

**개인정보보호
자율규제 규약
(병원급 의료기관)**

2020. 08.

대한병원협회 개인정보 보호 자율규제 규약

제1장 총칙

1. 목적	1
2. 용어의 정의	1
3. 개인정보 보호 원칙	2
4. 관련 법령의 준수	3
5. 자율규제단체	3
6. 회원사의 권리	5
7. 자율규제 규약	5

제2장 개인정보 처리단계별 조치기준

1. 개인정보의 수집·이용	6
2. 개인정보 제3자 제공	8
3. 개인정보 처리 업무위탁	10
4. 영업의 양도	11
5. 영상정보처리기기의 설치·운영	12
6. 개인정보파일의 등록	14
7. 개인정보의 안전성 확보조치	15
8. 개인정보의 파기	20
9. 개인정보 처리방침의 수립 및 공개	21
10. 개인정보 보호책임자 지정	21
11. 정보주체의 권익보호	22
12. 피해 구제방법	25

제3장 별첨

1. 각종 서식	27
2. 벌칙 및 과태료 규정	45

개인정보보호 자율규제 규약

2017. 2. 23. 제정
2018. 07. 19. 개정
2019. 05. 16. 개정
2019. 10. 24. 개정
2020. 08. 04. 개정

제1장 총칙

1. 목적

이 규약은 관련규정에 따라 대한병원협회(이하“병원협회”라 한다)와 그 회원사가 수행하는 개인정보 보호 및 자율규제 활동에 관한 사항을 정함으로써 회원사의 개인정보 보호 수준을 제고하고 개인정보 관련 분쟁을 예방하기 위한 내용을 정함을 그 목적으로 한다.

▶ 관련규정

- ① 개인정보 보호법 제5조제3항, 제13조제2호, 제4호 및 제5호
- ② 개인정보 보호법 시행령 제14조
- ③ 개인정보보호 자율규제단체 지정 등에 관한 규정(이하‘자율규제단체지정 규정’이라 한다)
(행정안전부고시 제2019-8호)

2. 용어의 정의

이 규약에서 사용하는 용어의 뜻은 다음과 같다.

- ① “개인정보”란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.
- ② “정보주체”란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
- ③ “회원사”란 「의료법」 제3조제2항 제3호에 따른 병원급 의료기관 중 병원, 요양병원, 종합병원을 말한다.
- ④ “의료인”이란 보건복지부장관의 면허를 받은 의사·치과의사·한의사·조산사 및 간호사를 말한다.
- ⑤ “진료정보”란 진료를 목적으로 수집하여 처리하는 개인정보가 포함된 정보로 진료기록부, 수술기록부, 조산기록부, 간호기록부, 환자명부 등으로 관리되는 정보를 말하고, 사망한 자의

진료정보도 포함한다.

⑥“개인정보의 처리”란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 이와 유사한 행위를 말한다.

⑦“개인정보파일”이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물을 말한다.

⑧“영상정보처리기기”란 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 일체의 장치로써 개인정보 보호법 시행령 제3조에 따른 폐쇄회로 텔레비전(CCTV) 및 네트워크 카메라를 말한다.

⑨“개인정보처리자”란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.

⑩“개인정보 보호책임자”란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지거나 업무처리를 최종적으로 결정하는 자로서, 개인정보 보호법(이하 “법”이라 한다) 제31조(개인정보 보호책임자의 지정)에 따른 지위에 해당하는 자를 말한다.

⑪“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.

⑫“내부관리 계획”이란 회원사의 개인정보를 안전하게 처리하기 위하여 내부 의사결정 절차를 통하여 수립·시행하는 내부 기준을 말한다.

⑬“자율규제 협의회”란 「개인정보보호 자율규제단체 지정 등에 관한 규정」 제4조에 따라 행정안전부장관이 자율규제단체 지정 등에 관한 업무를 위하여 구성·운영하는 협의회를 말한다.

⑭“접속기록”이란 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무내역에 대하여 개인정보취급자 등의 계정, 접속일시, 접속지 정보, 처리한 정보 주체 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우 “접속”이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신 가능한 상태를 말한다

3. 개인정보 보호 원칙

병원협회와 회원사는 다음의 원칙을 준수하면서 개인정보 보호 관련 업무 및 활동을 한다.

① 처리목적의 명확화 원칙

회원사는 개인정보의 처리 목적을 명확하게 하여야 함

② 최소수집의 원칙

회원사는 개인정보의 처리 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 함

③ 적법한 수집 원칙

회원사는 개인정보를 적법하고 정당하게 수집하여야 함

④ 목적 외 이용금지 원칙

회원사는 처리목적에 직접적으로 필요한 범위 내에서 적합하게 개인정보를 처리하여야 하며 그 목적 외의 용도로 활용하지 않아야 함

⑤ 정확성의 원칙

회원사는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 함

⑥ 안전성의 원칙

회원사는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 그에 상응하는 적절한 관리적·기술·물리적 보호조치를 통하여 개인정보를 안전하게 관리하여야 함

⑦ 공개의 원칙

회원사는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 함

⑧ 정보주체 권리 존중의 원칙

회원사는 열람청구권, 정정·삭제요구권, 처리정지요구권 등 정보주체의 권리를 보장하여야 함

⑨ 사생활 침해 최소화의 원칙

회원사의 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 함

⑩ 익명처리의 원칙

회원사는 개인정보를 적법하게 수집한 경우에도 익명에 의하여 업무 목적을 달성할 수 있으면 개인정보를 익명에 의하여 처리될 수 있도록 하여야 함

⑪ 책임의 원칙

회원사는 개인정보 보호 관련 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 함

4. 관련 법령의 준수

이 규약은 병원협회와 회원사 사이의 개인정보 보호 활동 의지를 확인하고 자율 규제 활동을 통하여 이를 실현하고자 하는 약속으로서의 효력을 지닌다. 이 규약에서 정하고 있지 않은 회원사의 개인정보 보호 활동에 대해서는 『의료법』, 『개인정보 보호법』 등 개인정보 보호 관련 법령이 정하는 바에 따른다.

▶ 개인정보 보호와 관련한 구체적이고 실제적인 규범은 「의료법」, 「개인정보 보호법」, 「정보통신망 이용촉진 및 정보보호에 관한 법률」, 「모자보건법」 등 개인정보 보호 관련 법령에 따름.

5. 자율규제단체

가. 자율규제단체의 지위 및 역할

회원사는 병원협회가 「자율규제단체지정 규정」에 따른 자율규제단체임을 확인하며,

병원협회는 자율규제단체로서 회원사를 대상으로 다음과 같은 업무를 수행한다.

- ① 연간 개인정보 보호 자율규제 수행계획 수립
- ② 개인정보 보호 교육 및 홍보 활동
- ③ 개인정보 보호 자율규제 규약 제정·개정
- ④ 개인정보 자율점검 및 컨설팅
- ⑤ 그 밖의 소속 개인정보처리자의 개인정보 보호 활동에 관하여 필요한 업무

나. 보고의무

병원협회는 년 1회 개인정보보호 자율규제 수행 결과를 자율규제 협의회에 보고하여야 한다.

다. 자율점검의 실시

- ① 병원협회는 회원사의 개인정보 처리 실태를 점검하고 미흡한 점을 개선하도록 지도할 수 있다.
- ② 병원협회는 회원사의 실태점검을 하기 최소 1개월 전에 회원사가 스스로 개인정보 처리 실태를 점검할 수 있도록 「표준 자율점검표」를 마련하여 배포하여야 한다.
- ③ 실태점검은 인력 및 비용 등을 고려하여 병원협회에 가입한 회원사를 우선적으로 실시할 수 있다.

라. 자율점검에 따른 포상 등

- ① 『개인정보보호 자율규제단체 지정 등에 관한 규정』 제15조(수행계획에 따른 결과의 평가 등) ②에 따라 평가 결과가 우수한 회원사는 행정안전부장관 포상을 받을 수 있다.

마. 자율규제단체 인센티브

- ① 『개인정보보호 자율규제단체 지정 등에 관한 규정』 제15조의2(자료제출 및 검사의 면제 등)에 따라 자율규제단체의 자율규제 활동에 참여하는 소속 회원사가 자율규제 규약을 충실히 준수하고 자율점검을 성실히 수행하여 수행결과가 우수하다고 인정되는 경우에는 자료제출 요구 및 검사를 1년 간 면제할 수 있다.
- ② 법 63조 제1항의 어느 하나에 해당하는 경우에는 인센티브를 적용하지 아니한다.

바. 병원협회 소속 회원사의 참여 제한

- ① 병원협회는 소속 회원사가 다음의 어느 하나에 해당하는 경우에는 자율규제 활동의 전부 또는 일부를 1년 동안 제한할 수 있다.
 - 1) 법 위반으로 인해 형벌 또는 행정처분을 받은 경우

- 2) 개인정보 처리실태에 따른 개선을 지도받았음에도 불구하고 이를 이행하지 아니한 경우
- 3) 소속 회원사가 자율점검을 허위 또는 불성실하게 이행한 경우
- 4) 병원협회의 개선이행 확인 및 허위 확인을 위한 최근 5년 이내 현장확인을 받지 않은 경우
- 5) 병원협회가 진행하는 개인정보보호 교육을 연 1회 이상 이수 하지 않은 경우

6. 회원사의 권리

회원사는 개인정보 보호 자율규제 활동의 참여 여부에 관하여 자율적으로 선택할 수 있다.

7. 자율규제 규약

- ① 행정안전부 개인정보보호 자율규제 협의회의 검토와 병원협회 상임이사회의 승인을 득하여 본 규약을 제정 및 개정할 수 있다.
- ② 병원협회는 회원사가 이 규약을 준수하도록 개선지도·권고(규약 동의, 자율점검 등) 등 필요한 조치를 할 수 있으며, 이에 응하지 않는 경우 회원사 자율규제 규약 동의를 철회 할 수 있다.
- ③ 회원사는 개인정보 보호 활동을 하며 이 규약을 준수하도록 노력해야 한다.
- ④ 본 규약은 병원협회와 소속 회원사와의 상호 합의에 의한 자율 규약이며, 개인정보 보호법과 상이할 경우 개인정보 보호법령과 지침을 우선 적용한다.
- ⑤ 병원협회는 자율점검을 허위 또는 불성실하게 진행하거나 개선 지도 이행 확인을 위해 회원사에 대해 자료제출 및 현장이행 확인을 요구할 수 있다.

제2장 개인정보 처리단계별 조치기준

1. 개인정보의 수집·이용

회원은 최소수집의 원칙에 따라 목적에 필요한 최소한의 개인정보를 수집하여야 하며, 그 수집목적의 범위에서 이용하여야 한다. 필요한 최소한의 개인정보에 관한 입증책임은 회원사에게 있다.

가. 개인정보 수집·이용 요건

1) 회원사는 다음 중 어느 하나에 해당하는 경우에 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.

○ 정보주체의 동의를 받은 경우

* 이 경우 회원사는 정보주체에게 다음 사항을 고지하여야 한다.

- ① 개인정보의 수집·이용 목적 (예 : 병적 조회, 진료기록 작성 등)
 - ② 수집하려는 개인정보의 항목 (예 : 성명, 주소, 연락처, 생년월일 등)
 - ③ 개인정보의 보유 및 이용 기간
(예 : 의료법 시행규칙에 따라 환자명부는 5년, 진료기록부는 10년간 보유함)
 - ④ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용
- ▶ 동의를 서면(전자문서 포함)으로 받을 경우 중요한 내용*은 글씨 크기 최소 9pt 이상, 다른 내용보다 20퍼센트 이상 크게 하고, 색깔, 굵기 또는 밑줄 등을 통하여 명확히 표시되도록 하여 고객이 쉽게 알아볼 수 있도록 하여야 한다. (동의 사항이 많아 중요한 내용이 명확히 구분되기 어려운 경우 중요한 내용을 다른 내용과 별도로 구분하여 표시)
- * 1) 개인정보의 수집·이용 목적 중 재화나 서비스의 홍보 또는 판매 권유 등을 위하여 해당 개인정보를 이용하여 정보주체에게 연락할 수 있다는 사실
2) 처리하는 개인정보 중 민감정보, 여권번호, 운전면허번호, 외국인등록번호
3) 개인정보의 보유 및 이용 기간
- ▶ 이 중 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.
- ▶ 위반 시, 3천만원 이하의 과태료가 부과 (법 제75조)

- 법률에 특별한 규정이 있거나 법령상 의무 준수를 위해 불가피한 경우
- 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우
- 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
- 회원사의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우

- * 이 경우 회원사의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.
- 회원사 근로자인 의료인 또는 직원의 징계, 각종 소청 또는 소송의 제기 및 진행 등을 위하여 증빙자료를 조사하고 확보하는 경우

나. 개인정보의 수집 제한과 입증책임

- 1) 회원사는 개인정보를 수집하는 경우 최소수집 원칙에 따라 개인정보를 수집하여야 하며, 그 입증책임은 해당 개인정보를 수집한 회원사가 부담한다.
- 2) 회원사는 정보주체의 동의를 받아 개인정보를 수집하는 경우 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 않을 수 있다는 사실을 구체적으로 알려야 한다.
- 3) 회원사는 필요 최소한의 개인정보 외의 수집에 동의하지 아니한다는 이유로 정보주체에게 서비스 제공을 거부해서는 안 된다.

다. 고유식별정보·민감정보의 처리 제한

- 1) 본 항에서의 '고유식별정보'란 여권번호, 운전면허번호, 외국인등록번호를 말하며, '민감정보'란 사상·신념, 정치적 견해, 건강, 성생활 및 개인정보 보호법 시행령에 따른 유전정보 및 범죄경력 등 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보를 말한다.
- 2) 회원사는 다음 중 하나에 해당하는 경우 고유식별정보·민감정보를 처리할 수 있다.

- ① 정보주체에게 다른 개인정보의 처리와 별도로 동의를 받은 경우
- ② 법령에서 구체적으로 처리를 요구하는 경우

라. 주민등록번호의 처리 제한

- 1) 회원사는 다음 중 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다.

- ① 법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회 규칙 및 감사원 규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우*
- ② 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우

* 의료법 시행령 제42조의2, 의료법 제17조제1항 및 시행규칙 제9조, 제12조, 제14조 등

- 2) 회원사는 주민등록번호를 보관할 시 암호화 조치를 통하여 안전하게 보관하여야 한다. 암호화 조치를 어긴 경우 5천만 원 이하의 과태료가 부과된다.

마. 금지되는 개인정보의 수집·이용

- 1) 거짓이나 그 밖의 부정한 수단이나 방법으로 개인정보를 취득하거나 처리에 관한 동의를 받는 행위를 하는 경우, 3년 이하의 징역 또는 3천만 원 이하의 벌금이 부과된다.

2. 개인정보 제3자 제공

개인정보는 정보주체의 동의를 받은 경우, 법령에서 정한 개인정보 수집목적 범위 내에서 제3자에게 제공할 수 있다.

가. 제3자 제공 요건

- 1) 회원사는 다음의 경우 중 어느 하나에 해당하는 경우 정보주체의 개인정보를 제3자에게 제공할 수 있다.
 - 정보주체의 동의를 받은 경우 및 목적 외의 용도로 제3자에게 제공하는 경우
 - * 이 경우 회원사는 정보주체에게 다음 사항을 고지하여야 한다.

- 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 경우에는 그 불이익의 내용

▶ 동의를 서면(전자문서 포함)으로 받을 경우 중요한 내용*은 글씨 크기 최소 9pt 이상, 다른 내용보다 20퍼센트 이상 크게 하고, 색깔, 굵기 또는 밑줄 등을 통하여 명확히 표시되도록 하여 고객이 쉽게 알아볼 수 있도록 하여야 한다. (동의 사항이 많아 중요한 내용이 명확히 구분되기 어려운 경우 중요한 내용을 다른 내용과 별도로 구분하여 표시)

* 1) 처리하는 개인정보 항목 중 민감정보, 여권번호, 운전면허번호, 외국인등록번호
 2) 개인정보를 제공받는 자의 보유 및 이용 기간
 3) 개인정보를 제공받는 자 및 개인정보를 제공받는 자의 개인정보 이용 목적

▶ 이 중 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.
 ▶ 위반 시, 5천만 원 이하의 벌금 부과 (법 제71조)

- 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위해 불가피한 경우*
 - * 다만, 법령상 의무 준수하기 위해 불가피한 경우에는 개인정보 수집 목적 범위 내에서만 가능
 - 「의료법」 제21조(기록열람 등) 제3항 요건을 부합하는 경우에 한하여만 환자

에 관한 기록을 제3자에게 열람하게 하거나 사본을 교부할 수 있다.

- 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소 불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우

나. 고유식별정보·민감정보의 처리 제한

- 1) 본 항에서의 '고유식별정보'란 여권번호, 운전면허번호, 외국인등록번호를 말하며, '민감정보'란 사상·신념, 정치적 견해, 건강, 성생활 및 개인정보 보호법 시행령에 따른 유전정보 및 범죄경력 등 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보를 말한다.
- 2) 회원사는 다음 중 하나에 해당하는 경우 고유식별정보·민감정보를 처리할 수 있다.

- ① 정보주체에게 다른 개인정보의 처리와 별도로 동의를 받은 경우
- ② 법령에서 구체적으로 처리를 요구하는 경우

다. 주민등록번호의 처리 제한

- 1) 회원사는 다음 중 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다.

- ① 법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회 규칙 및 감사원 규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우*
- ② 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우

* 의료법 시행령 제42조의2, 의료법 제17조제1항 및 시행규칙 제9조, 제12조, 제14조 등

- 2) 회원사는 주민등록번호를 보관할 시 암호화 조치를 통하여 안전하게 보관하여야 한다. 암호화 조치를 어긴 경우 5천만 원 이하의 과태료가 부과된다.

라. 금지되는 개인정보 제공 행위

- 1) 업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공하는 행위는 5년 이하의 징역 또는 5천만 원 이하의 벌금이 부과된다.

3. 개인정보 처리 업무위탁

회원사는 개인정보의 처리 업무를 제3자에게 위탁하는 경우에는 문서로 하여야 하며, 위탁하는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자를 정보주체가 언제든지 쉽게 확인할 수 있도록 공개하여야 한다.

가. 위탁 방법

- 1) 회원사에서 정보주체 개인정보 처리업무(예 : 진료 신청서 처리사무, 진료비 수납사무, 연말정산사무, 각종 증명서 발급사무 등)를 위탁하는 경우 아래 사항이 포함된 문서로 하여야 함

<개인정보 처리 위탁 계약서 기재사항>

- ① 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
- ② 개인정보의 기술적·관리적 보호조치에 관한 사항
- ③ 위탁업무의 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 법 제26조제2항에 따른 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

나. 위탁업무 등의 공개

- 1) 개인정보처리업무를 위탁하는 회원사는 개인정보처리업무를 위탁받아 처리하는 수탁자를 정보주체가 언제든지 쉽게 확인할 수 있도록 홈페이지에 '개인정보 처리방침'으로 지속적으로 게재하여야 함
- 2) 인터넷 홈페이지에 게재할 수 없는 경우에는 다음의 방법 중 어느 하나 이상의 방법으로 위탁하는 업무의 내용과 수탁자를 공개하여야 함

<인터넷 이외의 방법에 의한 위탁업무 공개방법>

- ① 위탁자의 사업장·영업소·사무소·점포 등(이하 "사업장 등"이라 한다)의 보기 쉬운 장소에 게시하는 방법
- ② 관보나 위탁자의 사업장 등이 있는 시·도 이상의 지역을 주된 보급지역으로 하는 「신문 등의 진흥에 관한 법률」 제2조제1호가목·다목 및 같은 조 제2호에 따른 일반일간신문, 일반주간신문 또는 인터넷신문에 실는 방법
- ③ 같은 제목으로 연 2회 이상 발행하여 정보주체에게 배포하는 간행물·소식지·홍보지 또는 청구서 등에 지속적으로 실는 방법
- ④ 재화나 용역을 제공하기 위하여 위탁자와 정보주체가 작성한 계약서 등에 실어 정보주체에게 발급하는 방법

다. 수탁자 교육 및 감독

- 1) 개인정보처리업무를 위탁한 회원사는 수탁자에 대하여 개인정보가 분실·도난·유출·변조·훼손되지 않도록 교육하여야 함
- 2) 개인정보처리업무를 위탁한 회원사는 수탁자가 '개인정보 보호법과 시행령, 보건복지부 개인정보 보호 기본지침'에 따라 준수하고 있는지 감독하여야 함

라. 손해배상 책임

- 1) 수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에 개인정보 보호법을 위반하여 발생한 손해배상 책임에 대하여는 수탁자를 회원사의 소속직원으로 간주함

4. 영업의 양도

영업양도, 합병 등으로 다른 회원사에 정보주체의 개인정보를 이전할 때에는 영업양도자는 해당 정보주체에게 알려야 하며, 개인정보를 이전받은 회원사는 이전 당시의 본래 목적으로만 개인정보를 이용할 수 있다.

- 1) 영업양도, 합병 등으로 정보주체의 개인정보를 다른 회원사에게 이전하여야 하는 때에는 개인정보를 이전하기 전에 해당 정보주체에게 다음의 사항을 통지하여야 함
 - 정보주체가 최소한 이전 사실을 확인하고 회원탈퇴, 동의철회 등의 권리를 행사할 수 있는 시간적 여유를 주어야함
- 2) 회원사는 영업양도 등에 따라 개인정보 이전 사실을 통지하여야 함
- 3) 개인정보를 이전받은 회원사는 정보주체에게 개인정보의 이전사실 등을 개인정보를 이전받은 후 지체 없이 통지*하여야 함
 - 회원사가 개인정보의 이전사실 등을 이미 알린 경우에는 통지하지 않아도 됨

* 통지사항

- 개인정보를 이전하려는 사실
- 개인정보를 이전받는 자(영업양수자 등)의 성명(법인의 경우에는 법인의 명칭을 말한다), 주소, 전화번호 및 그 밖의 연락처
- 정보주체가 개인정보의 이전을 원하지 아니하는 경우 조치할 수 있는 방법 및 절차

* 통지방법

- 영업양도 등에 따라 개인정보 이전 사실을 아래의 방법으로 통지하여야 함
- 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법

- 개인정보를 이전하려는 의료기관이 과실 없이 서면 등에 따른 방법으로 통지사항을 정보주체에게 알릴 수 없는 경우에는 해당 사항을 인터넷 홈페이지에 30일 이상 게재하여야 함
- 다만, 인터넷 홈페이지를 운영하지 아니하는 의료기관은 사업장 등의 보기 쉬운 장소에 30일 이상 게시하여야 함
- 개인정보를 이전받은 의료기관은 환자 등 정보주체에게 개인정보의 이전사실 등을 개인정보를 이전받은 후 지체 없이 통지하여야 함

- 4) 개인정보를 이전받은 회원사는 영업의 양도·합병 등으로 개인정보를 이전받은 경우, 이전 당시의 본래 목적으로만 개인정보를 이용할 수 있으며, 「개인정보 보호법」의 개인정보처리자로서의 권리와 의무를 짐
- 영업의 양도, 합병 당시의 처리 목적과 다른 용도로 개인정보를 이용하고자 하는 경우에는 정보주체로부터 별도로 동의를 받아야 함

5. 영상정보처리기의 설치·운영

회원사가 영상정보처리기기(CCTV, 네트워크 카메라)를 설치·운영하고자 할 때에는 개인의 사생활이 침해되지 않도록 영상정보처리기기를 최소한으로 설치·운영하여야 한다.

가. 영상정보처리기기 설치·운영 제한

- 1) 공개된 장소에서 영상정보처리기기 설치·운영은 원칙적으로 금지되지만, 예외적으로 다음의 사유에 해당하는 경우에는 설치할 수 있음

<영상정보처리기기 설치·운영 사유>

- ① 법령에서 구체적으로 허용하고 있는 경우
- ② 범죄의 예방 및 수사를 위하여 필요한 경우
- ③ 시설안전 및 화재 예방을 위하여 필요한 경우
- ④ 교통단속을 위하여 필요한 경우
- ⑤ 교통정보의 수집·분석 및 제공을 위하여 필요한 경우

- 2) 목욕실, 화장실, 탈의실 등 개인의 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있도록 하는 영상정보처리기기 설치·운영은 금지됨

나. 영상정보처리기기 임의조작·녹음 금지

- 1) 영상정보처리기기는 설치목적과 다른 목적으로 임의로 조작하거나 다른 곳을 비추거나 녹음기능을 사용하는 것은 금지됨

다. 영상정보처리기기 설치 시 의견수렴 절차 실시

- 1) 공공기관이 공개된 장소 및 교도소·정신보건시설 등 대통령령으로 정한 장소에

영상정보처리기기를 설치·운영하려는 경우에는 다음의 절차 중 하나를 거쳐 관계 전문가 및 이해관계인의 의견을 수렴해야 함

- 「행정절차법」에 따른 행정예고의 실시 또는 의견청취
 - 해당 영상정보처리기기의 설치로 직접 영향을 받는 지역 주민 등을 대상으로 하는 설명회, 설문조사 또는 여론조사
- 2) 법에 따른 교정시설이나 정신의료기관 등 개인 사생활 침해우려 장소에 영상정보처리기기를 설치·운영하려는 자는 다음의 사람들로부터 모두 의견을 수렴하여야 함
- 관계 전문가
 - 해당 시설에 종사하는 사람, 해당 시설에 구금되어 있거나 보호받고 있는 사람 또는 그 사람의 보호자 등 이해관계인

라. 안내판 설치를 통한 설치·운영 사실 공개

- 1) 회원사가 공개된 장소에 영상정보처리기기를 설치·운영할 때 정보주체가 쉽게 알아 볼 수 있도록 안내판을 설치하여야 함

마. 영상정보처리기기 운영·관리 방침

- 1) 영상정보처리기기를 운영하는 회원사는 영상정보처리기기 운영·관리 방침을 수립하여 홈페이지, 게시판 등에 공개하여야 함
- 2) 영상정보처리기기를 운영하는 회원사는 개인영상정보 처리에 관한 업무를 총괄하여 책임질 '개인영상정보 관리책임자'를 지정하여야 함

바. 영상정보의 목적 외 이용·제공 제한 및 보관·파기 철저

- 1) 영상정보처리기기를 운영하는 회원사는 다음의 사유에 해당하는 경우를 제외하고 개인영상정보를 수집목적 이외로 이용하거나 제3자에게 제공하는 것은 금지됨

<개인영상정보 이용 및 제3자 제공의 허용>

- ① 정보주체의 별도의 동의를 얻은 경우
- ② 다른 법률에 특별한 규정이 있는 경우
- ③ 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
- ④ 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인영상정보를 제공하는 경우

- ⑤ 개인영상정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 개인정보 보호위원회의 심의·의결을 거친 경우
- ⑥ 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우
- ⑦ 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
- ⑧ 법원의 재판업무 수행을 위하여 필요한 경우
- ⑨ 형(形) 및 감호, 보호처분의 집행을 위하여 필요한 경우

※ ⑤~⑨번은 공공회원사에 한함

- 2) 영상정보처리기를 운영하는 회원사는 영상정보 보유목적 달성을 위한 특별한 기간 산정이 곤란한 때에는 영상정보의 보관기간은 개인영상정보 수집 후 30일 이내로 하고, 이 기간이 종료한 때에는 파기하여야 함

사. 영상정보처리기의 설치·운영 위탁 시 관리·감독 철저

- 1) 영상정보처리기를 운영하는 회원사는 영상정보처리기의 설치·운영에 관한 사무를 위탁할 수 있으며, 이 경우 개인정보 처리업무 위탁에 관한 규정을 준수하여야 함

아. 개인영상정보 열람·존재확인·파기 청구권 보장

- 1) 영상정보처리기를 운영하는 회원사는 정보주체로부터 개인영상정보의 열람, 존재확인 또는 파기를 요청받은 경우 지체 없이 필요한 조치를 취해야 함
- 다만, 의료인 폭행 등과 같이 정보주체의 요구를 거부할 만한 정당한 사유가 존재하는 경우에는 거부사유를 10일 이내에 서면으로 정보주체에게 통지하고 열람 등 거부

자. 개인영상정보의 안전성 확보 조치 및 자체 점검 실시

- 1) 영상정보처리기를 운영하는 회원사는 개인영상정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 조치를 하여야 함
- 2) 한편, 영상정보처리기를 운영하는 보건복지부 소관 회원사는 「보건복지부 개인정보 보호 기본지침」 준수 여부에 대한 자체점검을 통해 개인영상정보의 침해 방지를 위해 노력하여야 함

6. 개인정보파일의 등록(공공 회원사에만 적용)

공공 회원사가 개인정보파일을 운용하기 위해서는 행정안전부에 등록하여야 하며, 변경한 경우에도 같다.

- 1) 개인정보파일의 등록·변경등록은 개인정보 보호책임자가 행정안전부에 등록하여야 함
- 2) 개인정보파일의 등록·변경등록은 개인정보취급자의 신청을 받은 개인정보 분야별 책임관이 소속 기관의 개인정보 보호책임자에게 신청하여야 함
- 3) 개인정보파일의 등록·변경등록 신청을 받은 개인정보 보호책임자는 등록·변경 등록 사항을 검토하고, 그 적정성을 판단하여야 하며, 해당 개인정보파일을 운용하기 시작한 날부터 60일 이내에 행정안전부에 등록·변경등록을 하여야 함
 - 다만, 개인정보파일 등록 시 보건복지부에 사전에 보고하고 확인을 받아야 함
- 4) 개인정보파일을 등록·변경등록하기 위하여서는 '개인정보 파일 등록·변경등록 신청서'를 작성하여 신청하고, 등록된 개인정보파일을 보유하는 경우에는 1개의 개인정보파일에 1개의 개인정보파일대장을 작성하여 관리하여야 함

7. 개인정보의 안전성 확보조치

회원은 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리 계획 수립, 접속기록 보관 등 안전성 확보에 필요한 조치를 하여야 한다.

가. 원칙

사업자는 처리하는 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 관리적·물리적 및 기술적 안전조치를 하여야 한다. 이 규약에서 제시된 안전조치 사항은 최소한의 기준을 정한 것으로서 사업자의 규모 및 유형, 개인정보 보유량 등을 고려하여 스스로의 환경에 맞는 안전조치 기준을 수립하여 시행하여야 한다.

나. 적용 기준

개인정보의 안전성 확보조치는 사업자의 규모 및 유형, 개인정보 보유량에 따라 필수적으로 적용해야 하는 항목이 서로 다르므로, 각 사업자는 아래의 표를 참조하여 어떤 유형에 속하는지를 우선 파악한 후 필요한 안전조치를 적용하여야 한다.

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	-	○	○
2. 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항	-	○	○
3. 개인정보취급자에 대한 교육에 관한 사항	-	○	○
4. 접근권한의 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. 위험도 분석 및 대응방안 마련에 관한 사항	-	-	○
13. 재해 및 재난 대비 개인정보처리시스템의 물리적 안전조치에 관한 사항	-	-	○
14. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항	-	-	○
15. 그 밖에 개인정보 보호를 위하여 필요한 사항	-	○	○

- ▶ 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 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부 관리 계획의 이행 실태를 연 1회 이상으로 점검·관리하여야 함

다. 비밀번호 관리

- 1) 개인정보취급자가 안전한 비밀번호를 설정할 수 있도록 이행 가능한 '비밀번호 작성규칙'을 수립한 후, 개인정보처리시스템 및 접근통제시스템 등에 이를 적용하고 운영하여야 함

<비밀번호 작성규칙>

- ① 비밀번호 최소길이
 - 최소10자리 : 영문자(26개), 숫자(0~9, 10개), 특수문자 (#, [, “, < 등, 32개) 중 2종 류 이상으로 조합·구성한 경우
 - 영문자, 숫자, 특수문자 중 3종류 이상으로 구성된 경우
- 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 입력값의 자리수와 조합을 체크하여 안전한 비밀번호 작성규칙에 위배되는 경우, 법 위반을 알리고 작성규칙을 준수하도록 함

- 2) 비밀번호 분실 시, SMS 등을 통해 본인 확인 절차를 거쳐 비밀번호를 재설정할 수 있도록 하여야 함
- 3) 일정 횟수 이상 비밀번호 입력 오류 시 계정 잠금을 통해 무작위 대입 공격(Brute Force Attack) 등에 의한 비인가자의 로그인 시도를 차단하여야 하며, 잠금 해제 시에도 본인확인 절차를 마련하여 적용하여야 함

라. 접근통제 시스템의 설치·운영

- 1) 회원사는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 함
- 2) 회원사는 개인정보가 저장된 업무용 컴퓨터에 해커 등 비인가자의 접근을 통제하기 위해 상용 침입차단 프로그램 또는 업무용 컴퓨터 운영체제에서 제공되는 침입차단 프로그램을 사용하여 불법적인 접근을 차단하여야 함
- 3) 회원사 내에서 업무용으로 무선네트워크를 사용할 경우, 무선 네트워크를 통한 내부망 침투, 개인정보처리시스템 접근 및 네트워크 도청 등 유선 네트워크에 비해

침해 가능성이 높으므로 이를 방지하기 위한 보안 조치 적용이 필요함

- 4) 개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보 취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하여야 함
- 5) 고유식별정보를 처리하는 회원사는 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연1회 이상 취약점을 점검하고 필요한 보완조치를 하여야 함(의료통합관리시스템이 홈페이지와 연계되어 서비스되는 경우에 한함)

마. 개인정보 암호화

- 1) 고유식별정보, 비밀번호, 바이오정보 등과 같은 주요 개인정보가 암호화되지 않고 개인정보처리시스템에 저장되거나 네트워크를 통하여 전송될 경우, 유출·노출 및 위·변조 등의 위험이 있으므로 암호화 등의 안전한 보호조치가 제공되어야 함
- 2) 암호화대상 개인정보를 저장할 때 암호화를 적용하는 경우 ① 개인정보의 저장 현황, ② 개인정보의 저장에 따른 위험도 분석절차(또는 영향평가 절차) 및 방법, ③ 암호화 추진 일정 등이 포함된 “암호화계획”을 수립하여야 함

바. 접속기록의 보관 및 위·변조 방지

- 1) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하여야 함. 다만, 5만명 이상의 정보주체에 관하여 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 함.
- 2) 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 함. 특히 개인정보를 다운로드한 것이 발견되었을 경우에는 내부관리 계획으로 정하는 바에 따라 그 사유를 반드시 확인하여야 함.
- 3) 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 함.

사. 보안 프로그램의 설치 및 운영

- 1) 회원사는 악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영할 것

아. 개인정보의 안전한 보관을 위한 보관시설 등

- 1) 회원사는 원무실, 전산실, 의무기록실 및 그 밖의 문서보관실 등 개인정보를 보관하는 장소에 대한 출입통제 계획을 마련하고 시행하여야 함

자. 전자의무기록의 안전한 관리·보존

- 1) 의료인이나 회원사의 개설자가 전자의무기록을 안전하게 관리·보존하기 위한 장비를 갖추어야 함

차. 개인정보 표시 제한 보호조치 적용(권고 사항)

- 1) 개인정보의 조회, 출력, 다운로드 시 업무상 불필요한 개인정보의 노출을 최소화할 수 있도록 개인정보의 일부분을 마스킹하여 표시제한 조치를 취하는 것이 바람직함
- 2) 이 경우, 상이한 마스킹 적용에 따른 완전한 개인정보 조합 가능성을 차단하기 위하여 회원사별로 마스킹 적용규칙을 수립하여 일관성을 유지하는 것이 필요함

타. 관리용 단말기의 안전조치

- 1) 회원사는 개인정보 유출 등 개인정보 침해사고 방지를 위하여 관리용 단말기에 대해 다음과 같은 안전조치를 하여야 함
 - 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치
 - 본래 목적 외로 사용되지 않도록 조치
 - 악성프로그램 감염 방지 등을 위한 보안조치 적용

파. 재해·재난 대비 안전조치

- 1) 회원사는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 위기 대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검하여야 함
- 2) 회원사는 재해·재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하여야 함

8. 개인정보의 파기

회원사는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 하고, 파기할 때에는 복구 또는 재생되지 아니하도록 조치하여야 한다.

- 1) 회원사는 보존기간이 경과하거나 수집·목적 달성한 진료기록 등 의료정보에 대해서는 지체 없이 파기하는 것이 바람직함
 - 개인정보 보호책임자는 파기 계획수립, 시행 등을 관리하여야 하며, 그 사실을 기록하고 관리하여야 함
- 2) 민간 회원사 개설자가 폐업 또는 휴업 신고를 할 때에는 기록·보존하고 있는 진료기록부, 조산기록부, 간호기록부, 그 밖의 진료에 관한 기록을 관할 보건소장에게 넘겨야 함
- 3) 공공 회원사가 폐업한 경우 그 사무를 승계하는 기관이 없을 때에는 폐업하는 회원사의 장은 지체 없이 그 기관의 기록물을 소관 영구기록물관리기관으로 이관하여야 함
- 4) 정보주체가 회원사의 인터넷 홈페이지 회원에서 탈퇴하는 경우에는 더 이상 해당 정보주체의 개인정보를 보유할 이유가 없으므로 회원사는 정보주체가 탈퇴한 날부터 5일 이내에 파기하여야 함
- 5) 회원사의 개인정보 가운데 진료기록의 보존기간과 보존방법은 다음과 같음

< 진료기록의 보존기간 >

종 류	보존기간	종 류	보존기간
환자명부	5년	방사선사진 및 그 소견서	5년
진료기록부	10년	간호기록부	5년
처방전	2년	조산기록부	5년
수술기록	10년	진단서 등의 부분	3년
검사소견기록	5년		

- 6) 개인정보를 파기할 때에는 개인정보가 복구 또는 재생되지 않도록 조치하여야 함
- 7) 정보주체의 진료정보는 법정 보존기간이 경과하여 처리 목적을 달성한 경우에는 지체 없이 파기하는 것이 원칙이며 다만, 계속적인 진료를 위하여 필요한 경우에는 1회에 한정하여 <진료기록의 보존기간>에 정하는 기간의 범위에서 그 기간을 연장하여 보존할 수 있음

9. 개인정보 처리방침의 수립 및 공개

- 1) 회원사는 개인정보처리방침을 수립하여 정보주체가 쉽게 확인할 수 있도록 인터넷 홈페이지의 첫 화면에 공개하여야 하며, 홈페이지가 없는 경우에는 사업장의 보기 쉬운 장소에 게시하는 방법 등으로 공개하여야 함

<개인정보 처리방침 기재사항>

필수적 기재사항	임의적 기재사항
1. 개인정보의 처리 목적 2. 개인정보의 처리 및 보유 기간 3. 개인정보의 제3자 제공에 관한 사항 (해당되는 경우에만 정함) 4. 개인정보처리의 위탁에 관한 사항 (해당되는 경우에만 정함) 5. 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항 6. 처리하는 개인정보의 항목 7. 개인정보의 파기에 관한 사항 8. 개인정보 보호책임자에 관한 사항 9. 개인정보 처리방침의 변경에 관한 사항 10. 개인정보의 안전성 확보조치에 관한 사항 11. 개인정보 자동 수집 장치의 설치·운영 및 그 거부에 관한 사항	1. 정보주체의 권익침해에 대한 구제방법 2. 개인정보의 열람청구를 접수·처리하는 부서 3. 영상정보처리기기 운영·관리에 관한 사항 (개인정보 보호법 제25조제7항에 따른 ‘영상정보처리기기 운영·관리방침’을 개인정보처리방침에 포함하여 정하는 경우)

※ 필수적 기재사항이란 개인정보 보호법 제30조, 시행령 제31조, 표준 개인정보 보호지침 제37조에 따라 「개인정보 처리방침」에 반드시 모두 포함해야 하는 사항임
 ※ 임의적 기재사항이란 「개인정보 처리방침」에 포함시킬지 여부를 사업자/단체 스스로가 개인정보 처리현황을 고려하여 자율적으로 정할 수 있는 사항임

10. 개인정보 보호책임자 지정

- 1) 개인정보의 처리에 관한 업무 총괄 및 다음의 업무 수행을 위해 개인정보 보호 책임자를 지정하여야 함

< 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 행정안전부 등록
- ⑫ 그 밖에 개인정보 보호를 위하여 필요한 업무

< 개인정보 보호책임자의 자격 요건(아래 요건 중 하나에 해당되어야 함) >

- ① 사업주 또는 대표자
- ② 임원(임원이 없는 경우에는 개인정보 처리 관련 업무를 담당하는 부서의 장)
 - ▶ 위반 시, 1천만원 이하 과태료 부과(법 제75조제3항제8호)
 - ▶ 사업주 또는 대표자가 아닌 경우에는, 인사 발령 등 공식적인 지정 절차 필요

11. 정보주체의 권익보호

회원은 정보주체의 요구가 있으면 정보주체의 정보를 열람·정정·삭제하여야 하고, 정보주체 개인정보가 유출된 경우 정보주체에게 그 사실을 알려야 한다.

가. 정보주체 이외로부터 수집한 개인정보에 대한 고지

- 1) 정보주체 이외로부터 수집한 개인정보를 처리하는 때에는 정당한 사유가 없는 한 정보주체의 요구가 있는 날로부터 3일 이내에 다음의 사항을 알려야 함

< 고지사항 >

- ① 개인정보의 수집 출처 및 개인정보의 처리 목적
- ② 개인정보의 처리정지를 요구할 권리가 있다는 사실

<고지의 예외>

다만, ① 고지를 요구하는 대상이 되는 개인정보가 행정안전부 등록 대상이 되는 개인정보 파일에 포함되어 있거나 ② 고지로 인하여 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우 가운데 어느 하나에 해당하는 경우에는 정보주체의 권리보다 명백히 우선하는 경우에 한하여 고지하지 않을 수 있음

- 2) 정보주체의 요구를 거부하는 경우에는 정당한 사유가 없는 한 그 요구가 있는 날로부터 3일 이내에 그 거부의 사유를 정보주체에게 알려야 함

- 3) 5만명 이상의 민감정보 처리, 100만명 이상의 개인정보 처리자는 개인정보를 제공 받은 날부터 3개월 이내에 서면, 전화, 문자전송, 전자우편 등 정보주체가 쉽게 알 수 있는 방법으로 정보주체에게 알려야 함

나. 개인정보 열람·정정·삭제·처리정지 요구 방법 마련

- 1) 회원사는 정보주체가 자신의 개인정보에 대한 열람, 정정, 삭제, 처리 정지를 요구 하기 위한 방법과 절차를 마련하여야 함.
- 2) 이때 열람, 정정, 삭제, 처리 정지 요구를 위한 방법과 절차는 개인정보의 수집 방법과 절차에 비하여 어렵지 않도록 다음 사항을 준수하여야 함
 - 서면, 전화, 전자우편, 인터넷 등 정보주체가 쉽게 활용할 수 있는 방법으로 제공할 것
 - 개인정보를 수집한 창구의 지속적 운영이 곤란한 경우 등 정당한 사유가 있는 경우를 제외하고는 최소한 개인정보를 수집한 창구 또는 방법과 동일 하게 개인정보의 열람을 요구할 수 있도록 할 것
 - 인터넷 홈페이지를 운영하는 회원사는 홈페이지에 열람 요구 방법과 절차를 공개할 것

다. 개인정보 열람 요구

- 1) 정보주체가 개인정보에 대한 열람을 요구할 경우 회원사는 「개인정보 보호법」에 따라 열람 요구를 받은 날부터 10일 이내에 조치하여야 함
 - 다만, 환자의 기록에 대해서는 「의료법」 제21조(열람요구 등)에 따라 열람요구를 처리해야 함
- 2) 10일 이내에 열람할 수 없는 정당한 사유가 있으면 그 사유를 알리고 열람을 연기할 수 있으며, 사유가 소멸하면 소멸한 날로부터 10일 이내에 열람하도록 하여야 함
- 3) 회원사에서는 열람의 제한·거절사유에 해당하는 경우에는 열람을 요구하는 정보주체에게 그 사유를 알리고 열람을 제한하거나 거절할 수 있음
- 4) 의료인이나 직원 등 회원사 근로자는 정보주체가 아닌 다른 사람에게 정보주체에 관한 기록을 열람하게 하거나 그 사본을 내주는 등 정보주체의 개인정보의 내용을 확인할 수 있게 하여서는 아니 됨
 - 다만, 의료인이나 회원사 종사자는 아래의 '열람 또는 사본의 교부 등 허용사유'에 해당하는 경우 기록을 열람하게 하거나 그 사본을 교부하는 등 내용을 확인 할 수 있도록 함

- 위의 '열람 또는 사본의 교부 등 허용 사유'에 대해 의사가 환자의 진료를 위하여 불가피하다고 인정하는 경우에는 허용하지 않을 수 있음
 - 정보주체가 본인에 관한 진료기록 등을 열람하거나 그 사본의 발급을 원하는 경우에는 본인임을 확인할 수 있는 신분증을 회원사 개설자에게 제시하여야 함
 - '열람 또는 사본의 교부 등 허용사유' 가운데 '정보주체가 지정하는 대리인이 환자 본인의 동의서와 대리권이 있음을 증명하는 서류를 첨부하는 등 보건복지부령으로 정하는 요건을 갖추어 요청한 경우'에는 회원사 개설자는 해당 정보주체에 관한 기록의 열람 또는 사본의 교부 등을 하여야 함
- 5) 회원사의 정보주체로부터 개인정보의 제3자 제공 현황의 열람청구를 받은 경우, 국가안보에 긴요한 사안으로 “다른 법률에 따라 진행 중인 감사 및 조사에 관한 업무”를 수행하는데 지장을 초래할 때에는 제3자에게 열람청구의 허용 또는 제한, 거부와 관련한 의견을 조회하여 결정할 수 있음

라. 개인정보의 정정·삭제 요구

- 1) 자신의 개인정보를 열람한 정보주체가 해당 개인정보의 정정·삭제를 요구할 경우, 10일 이내에 조사·조치하고 그 결과를 해당 정보주체에게 통지하여야 함
 - 다른 법령에서 그 개인정보가 수집 대상으로 명시되어 있는 경우에는 그 삭제를 요구할 수 없으므로, 해당 정보주체에게 그 사실 및 이유와 이의제기 방법을 알려야 함
 - 진료기록부, 조산기록부, 간호기록부에 기재되어 있는 개인정보는 의료법관련 법령에 근거하여 수집되고 있으므로 환자는 그 삭제를 요청할 수 없음
 - 진료기록부 등의 진료정보 이외의 회원정보, 인사정보 등에 대해서는 정보주체가 해당 개인정보의 정정·삭제를 요구할 경우 10일 이내에 조사·조치하고 그 결과를 통지하여야 함

- 2) 의료인은 진료기록부, 조산기록부, 간호기록부, 그 밖의 진료에 관한 기록을 고의로 사실과 다르게 정정하거나 삭제할 수 없음

마. 개인정보 처리정지 요구

- 1) 정보주체는 회원사에 대하여 자신의 개인정보에 대한 처리정지를 요구할 수 있음
 - 이 경우, 공공 회원사에 대해서는 행정안전부에 등록하여야 하는 개인정보파일 가운데 자신의 개인정보에 대한 처리의 정지를 요구할 수 있음

- 2) 정보주체는 자신의 개인정보에 대한 처리정지를 요구할 경우 정당한 사유가 없는 한 그 요구를 받은 해당 회원사는 요구를 받은 날로부터 10일 이내에 해당 개인정보의 파기 등 정보주체의 요구에 상응하는 조치 결과를 알려야 함
 - 다만, 다음과 같은 경우에는 처리정지 요구를 거절할 수 있고, 이 경우 거절의 사유, 거절 사실 및 이유, 이의제기 방법을 요구 받은 날로부터 10일 이내에 알려야 함

- ① 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
- ② 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우
- ③ 공공기관이 개인정보를 처리하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우
- ④ 개인정보를 처리하지 아니하면 정보주체와 약정한 서비스를 제공하지 못하는 등 계약의 이행이 곤란한 경우로서 정보주체가 그 계약의 해지 의사를 명확하게 밝히지 아니한 경우

바. 개인정보 유출 시 통지

- 1) 정보주체의 개인정보 유출사고가 발생한 것을 확인 한 때부터 5일 이내에 알려야 함
 - 다만, 유출된 개인정보의 확산 및 추가 유출을 방지하기 위하여 접속경로의 차단, 취약점 점검·보완, 유출된 개인정보의 삭제 등 긴급한 조치가 필요한 경우에는 그 조치를 한 후 지체 없이 정보주체에게 알릴 수 있음
- 2) 1천명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 정보주체에게 지체없이 통지하고, 조치결과를 행정안전부장관 또는 전문기관(한국인터넷진흥원) 중 어느 하나에 신고하여야 함

- ▶ 유출신고는 개인정보 유출신고(보고)서 작성하여 신고
- ▶ 신고 방법은 <https://www.privacy.go.kr/wcp/dcl/spl/splRptInfo.do> 에 접속하여 확인

- 3) 개인정보 유출시 정보주체에 대한 통지 및 통지사항을 인터넷 홈페이지에 정보주체가 알아보기 쉽도록 7일 이상 게재하여야 함

12. 피해 구제방법

- 1) 개인정보 보호법은 다음과 같은 피해 구제방법을 규정하고 있음
 - 개인정보 처리 관련 모든 당사자 사이의 분쟁을 조정하는 ‘개인정보 분쟁조정’
 - 정보주체의 피해 또는 권리침해가 다수의 정보주체에게 같거나 비슷한 유형으로

발생하고 다음의 요건을 갖춘 경우에 이루어지는 ‘개인정보 집단분쟁조정’

< 집단분쟁조정 신청요건 >

- | |
|--|
| <p>① 피해 또는 권리침해를 입은 정보주체의 수가 다음 각 목의 정보주체를 제외하고 50명 이상일 것
가. 개인정보처리자와 분쟁해결이나 피해보상에 관한 합의가 이루어진 정보주체
나. 같은 사안으로 다른 법령에 따라 설치된 분쟁조정기구에서 분쟁조정 절차가 진행 중인 정보주체
다. 해당 개인정보 침해로 인한 피해에 대하여 법원에 소(訴)를 제기한 정보주체</p> <p>② 사건의 중요한 쟁점이 사실상 또는 법률상 공통될 것</p> |
|--|

- 개인정보처리자가 집단분쟁조정을 거부하거나 집단분쟁조정 결과를 수락하지 아니한 경우에 하는 ‘개인정보 단체소송’
- 개인정보를 처리할 때 개인정보에 관한 권리 또는 이익을 침해받은 사람이 행정안전부장관 또는 개인정보침해 신고센터(118센터)로 그 침해 사실을 신고 하는 ‘침해사실 신고’

[회원사명] 개인정보 수집·이용 동의서(예시)

[회원사명]은(는) 개인정보보호법 등 관련 법령상의 개인정보 보호 규정을 준수하며 [정보주체](예: 환자)의 개인정보 보호에 최선을 다하고 있습니다. [회원사명]은(는) 개인정보보호법 제15조 및 같은 법 제22조에 근거하여, 다음과 같이 [수집·이용 목적 (예: 홈페이지 회원관리)]을(를) 위하여 개인정보를 수집·이용하는데 동의를 받고자 합니다.

1. 개인정보의 수집·이용 목적 : [예 : 홈페이지, 회원관리]

- 회원사홈페이지 : www.oooo.co.kr

2. 수집하는 개인정보의 항목 : [예 : ▶ 필수정보-ID, 비밀번호, 성명 ▶선택(부수)정보- 생년월일, 전화번호, 이메일주소, 관심정보 등]

* 필요한 최소한의 항목으로 작성

3. 개인정보의 보유 및 이용 기간 : [예 : 수집일('00.00.00.)로부터 3개월, 20%이상 글자크게, 진하게 작성]

* 필요한 최소한의 기간으로 작성

4. 동의거부권 및 동의 거부에 따른 불이익 안내

: 본인은 위와 같이 개인정보를 수집·이용하는 데 대한 동의를 거부할 권리가 있습니다. 그러나 동의를 거부할 경우 [회원사명]에서 제공하는 [재화 또는 서비스의 명칭]을(를) 받을 수 없음을 참고하시기 바랍니다.

* 동의 거부에 따른 불이익이 없을 경우, 작성 하지 않아도 됨.

개인정보의 수집 및 이용에 동의하십니까? 동의함 동의하지 않음

■ 그 밖에 개인정보 취급에 관한 자세한 사항은 홈페이지(<http://www.oooo.co.kr>)에 공개하고 있는 “개인정보 처리방침”을 참고하시기 바랍니다.

 년 월 일 성명 : (인 또는 서명)

[회원사명] 귀중

[회원사명] 개인정보 제3자 제공 동의서

[회원사명]은(는) 개인정보보호법 등 관련 법령상의 개인정보 보호 규정을 준수하며 이용자의 개인정보 보호에 최선을 다하고 있습니다. **[회원사명]**은(는) 개인정보보호법 제17조제1항제1호에 근거하여, 다음과 같이 **[제공 목적]**을(를) 위하여 개인정보를 제3자에게 제공하는데 동의를 받고자 합니다.

1. 개인정보를 제공받는 자 : **[자연인은 성명, 법인 또는 단체는 그 명칭, 20%이상 글자크게, 진하게 작성]**
2. 개인정보를 제공받는 자의 개인정보 이용 목적 : (예: 처방 시 고려사항, 20%이상 글자크게, 진하게 작성)
3. 제공하는 개인정보의 항목 :
4. 개인정보를 제공받는 자의 개인정보 보유 및 이용기간 : [예 : 수집일(“00.00.00.)로부터 3개월, 20%이상 글자크게, 진하게 작성]
5. 동의거부권 및 동의 거부에 따른 불이익 안내
: **[환자 성명]**은(는) 위와 같이 개인정보를 제공하는 데 대한 동의를 거부할 권리가 있습니다. 그러나 동의를 거부할 경우 **[제공받는 기관]**에서 제공하는 **[재화 또는 서비스의 명칭]**을(를) 받을 수 없음을 참고하시기 바랍니다. * 동의 거부에 따른 불이익이 없을 경우, 작성 하지 않아도 됨.

개인정보의 제3자 제공에 동의하십니까? 동의함 동의하지 않음

- 그 밖에 개인정보 취급에 관한 자세한 사항은 홈페이지(<http://www.○○○.○○.kr>)에 공개하고 있는 “개인정보 처리방침”을 참고하시기 바랍니다.

 년 월 일 성명 : (인 또는 서명)

[회원사명] 귀중

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.

개인정보 처리 업무를 위탁하거나 위탁업무에 개인정보 처리가 포함된 경우에는 본 표준 개인정보처리위탁 계약서의 내용을 위탁계약서에 첨부하거나 반영하여 사용하실 수 있습니다.

표준 개인정보처리 위탁 계약서(안)

○○○(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 제2019-8호)에서 정의된 바에 따른다.

제3조 (위탁업무의 목적 및 범위) “을”은 계약이 정하는 바에 따라 () 목적으로 다음과 같은 개인정보 처리 업무를 수행한다.¹⁾

- 1.
- 2.

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

계약 기간 : 2000년 0월 0일 ~ 2000년 0월 0일

제5조 (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.

제6조 (개인정보의 안전성 확보조치) “을”은「개인정보 보호법」제23조제2항 및 제24조 제3항 및 제29조, 같은 법 시행령 제21조 및 제30조, 「개인정보의 안전성 확보조치 기준」(행정안전부 고시 제2019-47호)에 따라 개인정보의 안전성 확보에 필요한 기술적·관리적 조치를 취하여야 한다.

제7조 (개인정보의 처리제한) ① “을”은 계약기간은 물론 계약 종료 후에도 위탁업무 수행 목적 범위를 넘어 개인정보를 이용하거나 이를 제3자에게 제공 또는 누설하여서는 안 된다.

② “을”은 계약이 해지되거나 또는 계약기간이 만료된 경우 위탁업무와 관련하여 보유하고 있는 개인정보를 「개인정보 보호법 시행령」 제16조 및 「개인정보의 안전성 확보조치 기준」(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.

제8조 (수탁자에 대한 관리·감독 등) ① “갑”은 “을”에 대하여 다음 각 호의 사항을 감독할 수 있으며, “을”은 특별한 사유가 없는 한 이에 응하여야 한다.

1. 개인정보의 처리 현황
2. 개인정보의 접근 또는 접속기록
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 한다²⁾

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

제9조 (정보주체 권리보장) ① “을”은 정보주체의 개인정보 열람, 정정·삭제, 처리 정지 요청 등에 대응하기 위한 연락처 등 민원 창구를 마련해야 한다.

제10조 (개인정보의 파기) ① “을”은 제4조의 위탁업무기간이 종료되면 특별한 사유가 없는 한 지체 없이 개인정보를 파기하고 이를 “갑”에게 확인받아야 한다.

제11조 (손해배상) ① “을” 또는 “을”의 임직원 기타 “을”의 수탁자가 이 계약에 의하여 위탁 또는 재위탁 받은 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

○○시 ○○구 ○○동 ○○번지

성 명 : (인)

을

○○시 ○○구 ○○동 ○○번지

성 명 : (인)

-
- 1) 각호의 업무 예시 : 고객만족도 조사 업무, 회원가입 및 운영 업무, 사은품 배송을 위한 이름, 주소, 연락처 처리 등
 - 2) 「개인정보의 안전성 확보조치 기준」(행정안전부 고시 제2019-47호) 및 「개인정보 보호법」 제26조에 따라 개인정보처리자 및 취급자는 개인정보보호에 관한 교육을 의무적으로 시행하여야 한다.

○○ 병원은

**범죄예방과 시설안전을 위해
영상정보처리기기를 운영하고 있습니다.**

- ◎ 설치장소 및 대수 : 출입구 X대, 복도 X대
- ◎ 촬영범위 : 건물내부 출입구 근처 및 복도
- ◎ 촬영시간 : 24시간
- ◎ 관리책임자 : ○○병원 ○○처장 ○○○

(전화 XX-XXX-XXXX)

[붙임5] 개인정보파일 (등록, 변경등록) 신청서

개인정보파일 ([] 등록 [] 변경등록) 신청서

※ '변경정보 및 변경사유' 란은 변경등록시에만 작성합니다.

접수번호	접수일	처리기간	7일
공공기관 명칭	주소	등록부서	전화번호
등록항목	등록정보	변경정보 및 변경사유	
개인정보파일 명칭			
개인정보파일의 운영 근거 및 목적			
개인정보파일에 기록되는 개인정보의 항목			
개인정보의 처리방법			
개인정보의 보유기간			
개인정보를 통상적 또는 반복적으로 제공하는 경우 그 제공받는 자			
개인정보파일을 운용하는 공공기관의 명칭			
개인정보파일로 보유하고 있는 개인정보의 정보주체 수			
해당 공공기관에서 개인정보 처리 관련 업무를 담당하는 부서			
개인정보의 열람 요구를 접수·처리하는 부서			
개인정보파일에서 열람을 제한하거나 거절할 수 있는 개인정보의 범위 및 그 사유			

「개인정보 보호법」 제32조제1항과 같은 법 시행령 제34조제1항에 따라 위와 같이
개인정보파일 ([] 등록 [] 변경등록)을 신청합니다.

년 월 일

신청기관

(서명 또는 인)

행정안전부장관 귀하

210mm×297mm[일반용지 70g/㎡(재활용품)]

[붙임6] 개인정보 내부관리 계획 목차(예시)

개인정보 내부관리 계획 목차(예시)

- 내부관리 계획은 일반적으로 아래와 같은 내용을 포함하여야 한다.

목 차 (예 시)

제1장 총칙

제1조(목적)

제2조(적용범위)

제3조(용어 정의)

제2장 내부관리계획의 수립 및 시행

제4조(내부관리계획의 수립 및 승인)

제5조(내부관리계획의 공표)

제3장 개인정보 보호책임자의 역할과 책임

제6조(개인정보 보호책임자의 지정)

제7조(개인정보 보호책임자의 역할 및 책임)

제8조(개인정보취급자의 역할 및 책임)

제4장 개인정보 보호 교육

제9조(개인정보 보호책임자의 교육)

제10조(개인정보취급자의 교육)

제5장 기술적 안전조치

제11조(접근권한의 관리)

제12조(접근통제)

제13조(개인정보의 암호화)

제14조(접근기록의 보관 및 점검)

제15조(악성프로그램 등 방지)

제6장 관리적 안전조치

제16조(개인정보 보호조직 구성 및 운영)

제17조(개인정보 유출사고 대응)

제18조(위험도 분석 및 대응)

제19조(수탁자에 대한 관리 및 감독)

제7장 물리적 안전조치

제20조(물리적 안전조치)

제21조(재해 및 재난 대비 안전조치)

제8장 그 밖에 개인정보 보호를 위하여 필요한 사항

진료기록 열람 및 사본발급을 위한 확인서

확인자	성 명	생년월일 (외국인등록번호)
	환자와의 관계	
환자	성 명	생년월일 (외국인등록번호)
확인사항	상기 환자의 직계 존속·비속 및 환자의 배우자, 배우자의 직계존속의 부존재	

본인(확인자)은 「의료법」 제21조 제3항 및 같은 법 시행규칙 제13조의3의 제1항 및 제3항에 따라
상기 환자()의 배우자 및 직계 존속·비속, 배우자의 직계존속이 모두 없음을 확인합니다.

년 월 일

본인(확인자)

(자필서명)

유의사항

환자의 형제·자매가 「의료법 시행규칙」 [별표 2의2]에 따라 환자의 동의를 받을 수 없고, 환자의 배우자 및 직계 존속·비속, 배우자의 직계존속이 모두 없을 경우에 작성합니다.

210mm×297mm[백상지(80g/㎡) 또는 중질지(80g/㎡)]

진료기록 열람 및 사본발급 위임장

수임인	성 명	전 화 번 호
	생년월일(외국인등록번호)	위임인과의 관계
	주 소	
위임인	성 명	전 화 번 호
	생년월일(외국인등록번호)	
	주 소	

위임인은 「의료법」 제21조제2항 및 같은 법 시행규칙 제13조의2에 따라 「진료기록 등 열람 및 사본발급 동의서」에 기재된 사항에 대하여 일체 권한을 상기 수임인에게 위임합니다.

년 월 일

위임인

(자필서명)

[회원사명] 민감정보 처리 동의서

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

1. 민감정보의 수집·이용목적 :
2. 수집하려는 민감정보의 항목 : [예 : 질병, 병력, 유전정보 등, 20%이상 글자크게, 진하게 작성]
3. 민감정보의 보유 및 이용기간 : [20%이상 글자크게, 진하게 작성]
5. 동의거부권 및 동의 거부에 따른 불이익 안내
: **[환자 성명]**은(는) 위와 같이 민감정보를 수집·이용하는 데 대한 동의를 거부할 권리가 있습니다. 그러나 동의를 거부할 경우 **[회원사명]** 에서 제공하는 **[재화 또는 서비스의 명칭]**을(를) 받을 수 없음을 참고하시기 바랍니다. * 동의 거부에 따른 불이익이 없을 경우, 작성 하지 않아도 됨.

▪ 민감정보의 수집·이용에 동의하십니까? 동의함 동의하지 않음

- 그 밖에 개인정보 취급에 관한 자세한 사항은 홈페이지(<http://www.○○○.○○.kr>)에 공개하고 있는 “개인정보 처리방침”을 참고하시기 바랍니다.

년 월 일 성명 : (인 또는 서명)

[회원사명] 귀중

[붙임10]

개인정보 (열람 일부열람 열람연기 열람거절) 통지서

(앞 쪽)

수신자 (우편번호: , 주소:)

요구 내용						
열람 일시				열람 장소		
통지 내용 (<input type="checkbox"/> 열람 <input type="checkbox"/> 일부열람 <input type="checkbox"/> 열람연기 <input type="checkbox"/> 열람거절)						
열람 형태 및 방법	열람 형태	<input type="checkbox"/> 열람·시청	<input type="checkbox"/> 사본·출력물	<input type="checkbox"/> 전자파일	<input type="checkbox"/> 복제물·인화물	<input type="checkbox"/> 기타
	열람 방법	<input type="checkbox"/> 직접방문	<input type="checkbox"/> 우편	<input type="checkbox"/> 팩스	<input type="checkbox"/> 전자우편	<input type="checkbox"/> 기타
납부 금액	①수수료	원	②우송료	원	계(①+②)	원
	수수료 산정 명세					
사 유						
이의제기방법	※ 개인정보처리자는 이의제기방법을 적습니다.					

「개인정보 보호법」 제35조제3항·제4항 또는 제5항과 같은 법 시행령 제41조제4항 또는 제42조제2항에 따라 귀하의 개인정보 열람 요구에 대하여 위와 같이 통지합니다.

년 월 일

발 신 명 의 직인

210mm×297mm[신문용지 54g/㎡]

유의사항

1. 개인정보 열람 장소에 오실 때에는 이 통지서를 지참하셔야 하며, 요구인 본인 또는 그 정당한 대리인임을 확인하기 위하여 다음의 구분에 따른 증명서를 지참하셔야 합니다.
 - 가. 요구인 본인에게 공개할 때: 요구인의 신원을 확인할 수 있는 신분증명서(주민등록증 등)
 - 나. 요구인의 대리인에게 공개할 때: 대리인임을 증명할 수 있는 서류와 대리인의 신원을 확인할 수 있는 신분증명서
2. 수수료 또는 우송료는 다음의 구분에 따른 방법으로 냅니다.
 - 가. 국가기관인 개인정보처리자에게 내는 경우: 수입인지
 - 나. 지방자치단체인 개인정보처리자에게 내는 경우: 수입증지
 - 다. 국가기관 및 지방자치단체 외의 개인정보처리자에게 내는 경우: 해당 개인정보처리자가 정하는 방법

※ 국회, 법원, 헌법재판소, 중앙선거관리위원회, 중앙행정기관 및 그 소속 기관 또는 지방자치단체인 개인정보처리자에게 수수료 또는 우송료를 내는 경우에는 「전자금융거래법」 제2조제11호에 따른 전자지급수단 또는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제10호에 따른 통신과금서비스를 이용하여 수수료 또는 우송료를 낼 수 있습니다.
3. 열람제한, 열람연기 또는 열람거절의 통지를 받은 경우에는 개인정보처리자가 이의제기방법란에 적은 방법으로 이의제기를 할 수 있습니다.

[붙임11]

개인정보 ([] 정정·삭제, [] 처리정지) 요구에 대한 결과 통지서

수신자 (우편번호: , 주소:)

요구 내용	
<input type="checkbox"/> 정정·삭제 <input type="checkbox"/> 처리정지 조치 내용	
<input type="checkbox"/> 정정·삭제 <input type="checkbox"/> 처리정지 결정 사유	
이의제기방법	※ 개인정보처리자는 이의제기방법을 기재합니다.

「개인정보 보호법」 제36조제6항 및 같은 법 시행령 제43조제3항 또는 같은 법 제37조제5항 및 같은 법 시행령 제44조제2항에 따라 귀하의 요구에 대한 결과를 위와 같이 통지합니다.

년 월 일

발신명의

유의사항

개인정보의 정정·삭제 또는 처리정지 요구에 대한 결정을 통지받은 경우에는 개인정보처리자가 '이의제기방법'란에 적은 방법으로 이의제기를 할 수 있습니다.

210mm×297mm[신문용지 54g/㎡]

[붙임12]

개인정보 유출신고(보고)서

기관명					
정보주체에의 통지 여부					
유출된 개인정보의 항목 및 규모					
유출된 시점과 그 경위					
유출피해 최소화 대책·조치 및 결과					
정보주체가 할 수 있는 피해 최소화 방법 및 구제절차					
담당부서·담당자 및 연락처		성명	부서	직위	연락처
	개인정보 보호책임자				
	개인정보 취급자				

유출신고(보고) 접수기관	기관명	담당자명	연락처

[붙임13]

개인정보파일 파기 요청서

작성일		작성자	
파기 대상 개인정보파일			
생성일자		개인정보취급자	
주요 대상업무		현재 보관건수	
파기 사유			
파기 일정			
특기사항			
파기 승인일		승인자 (개인정보 보호책임자)	
파기 장소			
파기 방법			
파기 수행자		입회자	
파기 확인 방법			
백업 조치 유무			
매체 파기 여부			

[붙임14]

개인정보파일 파기 관리대장

번호	개인정보 파일명	자료의 종류	생성일	파기일	파기 사유	처리담당자	처리부서장

[붙임15]

개인영상정보 관리대장

번호	구분	일시	파일명/ 형태	담당자	목적/ 사유	이용· 제공받는 제3자 /열람등 요구자	이용· 제공 근거	이용·제공 형태	기간
1	<input type="checkbox"/> 이용 <input type="checkbox"/> 제공 <input type="checkbox"/> 열람 <input type="checkbox"/> 파기								
2	<input type="checkbox"/> 이용 <input type="checkbox"/> 제공 <input type="checkbox"/> 열람 <input type="checkbox"/> 파기								
3	<input type="checkbox"/> 이용 <input type="checkbox"/> 제공 <input type="checkbox"/> 열람 <input type="checkbox"/> 파기								
4	<input type="checkbox"/> 이용 <input type="checkbox"/> 제공 <input type="checkbox"/> 열람 <input type="checkbox"/> 파기								
5	<input type="checkbox"/> 이용 <input type="checkbox"/> 제공 <input type="checkbox"/> 열람 <input type="checkbox"/> 파기								
6	<input type="checkbox"/> 이용 <input type="checkbox"/> 제공 <input type="checkbox"/> 열람 <input type="checkbox"/> 파기								
7	<input type="checkbox"/> 이용 <input type="checkbox"/> 제공 <input type="checkbox"/> 열람 <input type="checkbox"/> 파기								

벌칙 규정

형량	요건	근거 법령
10년 이하의 징역 또는 1억원 이하의 벌금	공공기관의 개인정보 처리업무를 방해할 목적으로 공공기관에서 처리하고 있는 개인정보를 변경하거나 말소하여 공공기관의 업무 수행의 중단·마비 등 심각한 지장을 초래한 자	법 제70조제1호
	거짓이나 그 밖의 부정한 수단이나 방법으로 다른 사람이 처리하고 있는 개인정보를 취득한 후 이를 영리 또는 부정한 목적으로 제3자에게 제공한 자와 이를 교사·알선한 자 제17조제1항제2호에 해당하지 아니함에도 같은 항 제1호를 위반하여 정보주체의 동의를 받지 아니하고 개인정보를 제3자에게 제공한 자 및 그 사정을 알고 개인정보를 제공받은 자	법 제70조제2호
5년 이하의 징역 또는 5천만원 이하의 벌금	제18조제1항·제2항, 제19조, 제26조제5항 또는 제27조제3항을 위반하여 개인정보를 이용하거나 제3자에게 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자	법 제71조제2호
	제23조제1항을 위반하여 민감정보를 처리한 자	법 제71조제3호
	제24조제1항을 위반하여 고유식별정보를 처리한 자	법 제71조제4호
	제59조제2호를 위반하여 업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자	법 제71조제5호
	제59조제3호를 위반하여 다른 사람의 개인정보를 훼손, 멸실, 변경, 위조 또는 유출한 자	법 제71조제6호
	제25조제5항을 위반하여 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비추는 자 또는 녹음기능을 사용한 자	법 제72조제1호
3년 이하의 징역 또는 3천만원 이하의 벌금	제59조제1호를 위반하여 거짓이나 그 밖의 부정한 수단이나 방법으로 개인정보를 취득하거나 개인정보 처리에 관한 동의를 받는 행위를 한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자	법 제72조제2호
	제60조를 위반하여 직무상 알게 된 비밀을 누설하거나 직무상 목적 외에 이용한 자	법 제72조제3호
	제23조제2항, 제24조제3항, 제25조제6항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 아니하여 개인정보를 분실·도난·유출·위조·변조 또는 훼손당한 자	법 제73조제1호
2년 이하의 징역 또는 2천만원 이하의 벌금	제36조제2항을 위반하여 정정·삭제 등 필요한 조치를 하지 아니하고 개인정보를 계속 이용하거나 이를 제3자에게 제공한 자	법 제73조제2호
	제37조제2항을 위반하여 개인정보의 처리를 정지하지 아니하고 계속 이용하거나 제3자에게 제공한 자	법 제73조제3호

(양벌규정)	법인의 대표자나 법인 또는 개인의 대리인, 사용인, 그 밖의 종업원이 그 법인 또는 개인의 업무에 관하여 제70조에 해당하는 위반행위를 하면 그 행위자를 벌하는 외에 그 법인 또는 개인을 7천만원 이하의 벌금에 처한다.	법 제74조제1항
	법인의 대표자나 법인 또는 개인의 대리인, 사용인, 그 밖의 종업원이 그 법인 또는 개인의 업무에 관하여 제71조부터 제73조까지의 어느 하나에 해당하는 위반행위를 하면 그 행위자를 벌하는 외에 그 법인 또는 개인에게도 해당 조문의 벌금형을 과(科)한다.	법 제74조제2항

과태료 규정

부과액	요건	근거 법령
5천만원 이하	제15조제1항을 위반하여 개인정보를 수집한 자	법 제75조제1항제1호
	제22조제6항을 위반하여 법정대리인의 동의를 받지 아니한 자	법 제75조제1항제2호
	제25조제2항을 위반하여 영상정보처리기를 설치·운영한 자	법 제75조제1항제3호
3천만원 이하	제15조제2항, 제17조제2항, 제18조제3항 또는 제26조제3항을 위반하여 정보주체에게 알려야 할 사항을 알리지 아니한 자	법 제75조제2항제1호
	제16조제3항 또는 제22조제5항을 위반하여 재화 또는 서비스의 제공을 거부한 자	법 제75조제2항제2호
	제20조제1항 또는 제2항을 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 아니한 자	법 제75조제2항제3호
	제21조제1항을 위반하여 개인정보를 파기하지 아니한 자	법 제75조제2항제4호
	제24조의2제1항을 위반하여 주민등록번호를 처리한 자	법 제75조제2항제4호의2
	제24조의2제2항을 위반하여 암호화 조치를 하지 아니한 자	법 제75조제2항제4호의3
	제24조의2제3항을 위반하여 정보주체가 주민등록번호를 사용하지 아니할 수 있는 방법을 제공하지 아니한 자	법 제75조제2항제5호
	제23조제2항, 제24조제3항, 제25조제6항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 아니한 자	법 제75조제2항제6호
	제25조제1항을 위반하여 영상정보처리기를 설치·운영한 자	법 제75조제2항제7호
	제32조의2제6항을 위반하여 인증을 받지 아니하였음에도 거짓으로 인증의 내용을 표시하거나 홍보한 자	법 제75조제2항제7호의2
	제34조제1항을 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 아니한 자	법 제75조제2항제8호
	제34조제3항을 위반하여 조치 결과를 신고하지 아니한 자	법 제75조제2항제9호
	제35조제3항을 위반하여 열람을 제한하거나 거절한 자	법 제75조제2항제10호
	제36조제2항을 위반하여 정정·삭제 등 필요한 조치를 하지 아니한 자	법 제75조제2항제11호
제37조제4항을 위반하여 처리가 정지된 개인정보에 대하여	법 제75조제2항제12호	

	파기 등 필요한 조치를 하지 아니한 자	
	제64조제1항에 따른 시정명령에 따르지 아니한 자	법 제75조제2항제13호
1천만원 이하	제21조제3항을 위반하여 개인정보를 분리하여 저장·관리하지 아니한 자	법 제75조제3항제1호
	제22조제1항부터 제4항까지의 규정을 위반하여 동의를 받은 자	법 제75조제3항제2호
	제25조제4항을 위반하여 안내판 설치 등 필요한 조치를 하지 아니한 자	법 제75조제3항제3호
	제26조제1항을 위반하여 업무 위탁 시 같은 항 각 호의 내용이 포함된 문서에 의하지 아니한 자	법 제75조제3항제4호
	제26조제2항을 위반하여 위탁하는 업무의 내용과 수탁자를 공개하지 아니한 자	법 제75조제3항제5호
	제27조제1항 또는 제2항을 위반하여 정보주체에게 개인정보의 이전 사실을 알리지 아니한 자	법 제75조제3항제6호
	제30조제1항 또는 제2항을 위반하여 개인정보 처리방침을 정하지 아니하거나 이를 공개하지 아니한 자	법 제75조제3항제7호
	제31조제1항을 위반하여 개인정보 보호책임자를 지정하지 아니한 자	법 제75조제3항제8호
	제35조제3항·제4항, 제36조제2항·제4항 또는 제37조제3항을 위반하여 정보주체에게 알려야 할 사항을 알리지 아니한 자	법 제75조제3항제9호
	제63조제1항에 따른 관계 물품·서류 등 자료를 제출하지 아니하거나 거짓으로 제출한 자	법 제75조제3항제10호
제63조제2항에 따른 출입·검사를 거부·방해 또는 기피한 자	법 제75조제3항제11호	