2021년도 개인정보 보호 자율점검(병원급 의료기관)

〈 대한병원협회 〉

대한병원협회는「개인정보 보호법」제5조제3항, 제13조제2호, 제4호 및 제5호와 같은 법 시행령 제14조에 따라 병원급 의료기관을 대표하는 자율규제 단체입니다.

「개인정보보호 자율규제단체 지정 등에 관한 규정」제10조에 의거, 개인정보 자율점검을 실시하오니 자율점검에 대해 적극 협조 및 성실하게 점검하여 주시기 바랍니다.

□ 기관현황

<table>
<tr><th>병원명</th><th>법인명
(사업등록증상)</th><th>사업자등록번호</th><th>병원코드</th><th>요양기관코드</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>종별</td><td colspan="2">청구S/W 자체개발 유/무</td><td colspan="2">청구 S/W 외주시
업체명 / 프로그램(버전)</td></tr>
<tr><td rowspan="3"></td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="2">전자의무기록시스템 인증 유/무</td><td colspan="2">인증 형태(제품/사용) 및
업체명/프로그램명(버전)</td></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="3">주소</td><td colspan="2">개인정보 처리자 유형</td></tr>
<tr><td colspan="3"></td><td colspan="2"></td></tr>
</table>

- 병원명 / 법인명 : 병원명으로 기재 / 사업등록증상에 기재된 내용으로 기재
- 병원코드 : 병원협회에서 생성된 코드 기재 [*병원협회 홈페이지(www.kha.or.kr) 코드조회 이용]
- 종별 : 의료기관 개설허가증에 기재된 내용으로 기재
- 개인정보처리자 유형 : 병원이 보유한 전체 개인정보 보유건수 기준

개인정보처리자 유형 참고	
유형1 (완화)	1만명 미만의 정보주체에 관한 개인정보를 보유한 소상공인, 단체, 개인
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
유형3 (강화)	10만명 이상의 정보주체에 관한 개인정보를 보유한 대기업, 중견기업, 공공기관 100만명 이상의 정보주체에 관한 개인정보를 보유한 중소기업, 단체

□ 개인정보 보호 책임자 및 담당자 현황

개인정보 보호 책임자			개임정보 보호 담당자(작성자)				
부서 및 직책	성명	연락처	부서 및 직책	성명	연락처	이메일	팩스번호

- 개인정보 보호책임자 : 개인정보 보호책임자는 *자격요건을 갖춘 공식적으로 임명된 자
(개인정보 처리방침에 기재된 자와 동일하여야 함)

*** 개인정보 보호책임자 자격요건은『개인정보 보호법 시행령』제32조 제2항 참조**

□ 개인정보시스템별 개인정보 처리 현황

개인정보 처리시스템 명	개인정보 파일	구분	목적	개인정보 보유량	처리하는 개인정보 항목
ex) 홈페이지 시스템	홈페이지 회원	온라인	홈페이지 회원관리	190,350 명	이름, 생년월일, 성별
xx 시스템	xxx 파일	오프라인	고객 문의 사항 응대	540 명	이름, 연락처, 이메일주소

- 개인정보 처리시스템 : 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템과 연결되어 업무에 이용되는 시스템을 말하며, 본 점검 대상에서는 내부 직원의 개인정보 만을 관리하는 시스템 및 파일은 제외
- 개인정보 파일 : 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합체
- 개인정보 보유량(명) : 개인정보처리시스템별 보유하고 있는 개인정보 보유량

※ 병원이 보유한 개인정보처리시스템을 개인정보 보유량이 많은 순으로 모두 작성(표가 부족한 경우, 행을 삽입하여 작성)

※ '처리하는 개인정보 항목' 기재 시 "~등"으로 표기하지 않고 처리하는 모든 개인정보 항목을 기재

※ 사망자 제외

□ 고유식별정보 보유 현황

고유식별정보	보유현황
주민등록번호	(건)
여권번호	(건)
운전면허번호	(건)
외국인등록번호	(건)
합계	**(건)**

- 고유식별정보 보유현황 : 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호 보유건 작성

□ 개인정보 자율점검 이행 유의사항

○ 자율점검표는 거짓 없이 작성하는 것이 원칙

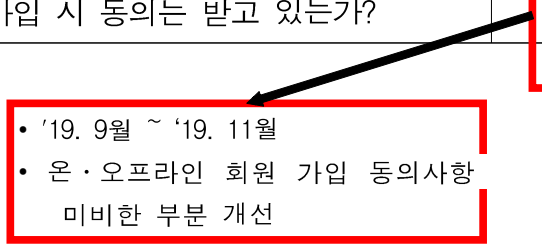
○ 점검표 항목 중 개선 필요 사항에 대하여 개선계획 성실 작성

- 개선기한* 등을 명확히 제시

※ 개선기한 수립은 최장 1년을 권장

<참고. 자율점검표 작성 예시>

순번	법조항	점검항목	양호	개선필요	개선계획(개선기한)	해당없음
1	제15조 제22조	1.1.1 진료목적 외로 서면가입(오프라인)·홈페이지 (온라인) 등을 통한 회원 가입 시 동의는 받고 있는가?		O		



○ **『정보통신망 이용촉진 및 정보보호 등에 관한 법률』제47조(정보보호 관리체계의 인증), 『개인정보보호법』제32조의2(개인정보 보호 인증) 및 『정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시』(개인정보보호위원회고시 제2020-13호)에 따른 정보보호 관리체계(ISMS) 인증 및 개인정보보호 관리체계(ISMS-P) 인증을 취득한 병원은 개인정보 보호 자율점검표 점검항목 중 ISMS 제외 표시 항목 점검 제외**

□ 참고자료

[참고 1] 『대한병원협회 개인정보보호 자율점검표 참고자료』대한병원협회 2021. 06.
(다운로드 위치 : 대한병원협회 홈페이지 > 협회업무 > 총무국

[참고 2] 『개인정보보호 법령 및 지침·고시 해설』개인정보 보호위원회 2020. 12.
(다운로드 위치 : 개인정보종합포털 홈페이지 > 자료마당 > 지침자료

[참고 3] 『개인정보의 안전성 확보조치 기준 해설서』개인정보 보호위원회, 한국인터넷진흥원 2020. 12.
(다운로드 위치 : 개인정보종합포털 홈페이지 > 자료마당 > 지침자료

[참고 4] 『개인정보의 기술적·관리적 보호조치 기준 해설서』개인정보 보호위원회, 한국인터넷진흥원 2020. 12.
(다운로드 위치 : 개인정보종합포털 홈페이지 > 자료마당 > 지침자료

[참고 5] 『개인정보 수집 최소화 가이드라인』개인정보 보호위원회, 한국인터넷진흥원 2020. 12.
(다운로드 위치 : 개인정보종합포털 홈페이지 > 자료마당 > 지침자료

[참고 6] 『개인정보의 암호화 조치 안내서』개인정보 보호위원회, 한국인터넷진흥원 2020. 12.
(다운로드 위치 : 개인정보종합포털 홈페이지 > 자료마당 > 지침자료

□ 자율규제단체 현장확인 신청(별도 안내 · 접수)

- 자율규제단체 현장확인은 회원병원의 원활한 자율점검을 진행하였는지에 대하여 현장을 방문하여 자율점검 항목별 증빙자료 확인 및 병원내 개인정보 취약점 확인, 개인정보보호 활동에 대한 컨설팅 등 원활한 개인정보보호 자율점검을 지원하기 위한 절차임
- 자율규제규약 제1장 5번..바 병원협회 소속 회원사의 참여 제한에 따라 병원협회의 개선이행 확인 및 허위 확인을 위한 최근 5년 이내 현장확인을 받지 않은 경우 자율규제단체 참여가 제한될 수 있음

□ 개인정보보호 자율점검표 (62개 점검항목)

순번	법조항	점검항목	양호	개선필요	개선계획(개선기한)	해당없음	법조항/처벌
1	【2021년 중점점검항목】						
	제15조 제22조	1.1.1 진료목적 외로 서면가입(오프라인)·홈페이지 (온라인) 등을 통한 회원 가입 시 동의는 받고 있는가?					제15조 미동의 수집(5천만원 이하 과태료) 동의, 동의사항 누락(3천만원 이하 과태료)
2	제15조	1.1.2 각종 게시판, 기타 개인정보 수집 시 동의는 받고 있는가?					제15조 미동의 수집(5천만원 이하 과태료) 동의, 동의사항 누락(3천만원 이하 과태료)
3	【2021년 중점점검항목】						
	제16조	1.2.1 목적에 필요한 최소한의 개인정보 수집하고 있는가?					제16조개인정보의 수집 제한(3천만원 이하 과태료)
4	【2021년 중점점검항목】						
	제16조	1.2.2 최소한 정보 외의 개인정보 수집에 대한 미동의를 이유로 재화 또는 서비스 제공 거부하고 있지는 않는가?					제16조개인정보의 수집 제한(3천만원 이하 과태료)
5	제22조	1.2.3 진료 목적 외로 만 14세 미만 아동의 개인정보를 처리 시, 법정대리인의 동의 여부					제22조 (5천만원 이하 과태료)
6	제29조	1.2.4 모바일앱의 기기 접근권한 고지 및 동의를 받고 있는가?					망법 제22조의2
7	제29조	1.2.5 모바일앱의 기기 접근권한에 대한 동의받을 경우, 필수적/선택적 접근권한을 구분하고, 동의 철회 방법과 기능을 제공하고 있는가?					망법 제22조의2 (3천만원 이하 과태료)
8	제29조	1.2.6 모바일앱을 제공하기 위하여 선택적 접근권한을 설정하는데 이용자가 동의하지 아니한다는 이유로 이용자에게					망법 제22조의2 (3천만원 이하 과태료)

		해당 서비스 제공을 거부하고 있지는 않는가?					
	【2021년 중점점검항목】						
9	제17조 제18조 제22조	1.3.1 제3자에게 개인정보 제공 및 목적 외 이용 시 정보주체(환자)의 별도 동의는 받고 있는가?					제17조, 제18조 미동의 제공(5년 이하의 징역 또는 5천만원 이하 벌금) 동의, 동의사항 누락(3천만원 이하 과태료)
10	제18조	1.4.1 개인정보를 목적 외로 이용하거나 제3자에게 제공하는 경우, 해당 내용을 기록하고 관리하는가? (공공의료기관)					제18조 (5천만원 이하 과태료)
11	제21조	1.5.1 진료목적 등으로 수집한 개인정보 보유기간 경과, 처리목적(제공받는 경우 제공받는 목적) 달성 후 지체 없이 개인정보를 파기(복구 또는 재상되지 않도록 조치)하고 관리대장을 작성하여 관리하고 있는가?					제21조 (3천만원 이하 과태료)
12	제21조	1.5.2 임시파일 및 출력자료 등은 목적달성 후 즉시 파기 하고 있는가?					제21조 (3천만원 이하 과태료)
13	제21조	1.5.3 타 법령에 따라 보존하는 경우 개인정보를 별도로 분리보관하고 있는가?					제21조 (1천만원 이하 과태료)
14	제39조	1.5.4 진료목적 외의 정보통신서비스 중 1년의 기간동안 이용하지 아니한 이용자의 개인정보를 보호하기 위하여 파기 또는 분리 별도 저장 관리 하는가?					제39조의6 (3천만원 이하 과태료)
15	제 28조의 4	1.5.5 가명정보를 처리하는 경우 추가정보를 별도로 분리하여 보관/관리하는 등 해당 정보가 분실/도난/유출/위조/변조 또는 훼손되지 않도록 기술적/관리적/물리적 조치를 하고 있는가?				ISMS 제외	제28조의4 (3천만원 이하 과태료)
16	제23조	2.1.1 민감정보의 동의에 의한 수집 및 제공 시 개인정보 수집 동의와 별도로 구분하여 동의 받고 있는가? (관련 법령에서 구체적으로 허용한 경우는 동의없이 처리 가능)					제23조 (5년 이하의 징역 또는 5천만원 이하 벌금)
17	제24조	2.2.1 고유식별정보(운전면허번호, 여권번호, 외국인등록번호) 수집 시 개인정보 수집 동의와 별도로 구분하여 동의를 받고 있는가?				ISMS 제외	제24조 (5년 이하의 징역 또는 5천만원 이하 벌금)

		(관련 법령에서 구체적으로 허용한 경우는 동의없이 처리 가능)					
18	제24조의 2	2.2.2 법률, 대통령령에 구체적으로 허용한 경우에 주민등록번호를 수집하고 있는가?				ISMS 제외	제24조의2 (3천만원 이하 과태료)
19	제24조의 2	2.2.3 주민등록번호 외 회원가입 방법 제공 여부					제24조의2 (3천만원 이하 과태료)
20	제25조	2.3.1 영상정보처리기기(CCTV) 운영·관리 방침을 수립하고 있는가?				ISMS 제외	제25조영상정보처리기기(5천만원이하 과태료)
21	제25조	2.3.2 영상정보처리기기(CCTV)를 설치한 장소에 정보주체가 영상정보 처리기기(CCTV) 설치 사실을 인지할 수 있도록 필수기재 사항을 포함한 안내판을 설치하고 있는가?					제25조 (1천만원 이하 과태료)
22	제25조	2.3.3 영상정보처리기기(CCTV)에 대한 이용 · 제공 · 열람 · 파기 내역을 기록하고 관리 하는가?					제25조
23	제25조	2.3.4 영상정보처리기기(CCTV)가 분실·도난·유출·변조 또는 훼손되지 아니하도록 안전성 확보조치를 하고 있는가?				ISMS 제외	제25조 (3천만원 이하 과태료)
24	제26조	2.4.1 위탁 계약 시 문서(계약서)에 의한 계약을 하였는가?				ISMS 제외	제26조 (1천만원 이하 과태료)
25	제26조	2.4.2 수탁업체에 대한 교육 및 처리현황 점검 등 관리 감독을 실시하고 있는가?				ISMS 제외	제26조
26	제26조	2.4.3 위탁에 관한 사실을 인터넷 홈페이지 또는 사보, 접수실, 대기실 등에 공개하고 있는가?				ISMS 제외	제26조 (1천만원 이하 과태료)
27	제28조	2.5.1 개인정보취급자에 대한 보안 서약서를 제출하도록 하고 있는가?				ISMS 제외	제28조
28	제28조	2.5.2 개인정보취급자에 대한 정기적인 교육은 실시하고 있는가?				ISMS 제외	제28조

29	제29조	3.1.1 개인정보의 안전한 처리를 위한 내부 관리계획을 수립 및 시행하고 내부 관리계획의 이행 실태를 연1회 이상 점검·관리하고 있는가?				ISMS 제외	제29조 (3천만원 이하 과태료) 유형 1은 제외
30	제29조	3.2.1 개인정보처리시스템에 대한 접근 권한을 최소한의 범위로 업무담당자에 따라(1인 1계정) 차등 부여하였는가?				ISMS 제외	제29조 (3천만원 이하 과태료) 유형 1은 제외
31	제29조	3.2.2 개인정보처리시스템 접근 권한의 부여・변경・말소 내역의 기록 관리를 최소 3년간 보관하는 절차를 마련하고 이를 실행하고 있는가?				ISMS 제외	제29조 (3천만원 이하 과태료)
32	제29조	3.2.3 안전한 비밀번호 작성규칙을 적용하고 있는가?				ISMS 제외	제29조 (3천만원 이하 과태료)
33	제29조	3.2.4 계정정보(ID) 또는 비밀번호(PW)를 일정 횟수 이상 잘못 입력한 경우 접근을 제한하는가?				ISMS 제외	제29조 (3천만원 이하 과태료) 유형 1은 제외
34	제29조	3.2.5 개인정보취급자가 일정 시간 이상 업무처리를 하지 않는 경우 시스템 접속 차단하고 있는가?				ISMS 제외	제29조 (3천만원 이하 과태료) 유형 1은 제외
35	제29조	3.2.6 개인정보처리시스템에 대하여 불법적인 접근 및 침해사고를 방지하기 위한 접근통제시스템을 설치/운영하고 있는가?				ISMS 제외	제29조 (3천만원 이하 과태료)
36	제29조	3.2.7 외부에서 정보통신망을 통하여 접속할 때 가상 사설망(VPN), 전용선 등 안전한 접속 수단이나 안전한 인증 수단을 적용하고 있는가?				ISMS 제외	제29조 (3천만원 이하 과태료) 유형 1은 제외
37	제29조	3.2.8 P2P, 공유설정, 공개된 무선망 이용 등을 통하여 개인정보가 유·노출 되지 않도록 접근 통제 등에 관한 조치를 하고 있는가?				ISMS 제외	제29조 (3천만원 이하 과태료)
38	제29조	3.2.9 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연1회 이상 취약점 점검하고 필요한 보완 조치를 하고 있는가?				ISMS 제외	제29조 (3천만원 이하 과태료) 유형 1은 제외
39	제29조	3.2.10 업무용 모바일 기기에 비밀번호를 설정하고 있는가?				ISMS 제외	제29조 (3천만원 이하 과태료)
40	제29조	3.3.1 비밀번호 및 바이오정보의 저장				ISMS	제29조 (3천만원 이하

		시 안전한 암호 알고리즘을 적용하여 암호화하고 있는가? (비밀번호는 일방향 암호화 저장)				제외	과태료)
41	제29조	3.3.2 고유식별정보(주민등록번호 제외)를 내부망에 저장 시 암호화 조치 또는 그에 상응하는 조치를 적용하고 있는가? (주민등록번호는 반드시 안전한 암호 알고리즘을 적용하여 암호화 저장)				ISMS 제외	제29조 (3천만원 이하 과태료)
42	제29조	3.3.3 고유식별정보, 비밀번호 및 바이오정보를 정보통신망을 통하여 송·수신하거나 보조저장매체를 통하여 전달 시 암호하고 있는가?				ISMS 제외	제29조 (3천만원 이하 과태료)
43	제29조	3.3.4 고유식별정보의 인터넷과 내부망의 중간지점(DMZ) 저장 시 안전한 암호 알고리즘을 적용하여 암호화하고 있는가?				ISMS 제외	제29조 (3천만원 이하 과태료)
44	제29조	3.3.5 고유식별정보를 업무용 컴퓨터 또는 모바일 기기에 저장시 안전한 암호화 알고리즘을 적용하고 있는가?				ISMS 제외	제29조 (3천만원 이하 과태료)
45	제29조	3.3.6 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용 보관, 배포 및 파기 등에 관한 절차 수립·시행 하였는가?				ISMS 제외	제29조 (3천만원 이하 과태료) 유형 1, 2는 제외
46	제29조	3.4.1 개인정보취급자의 접속기록을 1년 이상 보관 및 점검하여 관리하고 있고 월1회 이상 점검하고 있는가? (5만명 이상 개인정보를 처리하거나 고유식별정보 또는 민감정보를 처리하는 경우 2년)				ISMS 제외	제29조 (3천만원 이하 과태료)
47	제29조	3.4.2 접속기록의 위·변조 및 도난, 분실되지 않도록 접속 기록을 안전하게 보관하고 있는가?				ISMS 제외	제29조 (3천만원 이하 과태료)
48	제29조	3.5.1 백신 소프트웨어 등의 보안 프로그램을 설치하고 자동 업데이트 또는 일 1회 이상 업데이트를 실시·운영하여 발견된 악성프로그램 등에 대해 삭제 등을 하고 있는가?				ISMS 제외	제29조 (3천만원 이하 과태료)
49	제29조	3.6.1 인가받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도				ISMS 제외	제29조 (3천만원 이하 과태료)

		록 조치하고 있는가?					
50	제29조	3.6.2 관리용 단말기가 본래 목적 외로 사용되지 않도록 조치 하고 있는가?				ISMS 제외	제29조 (3천만원 이하 과태료)
51	제29조	3.6.3 관리용 단말기에 악성 프로그램 감염 방지 등을 위한 보안 조치하고 있는가?				ISMS 제외	제29조 (3천만원 이하 과태료)
52	제29조	3.7.1 전산실, 자료보관실 등 물리적 보관 장소에 대한 출입통제절차를 수립하여 운영하고 있는가?				ISMS 제외	제29조 (3천만원 이하 과태료)
53	제29조	3.7.2 개인정보가 포함된 서류, 보조저장 매체 등을 잠금장치가 있는 안전한 장소에 보관하고 있는가?				ISMS 제외	제29조 (3천만원 이하 과태료)
54	제29조	3.7.3 개인정보가 포함된 서류, 보조저장 매체의 반출·입 통제를 위한 보안 대책을 마련하고 있는가?				ISMS 제외	제29조 (3천만원 이하 과태료)
55	제29조	3.8.1 재해·재난 발생 대비 개인정보처리시스템 보호를 위한 대응절차 및 백업·복구 계획을 마련하고 있는가?				ISMS 제외	제29조 (3천만원 이하 과태료) 유형 1,2는 제외
56	제30조	3.9.1 개인정보처리방침을 수립하고 있는가?				ISMS 제외	제30조 (1천만원 이하 과태료)
57	제30조	3.9.2 개인정보처리방침을 홈페이지 또는 보기 쉬운 장소(접수대, 대기실 등)에 공개하고 개정사항 안내/개시 및 이전 버전의 처리방침을 공개하고 있는가?				ISMS 제외	제30조 (1천만원 이하 과태료)
58	제31조	3.10.1 개인정보보호책임자가 지정되고 그 역할이 정의되어 있는가?				ISMS 제외	제31조 (1천만원 이하 과태료)
59	제31조	3.10.2 개인정보보호 전담조직과 적정 인력을 운영하고 있는가?				ISMS 제외	-
60	제31조	3.10.3 개인정보보호책임자는 교육 및 관리 · 감독 등 역할을 수행하고 있는가?				ISMS 제외	제31조
61	제31조	3.10.4 개인정보보호 활동을 수행하는데 필요한 예산을 반영하고 있는가?				ISMS 제외	-
62	제39조	4.10.1 손해배상책임 의무가입 대상일 경우 법에 명시된 최소적립금액 이상으로 보험 또는 공제에 가입하거나 준비금을 적립하였는가?					제39조(2천만원 이하과태료)