노출 등 침해사고 발생에 대한 대응절차를 수립하였는가?		Seq: 55
판단기준 (해당여부)	※ 진료를 하지 않는 의료기관 중 개인정보를 수집 하지 않는 경우 해당 없음		
점검기준	※ 필수항목(4가지)을 포함하는 개인정보 침해사고 대응절차 수립 ① 침해사고 시 조치방법 ② 업무분장 및 연락체계 ③ 유출통지 등 침해구제 방법 ④ 침해신고 방법		
증빙자료	개인정보 침해사고 대응 절차, 지침		
관련근거	개인정보보호법 제34조(개인정보 유출통지 등)	행정자치부 점검항목	없음 (권고사항)
벌금과태료	없음		
세부설명	【설명】 개인정보 유·노출 및 침해사고를 통하여 발생할 수 있는 사회적, 경제적 피해 등 2차 피해를 예방하기 위하여 개인정보 침해사고 대응 범위, 절차, 담당자·부서별 업무, 피해구제 방법, 비상연락망·연락체계 등 침해사고 대응절차 마련이 필요하다. 【참고】 시행령 제40조(개인정보 유출 통지의 방법 및 절차) - 개인정보 침해사고 대응절차 수립 시 필수항목 ① 침해사고 시 조치방법 ② 업무분장 및 연락체계 ③ 유출통지 등 침해구제 방법 ④ 침해신고 방법 - 개인정보 침해사고 대응체계 구축 여부가 중요하므로 필수항목 중 ②업무분장 및 연락체계는 필히 점검 - 침해사고 대응절차 모의훈련 실시, 사내 정보시스템(인트라넷) 게시 등을 통해 개인정보취급자들이 침해사고 대응절차를 숙지하고 사고 발생 시 신속하고 효율적으로 대응할 수 있는 체계를 구축하도록 함		
점검결과 선택방법	① **(양호)** 점검기준 준수 ② **(개선필요)** 점검기준 준수 미흡 ③ **(취약)** 점검기준 미준수 ④ **(해당없음)** 진료를 하지 않는 의료기관 중 개인정보를 수집 하지 않는 경우 해당 없음		

[별표]

사업자 규모 및 유형, 개인정보 보유량에 따른 사업자의 유형

회사 규모 등	개인정보 보유량 (정보주체 수)	유형
소상공인(상시근로자 5인 미만), 단체, 개인	1만명 미만	유형1
	1만명 이상	유형2
중소기업	100만명 미만	유형2
	100만명 이상	유형3
중견기업, 대기업	10만명 미만	유형2
	10만명 이상	유형3

※ 단, 100만명 이상 정보주체의 개인정보를 보유한 단체는 "유형3"에 해당됨

내부관리계획에 포함되어야 하는 필수 사항

내부관리계획 포함 사항	유형별 적용 여부		
	유형1	유형2	유형3
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

▶ 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