개인정보 보호 자율규제 규약

- 약국 -

2020. 6. 30

대한약사회
THE KOREAN PHARMACEUTICAL ASSOCIATION

목 차

개인정보보호 자율규제 규약

2017. 8. 17 제정
2018. 4. 17 개정
2019. 4. 10 개정
2020. 6. 30 개정

제1장 총칙

1. 목적

이 규약은 관련 규정에 따라 사단법인 대한약사회(이하 "본회"라 한다)와 그 회원사가 수행하는 개인정보 보호 및 자율규제 활동에 관한 사항을 정함으로써 회원사의 개인정보 보호 수준 제고 및 개인정보 관련 분쟁을 예방하기 위한 내용을 정하는데 목적이 있다.

▶관련규정
① 「개인정보 보호법」 제5조제3항, 제13조제2호, 제4호 및 제5호
② 「개인정보 보호법 시행령」 제14조
③ 「개인정보보호 자율규제단체 지정 등에 관한 규정」 제11조
(**행정안전부 고시 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 「약사법」 제3조제2항 및 제20조에 따라 **본회에 입회한** 약국을 말한다.
④ **"조제정보"**란 의사 또는 치과의사의 처방전에 따라 의약품 조제 및 복약지도를 목적으로 수집하여 처리하는 개인정보가 포함된 정보로써 조제기록부(전자문서로 작성된 것을 포함한다)로 관리되는 정보를 말한다.
⑤ **"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.
⑥ **"개인정보처리시스템"**이란 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템을 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 개인정보 파일을 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」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 행정안전부 장관이 자율규제단체 지정 등에 관한 업무를 위하여 구성·운영하는 협의회를 말한다.

3. 개인정보 보호 원칙

본회와 회원사는 다음의 원칙을 준수하며, 개인정보 보호 관련 업무 및 활동을 한다.

① 처리목적의 명확화 원칙
회원사는 개인정보의 처리 목적을 명확하게 하여야 한다.
② 최소수집의 원칙
회원사는 처리 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.
③ 적법한 수집 원칙
회원사는 개인정보를 적법하고 정당하게 수집하여야 한다.
④ 목적 외 이용금지 원칙
회원사는 처리 목적에 직접적으로 필요한 범위 내에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하지 않아야 한다.
⑤ 정확성의 원칙
회원사는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.
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 한다.

⑦ 공개의 원칙
회원사는 개인정보처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 한다.
⑧ 정보주체 권리 존중의 원칙
회원사는 열람청구권, 정정·삭제요구권, 처리정지요구권 등 정보주체의 권리를 보장하여야 한다.
⑨ 사생활 침해 최소화의 원칙
회원사의 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.
⑩ 익명처리의 원칙
회원사는 개인정보를 적법하게 수집한 경우에도 익명에 의하여 업무 목적을 달성할 수 있으면 개인정보를 익명에 의하여 처리될 수 있도록 하여야 한다.
⑪ 책임의 원칙
회원사는 개인정보 보호 관련 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.

4. 관련 법령의 준수

이 규약은 본회와 회원사 사이의 개인정보 보호 활동 의지를 확인하고 자율규제 활동을 통하여 이를 실현하고자 하는 약속으로서의 효력을 지닌다. 이 규약에서 정하고 있지 않은 회원사의 개인정보 보호 활동에 대해서는「약사법」,「국민건강보험법」,「개인정보 보호법」등 관련 법령이 정하는 바에 따른다.

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

5. 자율규제단체

가. 자율규제단체의 지위 및 역할

회원사는 본회가「개인정보보호 자율규제단체 지정 등에 관한 규정」에 따른 자율규제단체임을 확인하며, 본회는 자율규제단체로서 회원사를 대상으로 다음과 같은 업무를 수행한다.

① 개인정보 보호 교육 및 홍보 활동
② 개인정보 보호 자율규제 규약의 제·개정
③ 개인정보 자율점검 및 컨설팅
④ 개인정보 보호 관리 시스템의 설치 및 운영
⑤ 그 밖의 개인정보 보호에 관한 업무

나. 보고의무

① 본회는 연 1회 개인정보보호 자율규제 수행결과를 자율규제협의회에 보고하여야 한다.

② 본회는 법령에 근거한 정부의 조사요청에 따라 회원사의 자율점검 자료를 제공할 수 있으며, 필요한 경우 회원사로부터 추가로 정보를 수집할 수 있다.

다. 자율점검의 실시

① 본회는 회원사의 개인정보 처리실태를 점검하고 미흡한 점을 개선하도록 지도할 수 있다.

② 개인정보 처리실태 점검은 회원사가 온라인으로 시스템에 접속하여 점검하는 자가점검과 회원사를 직접 방문하는 현장컨설팅으로 한다.

③ 본회는 회원사의 실태점검을 하기 최소 1개월 전에 회원사가 스스로 개인정보 처리실태를 점검할 수 있도록 「표준 자율점검표」를 마련하여 배포하여야 한다.

라. 자율점검에 따른 포상 및 인센티브

①「개인정보보호 자율규제단체 지정 등에 관한 규정」제15조(수행계획에 따른 결과의 평가 등) 제2항에 따라 평가 결과가 우수한 회원사는 행정안전부 장관 포상을 받을 수 있다.

②「개인정보보호 자율규제단체 지정 등에 관한 규정」제15조의2(자료제출 및 검사의 면제 등) <개정 2019.4.10.>

※ 행정안전부 장관은 자율규제단체 소속 회원사가 자율규제 규약을 충실히 준수하고 자율점검을 성실히 수행하여 수행결과가 우수하다고 인정되는 경우 인센티브

(행정안전부 개인정보협력과 2019-8호, 2019.1.29.)

- 자료제출 요구 및 검사를 1년간 면제

마. 자율규제단체 소속 회원사 참여 제한 <신설 2019.4.10.>

본회는 소속 회원사가 다음의 어느 하나에 해당하는 경우에는 자율규제 활동의 전부 또는 일부를 1년간 제한할 수 있다.

① 법 위반으로 인해 형벌 또는 행정처분을 받은 경우

② 이 자율규제 규약에 따라 회원사의 개인정보 처리실태에 따른 개선을 지도 받았음에도 불구하고 이를 이행하지 아니한 경우

③ 회원사가 자율점검을 허위 또는 불성실하게 이행한 경우

6. 회원사의 권리

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

7. 자율규제 규약

① 행정안전부 자율규제 협의회의 검토와 본회 상임이사회의 승인을 득하여 본 규약을 제정 및 개정할 수 있다.

② 본회는 회원사가 이 규약을 준수하도록 지도·권고 등 필요한 조치를 할 수 있다.

③ 회원사는 개인정보 보호 활동을 하며 이 규약을 준수하도록 노력해야 한다.

④ 본 규약은 본회가 자체적으로 회원사를 대상으로 자율규제 활동을 할 수 있는 근거가 되는 실무지침으로서, 법률적 검토와 실행은 개인정보보호법령과 지침을 우선 적용하여야 한다.

8. 자율규제단체에 대한 지원(전문기관)

① 전문기관은 자율규제단체의 개인정보보호 활동 등 관련 업무를 지원한다.

② 의약분야 개인정보보호 자율규제 전문기관인 건강보험심사평가원은 개인정보보호 전문인력 지원, 자율점검 현장컨설팅 지원, 개인정보보호 전문교육 실시, 보안도구의 제공 등 기술지원 및 자율규제 규약 검토 등의 역할을 지원할 수 있다.

9. 회원사 수집정보 및 점검결과에 대한 정보 제공

① 본회는 회원사 수집정보 및 점검결과에 대해 행정안전부, 보건복지부, 건강보험심사평가원, 한국인터넷진흥원에 해당 내용을 제공할 수 있다.

제2장 개인정보 처리단계별 조치기준

1. 개인정보의 수집·이용

회원사는 최소수집의 원칙에 따라 목적에 필요한 최소한의 개인정보를 수집하여야 하며, 그 수집목적의 범위에서 이용하여야 한다. 필요한 최소한의 개인정보에 관한 입증책임은 회원사가 진다.

가. 개인정보 수집·이용 요건

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

○ 법률에 특별한 규정이 있거나 법령상 의무 준수를 위해 불가피한 경우

○ 정보주체의 동의를 받은 경우

* 이 경우 회원사는 정보주체에게 다음 사항을 고지하여야 한다.

① 개인정보의 수집·이용 목적(예: 홍보 및 마케팅 목적의 SMS발송, 회원가입 등)
② 수집하려는 개인정보의 항목(예: 성명, 주소, 연락처, 생년월일 등)
③ 개인정보의 보유 및 이용 기간
*** 회원 탈퇴 시까지(회원 가입의 경우)**
④ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용
▶ 이 중 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.
▶ 위반 시, 3천만원 이하의 과태료 부과(법 제75조)

○ 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 약사 또는 직원의 징계, 각종 소청 또는 소송의 제기 및 진행 등을 위하여 증빙자료를 조사하고 확보하는 경우

2) 조제, 복약상담 목적 외로 수집한 개인정보 중 14세 미만 아동 개인정보가 있을 경우, 개인정보 수집 시 법정대리인으로부터 동의를 받아야 함

나. 개인정보의 수집 제한과 입증책임

1) 개인정보 수집 목적에 필요한 범위 내에서 최소한의 개인정보(필수정보)만을 수집하여야한다.

○ 서면(오프라인) 또는 홈페이지(온라인)등에서 개인정보를 수집하는 경우, 목적 달성을 위해 반드시 수집하여야 하는 최소한의 개인정보만을 수집

○ 필수정보는 아니나, 추가적인 서비스 제공 등을 위해 필여한 정보(선택정보)로 수집하는 경우에도 목적 달성을 위한 최소한의 정보를 수집

○ 필요한 최소한의 정보(필수정보) 외의 개인정보(선택정보) 수집에는 동의하지 아니할 수 있다는 사실을 명확하게 알려야 함

2) 최소한의 개인정보(필수정보) 외의 개인정보(선택정보) 수집에 동의하지 않아도 기본적인 서비스 제공(예: 회원가입)이 가능하여야 한다.

3) 회원사(개인정보처리자)가 개인정보의 처리에 대하여 환자(정보주체)의 동의를 받을 때에는 환자가 동의사항을 명확하게 인지할 수 있도록 구분하고 각각 동의를 받아야 한다.

<구분 동의가 필요한 경우>

① 개인정보 수집·이용 동의
② 마케팅 목적 처리 동의
③ 제3자 제공 동의
④ 목적 외 이용·제공 동의
⑤ 법정대리인 동의
⑥ 민감정보 처리 동의
⑦ 고유식별정보 처리 동의
⑧ 국외 제3자 제공 동의
※ ②, ④와 같은 경우에는 목적별로 각각 동의를 받아야 함

다. 고유식별정보·민감정보의 처리 제한

1) 본 항에서의 '고유식별정보'란 주민번호, 여권번호, 운전면허번호, 외국인등록번호를 말하며, '민감정보'란 사상·신념, 정치적 견해, 건강, 성생활 및「개인정보 보호법 시행령」에 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 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우*
② 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우

*「국민건강보험법」 제47조, 「약사법」 제23조의3(의약품안전사용정보시스템의 구축·운영 등) 및 동법 시행규칙 제15조의3(정보시스템의 구축·운영) 등

2) 회원사는 주민등록번호를 보관할 시 암호화 조치를 통하여 안전하게 보관하여야 한다. 암호화 조치를 어긴 경우 5천만원 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 3천만원 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

* 이 경우 회원사는 정보주체에게 다음의 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
▶ 이 중 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.
▶ 위반 시, 5천만원 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

- 건강보험심사평가원에 요양급여청구를 위한 제공(「국민건강보험법」 제47조)
- 응급환자의 치료를 위한 응급의료기관 요청에 따른 제공(「응급의료법」 제5조2항)
- 한국의약품안전관리원에 약품에 대한 부작용 등의 보고(「약사법」 제68조의8, 제21조제3항 4호 등)
- 「약사법」 제30조(조제기록부) 제3항 요건을 부합하는 경우에 한하여만 환자에 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. 금지되는 개인정보 제공 행위

1) 업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공하는 행위는 5년 이하의 징역 또는 5천만원 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 : 처방전 보관/폐기, 청구SW 유지보수, CCTV 운영 등)를 위탁하는 경우 아래 사항이 포함된 문서로 하여야 한다.

<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 '개인정보처리방침'으로 지속적으로 게재하여야 한다.
2) 인터넷 홈페이지에 게재할 수 없는 경우에는 약국의 보기 쉬운 장소에 위탁하는 업무의 내용과 수탁자를 공개하여야 한다.

다. 수탁자 교육 및 감독

1) 개인정보처리업무를 위탁한 회원사는 수탁자에 대하여 개인정보가 분실 · 도난 · 유출 · 변조 · 훼손되지 않도록 교육하여야 한다.
2) 개인정보처리업무를 위탁한 회원사는 수탁자가 '개인정보 보호법과 시행령'에 따라 준수하고 있는지 감독하여야 한다.

라. 손해배상 책임

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

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 한다.
   ○ 정보주체가 최소한 이전 사실을 확인하고 회원탈퇴, 동의철회 등의 권리를 행사할 수 있는 시간적 여유를 주어야 한다.

2) 회원사는 영업양도 등에 따라 개인정보 이전 사실을 통지하여야 한다.

3) 개인정보를 이전받은 회원사는 정보주체에게 개인정보의 이전사실 등을 개인정보를 이전받은 후 지체 없이 통지*하여야 한다.
   ○ 회원사가 개인정보의 이전사실 등을 이미 알린 경우에는 통지하지 않아도 된다

* 통지사항
  - 개인정보를 이전하려는 사실
  - 개인정보를 이전받는 자(영업양수자 등)의 성명, 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 한다.
  - 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법
  - 개인정보를 이전하려는 약국이 과실 없이 서면 등에 따른 방법으로 통지사항을 정보주체에게 알릴 수 없는 경우에는 해당 사항을 인터넷 홈페이지에 30일 이상 게재하여야 한다.
  - 다만, 인터넷 홈페이지를 운영하지 아니하는 약국은 사업장 등의 보기 쉬운 장소에 30일 이상 게시하여야 한다.

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 진다.

○ 영업의 양도, 합병 당시의 처리 목적과 다른 용도로 개인정보를 이용하고자 하는 경우에는 정보주체로부터 별도로 동의를 받아야 한다.

5. 영상정보처리기기의 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 설치는 원칙적으로 금지되지만, 예외적으로 다음의 사유에 해당하는 경우에는 설치할 수 있다.

<영상정보처리기기 설치·운영 사유>
① 법령에서 구체적으로 허용하고 있는 경우
② 범죄의 예방
③ 시설안전 및 화재 예방을 위하여 필요한 경우

2) 개인의 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있도록 하는 영상정보처리기기 설치・운영은 금지한다.

나. 영상정보처리기기 임의조작・녹음 금지

1) 영상정보처리기기는 설치목적과 다른 목적으로 임의로 조작하거나 다른 곳을 비추거나 녹음기능을 사용하는 것은 금지된다.

다. 안내판 설치를 통한 설치・운영 사실 공개

1) 회원사가 공개된 장소에 영상정보처리기기를 설치・운영할 때 정보주체가 쉽게 알아 볼 수 있도록 안내판을 설치하여야 한다.

라. 영상정보처리기기 운영・관리 방침

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

마. 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

2) 영상정보처리기기를 운영하는 회원사는 개인영상정보는 영상정보처리기기 운영·관리 방침에 보관기관을 명시할 수 있고 기간 산정이 곤란한 때에는 보관기간을 개인영상정보 수집 후 30일 이내로 정할 수 있으며, 이 기간이 종료한 때에는 파기하여야 한다.

바. 영상정보처리기기의 설치・운영 위탁 시 관리・감독 철저

1) 영상정보처리기기를 운영하는 회원사는 영상정보처리기기의 설치・운영에 관한 사무를 위탁할 수 있으며, 이 경우 개인정보 처리업무 위탁에 관한 규정을 준수하여야 한다.

사. 개인영상정보 열람·존재확인·파기 청구권 보장

1) 영상정보처리기기를 운영하는 회원사는 정보주체로부터 개인영상정보의 열람, 존재확인 또는 파기를 요청받은 경우 지체 없이 필요한 조치를 취해야 한다.

아. 개인영상정보의 안전성 확보 조치 및 자체 점검 실시

1) 영상정보처리기기를 운영하는 회원사는 개인영상정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 조치를 하여야 한다.

6. 개인정보의 안전성 확보조치

회원사는 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 안전성 확보에 필요한 조치를 하여야 한다.

가. 원칙

회원사는 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.

<개인정보처리자 유형 및 개인정보 보유량에 따른 안전조치 적용 유형>

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

다. 내부관리 계획수립 시행

1) 회원사(개인정보처리자)는 개인정보를 안전하게 처리하기 위하여 내부 의사결정 절차를 통하여 내부기준을 수립하여 시행하여야 한다.

<내부관리계획 수립 시 필수 반영사항>

① 개인정보 보호책임자의 지정에 관한 사항
② 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항
③ 개인정보취급자에 대한 교육에 관한 사항
④ 접근 권한의 관리에 관한 사항
⑤ 접근 통제에 관한 사항
⑥ 개인정보의 암호화 조치에 관한 사항
⑦ 접속기록 보관 및 점검에 관한 사항
⑧ 악성프로그램 등 방지에 관한 사항
⑨ 물리적 안전조치에 관한 사항
⑩ 개인정보 보호조직에 관한 구성 및 운영에 관한 사항
⑪ 개인정보 유출사고 대응 계획 수립·시행에 관한 사항
⑫ 그 밖에 개인정보보호를 위하여 필요한 사항

○ 회원사(개인정보처리자)는 각 호의 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 함

라. 접근권한 관리 및 접근통제

1) 회원사(개인정보처리자)는 개인정보처리시스템에 대한 접근권한을 각 업무담당자별로 1인 1계정을 부여하여야 한다.

○ 회원사(개인정보처리자)는 개인정보처리시스템에 대한 접근권한을 업무수행에 필요한 최소한의 범위로 업무담당자에 따라 차등 부여하여야 한다.

※ 단, 총 1만명 미만의 환자(정보주체) 개인정보를 보유한 소상공인(상시근로자 수 5인 미만)의 경우 해당없음

2) 회원사(개인정보처리자)는 권한 부여·변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.

○ 회원사(개인정보처리자)는 전보 또는 퇴직 등 인사이동이 발생하여 직원(개인정보취급자)이 변경되었을 경우 지체 없이 개인정보 처리시스템의 접근권한을 변경 또는 말소하여야 한다.

3) 회원사(개인정보처리자)는 직원(개인정보취급자) 또는 환자(정보주체)가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다.

<비밀번호 작성규칙>

① 비밀번호 최소길이
- 최소10자리: 영대문자(A~Z), 영소문자(a~z), 숫자(0~9), 특수문자(32개) 중 2종류 이상의 조합
- 최소8자리: 영대문자(A~Z), 영소문자(a~z), 숫자(0~9), 특수문자(32개) 중 3종류 이상의 조합

② 추측하기 어려운 비밀번호 사용
- 일련번호, 전화번호 등 쉬운 문자열이 포함되지 않도록 한다
- 잘 알려진 단어, 키보드 상에 나란히 있는 문자열이 포함되지 않도록 한다
- 사용자 ID와 동일한 비밀번호는 사용하지 않도록 한다

③ 비밀번호의 주기적인 변경 및 동일한 비밀번호 사용 제한
- 비밀번호를 최소 6개월마다 변경하여 동일한 비밀번호를 장기간 이용하지 않도록 관리
- 2개의 비밀번호를 교대로 사용하지 않도록 한다

④ 비밀번호 설정·변경할 때 입력값의 자리수와 조합을 체크하여 안전한 비밀번호 작성 규칙에 위배되는 경우, 법 위반을 알리고 작성규칙을 준수하도록 한다

4) 불법적인 접근 및 침해사고 방지를 위해 아래 방법중 하나 이상 적용하여야 한다.
○ 컴퓨터의 운영체제(윈도우 등)의 기본 기능을 이용하여 방화벽 운영
○ 보안프로그램(백신)의 방화벽 기능을 이용
○ 보안업체 등에서 제공하는 보안 서비스(침입방지시스템 등)를 활용하여 방화벽 설치

5) 외부망으로부터 개인정보처리시스템에 대한 접속은 원칙적으로 차단하여야 한다. 다만 회원사 직원(개인정보취급자)이 외부망을 통해 개인정보처리시스템에 접속이 필요한 경우에는 가상사설망(VPN: Virtual Private Network)또는 전용선 등의 안전한 접속수단을 적용하거나 안전한 인증수단(공인인증서, 일회용 비밀번호(OTP), 보안토큰 등)을 적용해야 한다.

6) 회원사(개인정보처리자)는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망(Wifi)이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터 및 모바일 기기 등에 조치를 하여야 한다.
○ 기업용 백신SW 등 프로그램을 이용하여 접속 차단 가능함
※ 방화벽(V3) 또는 브라우저(IE)등을 통해 유해 사이트 차단 기능
○ 차단이 힘든 경우 해당 비인가 프로그램을 삭제 조치하고 다시 설치되지 않도록 관리
○ 윈도우계열 OS의 경우 “시작>제어판>성능 및 유지관리>관리도구>컴퓨터관리”에서 공유폴더가 있는지 확인 가능
※ 공유폴더를 이용하여 업무를 진행해야 되는 경우, 공유폴더에 암호 설정 및 사용 후 공유폴더를 해제해야 함
○ 공유기를 이용한 무선망을 사용하는 경우 안전한 비밀번호를 적용해야 함

7) 회원사(개인정보처리자)는 인터넷 홈페이지를 통해 개인정보가 유출되지 않도록 연 1회 이상 홈페이지를 점검하는 것을 권장한다.

마. 개인정보 암호화

1) 고유식별정보, 비밀번호 및 바이오정보를 개인정보처리시스템(전자차트, 홈페이지, 청구S/W 등)에 저장 시 암호화 조치를 취해야 한다.

○ 비밀번호는 일방향암호화 하여야 함

※ 일방향암호화: 저장된 값으로 원래 값을 유추하거나 복원할 수 없도록 하는 방법

○ 바이오정보는 식별 및 인증 등의 고유기능으로 사용하는 경우에만 암호화 대상임(CT영상 등 의료행위 관련 바이오정보는 제외)

2) 업무용 컴퓨터 또는 모바일 기기에 고유식별정보, 비밀번호 및 바이오정보를 저장하여 관리하는 경우 안전한 암호화 알고리즘이 적용된 암호화 소프트웨어를 사용하여 암호화한 후에 저장하여야 한다.

○ 업무용 PC 및 모바일기기에 문서파일(hwp, xls, txt 등) 형태로 고유식별정보, 비밀번호 및 바이오정보를 보관 시 아래와 같은 방법으로 암호화 할 수 있음

- 문서편집기(한글, MS-Office 등)에서 제공하는 비밀번호 설정 기능
- 압축프로그램을 이용한 파일 압축 및 비밀번호 설정

※ 비밀번호 설정 시 단순 숫자 또는 문자열 사용 금지

3) 고유식별정보, 비밀번호 및 바이오정보를 정보통신망을 통하여 송·수신하거나 보조저장매체 등을 통해 전달하는 경우 암호화하여야 한다.

○ 개인정보가 포함된 문서파일(hwp, xls, txt 등)은 문서편집기 및 압축프로그램에서 제공하는 비밀번호 설정 기능을 통하여 암호화 후 송·수신 가능 함

※ 비밀번호 설정 시 단순 숫자 또는 문자열 사용 금지

○ 홈페이지에서 개인정보를 수집하는 기관의 경우 SSL/TLS 등의 통신 암호화를 적용하여야 함

바. 접속기록의 보관 및 위·변조 방지 <개정 2019.6.7>

1) 개인정보취급자가 개인정보처리시스템(전자차트, 청구S/W 등)에 접속한 기록을 1년 이상 보관·관리하여야 한다.(다만, 5만명 이상의 정보주체에 관하여 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 경우 2년 이상 보관·관리)

※ 접속기록: 개인정보취급자등이 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 개인정보취급자 등의 계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 전자적으로 기록한 것을 말함

○ 개인정보처리시스템을 위탁·운영하는 경우 수탁업체에 1년 이상 접속기록 보관 여부를 확인하여야 함

※ 해당 기능이 불가능한 개인정보처리시스템인 경우, 수탁업체에 기능 추가를 요청하여야 함

○ 회원사(개인정보처리자)는 개인정보의 유출·변조·훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 하며, 개인정보 다운로드가 발견된 경우 내부관리계획으로 정하는 바에 따라 그 사유를 반드시 확인

※ 접속기록의 필수 항목(5개): 개인정보취급자 등의 계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무

2) 대표자는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.

사. 보안 프로그램의 설치 및 운영

1) 회원사(개인정보처리자)는 악성프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 한다.

- 업무용 PC에는 개인용 백신S/W가 아닌 기업용 백신S/W를 사용하여야 함
- 기업용 백신S/W가 없는 경우, 심평원 제공 DUR모듈에 포함된 백신S/W(AhnLab Online Security)를 사용 가능
- 백신S/W는 항상 활성화 시켜두고, 월 1회 이상 정기적으로 검사하는 것을 권장

○ 보안 프로그램의 자동 업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지하여야 함

- 보안 프로그램 등을 통하여 발견된 바이러스, 트로이목마 등의 악성프로그램 등에 대해 삭제, 치료 등의 대응 조치를 취하여야 함

○ 사용 중인 으용 프로그램(한컴 오피스, ms 오피스 등)이나 운영체제 소프트웨어(Windows 7, 10 등)의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시하여야 함

아. 물리적 접근방지

1) 회원사(개인정보처리자)는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다.

2) 회원사(개인정보처리자)는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.

○ 개인정보가 포함된 서류, 보조저장매체 등의 보관 시, 별도 보관 장소가 없는 경우나 임시로 보관이 필요한 경우에는 잠금 장치가 있는 보관시설(캐비닛, 금고 등)에 보관하여야 함

7. 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 경과한 조제기록부, 처방전, 요양급여청구서류나 수집·목적을 달성한 기타 개인정보에 대해서는 지체 없이 파기하는 것이 바람직하다.
   ○ 개인정보 보호책임자는 파기 계획수립, 시행 등을 관리하여야 하며, 그 사실을 기록하고 관리하여야 한다.
2) 약국 개설자가 폐업하는 경우 개인정보보호법 제27조에 근거하여 개인정보 보유목적이 달성된 것으로 보아, 보유하고 있는 개인정보는 파기하는 것을 원칙으로 하나, 조제기록부·처방전·요양급여청구서류 등 약사법, 국민건강보험법에 의해 일정기간 보관이 의무화된 정보는 약국대표자가 의무기간 동안 보관해야 한다.
3) 정보주체가 회원사의 인터넷 홈페이지 회원에서 탈퇴하는 경우에는 더 이상 해당 정보주체의 개인정보를 보유할 이유가 없으므로 회원사는 정보주체가 탈퇴한 날부터 5일 이내에 파기하여야 한다.
4) 회원사의 개인정보 보존기간과 보존방법은 다음과 같다.

< 조제기록 보존기간 >

종 류	보존기간
처방전	2년(요양급여/의료급여비용 청구 처방전 3년)
조제기록부	5년
요양급여비용청구정보	5년

5) 개인정보를 파기할 때에는 개인정보가 복구 또는 재생되지 않도록 조치하여야 한다.
6) 회원사는 수집·이용목적을 달성하거나 보유기간에 도달한 조제정보 등 개인정보는 지체 없이 파기하는 것이 바람직하다.
   ○ 환자 등 정보주체로부터 개인정보 보유·이용기간에 대한 법적 의무보존기간 이외의 기간 동안 활용할 수 있도록 동의를 받은 경우에는 보존기간을 연장할 수 있다.
   ○ 약국개설자가 조제정보의 연장보관이 필요하다고 판단하는 경우에는 공공기관의 기록물관리에 준하는 절차(예: 조제기록심의회와 같은 내부심의절차)를 거쳐 보존기간 연장 또는 폐기를 결정할 수 있다.
   (보건복지부·안전행정부 '개인정보 가이드라인 [약국 편]' 2013.12.)

8. 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 한다.

< 개인정보처리방침에 포함되어야 하는 필수 사항 >

① 개인정보의 처리목적
② 개인정보의 처리 및 보유기간
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 자동수집 장치의 설치·운영 및 그 거부에 관한 사항

9. 개인정보 보호책임자 지정

1) 개인정보의 처리에 관한 업무 총괄 및 다음의 업무 수행을 위해 개인정보 보호책임자를 지정하여야 한다.

< 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 그 밖에 개인정보 보호를 위하여 필요한 업무

※ 개인정보 보호책임자 미지정시 1천만원 이하 과태료 부과(법 제75조제3항제8호)

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

① 약국장 ② 개인정보 보호 업무를 담당하는 부서의 장 ▶ 사업주 또는 대표자가 아닌 경우에는, 인사 발령 등 공식적인 지정 절차 필요

10. 개인정보 유출방지 등

1) 개인정보 유·노출 및 침해사고를 통하여 발생할 수 있는 사회적, 경제적 피해 등 2차 피해를 예방하기 위하여 개인정보 침해사고 대응 범위, 절차, 신고방법 등 침해사고 대응절차를 숙지하여야 한다.

○ 회원사(개인정보처리자)는 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이(5일 이내) 환자(정보주체)에게 통보하여야 함

<통보하여야 할 내용>
① 유출된 개인정보의 항목 ② 유출 시점 및 그 경위 ③ 피해 최소화를 위한 정보주체의 조치방법 ④ 기관의 대응조치 및 피해구제 절차 ⑤ 피해 신고 접수 담당부서 및 연락처 ※ 통보 방법으로는 서면, 이메일, SMS 통보 등의 방법을 이용

○ 1천 명 이상의 환자(정보주체)의 개인정보가 유출된 경우 유출 통지 결과를 신고하여야 함

- 행정안전부 또는 전문기관(한국인터넷진흥원)에 신고하여야 함
- 추가적으로 홈페이지 혹은 대기실 등 원내 보기 쉬운 장소에 7일 이상 게시하여야 함

제3장 별첨

1. 각종 서식

[붙임1] 개인정보 수집·이용 동의서(예시)

ㅇㅇㅇ서비스 제공을 위한 개인정보 수집·이용, 제공 동의서(예시)

ㅇㅇ약국은 ㅇㅇㅇ서비스 제공을 위하여 아래와 같이 개인정보를 수집·이용 및 제공하고자 합니다. 내용을 자세히 읽으신 후 동의 여부를 결정하여 주십시오.

☐ 선택적 개인정보 수집·이용 내역(선택사항, 동의거부 가능)

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

※ 위의 개인정보 수집·이용에 대한 동의를 거부할 권리가 있습니다. 다만, 이에 동의하지 않는 경우에는 맞춤형 건강정보(서비스명 구체화) 제공이 제한됩니다.

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

☐ 개인정보 제3자 제공 내역(선택사항, 동의거부 가능)

제공받는 기관	제공목적	제공하는 항목	보유기간
ㅇㅇ연구소	맞춤형 건강정보 연구	성별, 결혼 여부, 연령, 관심분야	1년

※ 위의 개인정보 제공에 대한 동의를 거부할 권리가 있습니다. 다만, 이에 동의하지 않는 경우에는 맞춤형 건강정보(서비스명 구체화) 서비스 제공이 제한됩니다.

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

<기타 고지 사항>

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

개인정보 처리사유	개인정보 항목	수집 근거
조제기록부 작성	성명, 주민등록번호, 주소, 연락처 등 인적사항	「약사법」 제30조

년 월 일

본인 성명 (서명 또는 인)

법정대리인 성명 (서명 또는 인)

ㅇㅇ약국장 귀중

[붙임2] 개인정보 처리방침(예시)

【 개인정보 처리방침 】

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

이 개인정보 처리방침의 순서는 다음과 같습니다.

1. 수집하는 개인정보의 항목 및 수집방법

A는 *처방·조제*를 **위해 필요한** *처방전*과 **건강보험급여 청구에 필요한 최소한의 개인정보만을 수집**합니다.

- 수집항목: *성명, 주민등록번호, 주소, 연락처, (관련내용 등)*
- 수집방법: 관련법(*「의료법」, 「약사법」*)에 의해 개인정보가 포함된 *문서명(처방전 등)*을 접수
  (관련법에 따라 정보주체의 별도 동의 없이 개인정보 수집 가능)

2. 개인정보의 수집 및 이용목적

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

3. 개인정보의 보유 및 이용기간 및 파기절차 및 파기방법

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

- 보유기간: *처방전 2년(요양급여비용 청구 처방전 3년), 건강보험청구 관련 자료 5년(법령기간),*
- 파기절차: 법정 보유기간 후 파기방법에 의하여 파기
- 파기방법: 전자적 파일형태로 저장된 개인정보는 기록을 재생할 수 없는 기술적 방법을 사용하여 삭제하고 종이에 출력된 처방전은 분쇄기로 분쇄하거나 소각하여 파기

4. 이용자 및 법정대리인의 권리와 그 행사방법

이용자 및 법정대리인은 개인정보와 관련하여 인터넷, 전화, 서면 등을 이용하여 *A*에 연락을 하여 개인정보 열람 등의 권리를 행사할 수 있으며, *A*는 지체 없이 필요한 조치를 합니다.

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

5. 개인정보의 제3자 제공

*A*는 건강보험심사평가원에 요양급여비용 청구를 위해 진료기록을 제출합니다.

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

6. 개인정보 처리의 위탁

개인정보를 정보시스템을 통해 관리하기 위해 다음의 회사에 개인정보를 위탁하고 있습니다.

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

- 폐기: 업체명(연락처) 기입

- CCTV: 업체명(연락처) 기입

7. 개인정보 보호책임자

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

8. 개인정보의 안전성 확보조치

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

9. 정책 변경에 따른 공지의무

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

공고일자: 20XX년 XX월 XX일

시행일자: 20XX년 XX월 XX일

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

[붙임3] 개인정보 처리 위탁 계약서(예시)

※ 계약 체결 시, 관련 법 조항의 변경사항 유무 등 확인 필요

본 표준 개인정보처리위탁 계약서는 「개인정보 보호법」 제26조제1항에 따라 위탁계약에 있어 개인정보 처리에 관하여 문서로 정하여야 하는 최소한의 사항을 표준적으로 제시한 것으로서, 위탁계약이나 위탁업무의 내용 등에 따라 세부적인 내용은 달라질 수 있습니다. 개인정보처리업무를 위탁하거나 위탁업무에 개인정보 처리가 포함된 경우에는 본 표준 개인정보처리위탁 계약서의 내용을 위탁계약서에 첨부하거나 반영하여 사용하실 수 있습니다.

표준 개인정보처리위탁 계약서(안)

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

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

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

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

1. 개인정보의 암호화 *2. 프로그램의 유지보수*

제4조 (재위탁 제한) ① "을"은 "갑"의 사전 승낙을 얻은 경우를 제외하고 "갑"과의 계약상의 권리와 의무의 전부 또는 일부를 제3자에게 양도하거나 재위탁할 수 없다.
② "을"이 다른 제3의 회사와 수탁계약을 할 경우에는 "을"은 해당 사실을 계약 체결 7일 이전에 "갑"에게 통보하고 협의하여야 한다.

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

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

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

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

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

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

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

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

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

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

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

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

20 . . .

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

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

[붙임4] 영상정보처리기기(CCTV) 설치 안내판(예시)

CCTV 설치 안내

◈ 설치 목적: *범죄예방 및 시설안전*

◈ 설치 장소: *건물 출입구 O대, 복도 O대*

◈ 촬영 범위: *50M 전방향*

◈ 촬영 시간: *24시간*

◈ 관리책임자: *OO과 홍길동 (00-OOO-OOOO)*

(설치·운영을 위탁한 경우)

◈ 위탁관리자: *OO업체 박길동 (00-OOO-OOOO)*

[붙임5] 개인정보 내부관리 계획 목차(예시)

개인정보 내부관리 계획 목차(예시)

- 내부관리 계획은 일반적으로 아래와 같은 내용을 포함하여야 한다.

목 차 (예시)

[붙임6] 개인정보 유출 신고서

개인정보 유출신고서

<table>
<tr><td>기관명</td><td colspan="5"></td></tr>
<tr><td>정보주체에의
통지 여부</td><td colspan="5"></td></tr>
<tr><td>유출된 개인정보의
항목 및 규모</td><td colspan="5"></td></tr>
<tr><td>유출된 시점과
그 경위</td><td colspan="5"></td></tr>
<tr><td>유출피해 최소화
대책·조치 및 결과</td><td colspan="5"></td></tr>
<tr><td>정보주체가 할 수 있는
피해 최소화 방법 및
구제절차</td><td colspan="5"></td></tr>
<tr><td rowspan="3">담당부서·담당자 및
연락처</td><td></td><td>성명</td><td>부서</td><td>직위</td><td>연락처</td></tr>
<tr><td>개인정보
보호책임자</td><td></td><td></td><td></td><td></td></tr>
<tr><td>개인정보
취급자</td><td></td><td></td><td></td><td></td></tr>
</table>

<table>
<tr><td rowspan="2">유출신고(보고)
접수기관</td><td>기관명</td><td>담당자명</td><td>연락처</td></tr>
<tr><td></td><td></td><td></td></tr>
</table>

[붙임7] 개인정보파일 파기 과니대장

개인정보파일 파기 관리대장

번호	개인정보 파일명	자료의 종류	생성일	폐기일	폐기사유	처리담당자	처리부서장

[붙임8] 개인영상정보 관리대장

개인영상정보 관리대장

번호	구분	일시	파일명/ 형태	담당자	목적/ 사유	이용· 제공받는 제3자 /열람등 요구자	이용· 제공 근거	이용·제공 형태	기간
1	□ 이용 □ 제공 □ 열람 □ 파기								
2	□ 이용 □ 제공 □ 열람 □ 파기								
3	□ 이용 □ 제공 □ 열람 □ 파기								
4	□ 이용 □ 제공 □ 열람 □ 파기								
5	□ 이용 □ 제공 □ 열람 □ 파기								
6	□ 이용 □ 제공 □ 열람 □ 파기								
7	□ 이용 □ 제공 □ 열람 □ 파기								

2. 벌칙 및 과태료 규정

벌칙 규정

형 량	요 건	근거 법령
10년 이하의 징역또는 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	법 제70조제2호
5년 이하의 징역 또는 5천만원 이하의 벌금	제17조제1항제2호에 해당하지 아니함에도 같은 항 제1호를 위반하여 정보주체의 동의를 받지 아니하고 개인정보를 제3자에게 제공한 자 및 그 사정을 알고 개인정보를 제공받은 자	법 제71조제1호
	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
3년 이하의 징역 또는 3천만원 이하의 벌금	제25조제5항을 위반하여 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비추는 자 또는 녹음기능을 사용한 자	법 제72조제1호
	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
2년 이하의 징역 또는 2천만원 이하의 벌금	제23조제2항, 제24조제3항, 제25조제6항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 아니하여 개인정보를 분실·도난·유출·위조·변조 또는 훼손당한 자	법 제73조제1호
	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	요 건	근거 법령
5천만원 이하	제15조제1항을 위반하여 개인정보를 수집한 자	법 제75조제1항제1호
	제22조제5항을 위반하여 법정대리인의 동의를 받지 아니한 자	법 제75조제1항제2호
	제25조제2항을 위반하여 영상정보처리기기를 설치·운영한 자	법 제75조제1항제3호
3천만원 이하	제15조제2항, 제17조제2항, 제18조제3항 또는 제26조제3항을 위반하여 정보주체에게 알려야 할 사항을 알리지 아니한 자	법 제75조제2항제1호
	제16조제3항 또는 제22조제4항을 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 영상정보처리기기를 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 파기 등 필요한 조치를 하지 아니한 자	법 제75조제2항제12호
	제64조제1항에 따른 시정명령에 따르지 아니한 자	법 제75조제2항제13호

1천만원 이하	제21조제3항을 위반하여 개인정보를 분리하여 저장·관리하지 아니한 자	법 제75조제3항제1호
	제22조제1항부터 제3항까지의 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

3. 안전조치 기준 적용 유형

조	항	호	유형1 (완화)	유형2 (표준)	유형3 (강화)
제1조(목적)					
제2조(정의)					
제3조(안전조치 기준 적용)					
제4조 (내부관리 계획의 수립·시행)	① 개인정보처리자는 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 다음 각 호의 사항을 포함하는 내부 관리계획을 수립·시행하여야 한다.	1. 개인정보 보호책임자의 지정에 관한 사항		○	○
		2. 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항		○	○
		3. 개인정보취급자에 대한 교육에 관한 사항		○	○
		4. 접근 권한의 관리에 관한 사항		○	○
		5. 접근 통제에 관한 사항		○	○
		6. 개인정보의 암호화 조치에 관한 사항		○	○
		7. 접속기록 보관 및 점검에 관한 사항		○	○
		8. 악성프로그램 등 방지에 관한 사항		○	○
		9. 물리적 안전조치에 관한 사항		○	○
		10. 개인정보 보호조직에 관한 구성 및 운영에 관한 사항		○	○
		11. 개인정보 유출사고 대응 계획 수립·시행에 관한 사항		○	○
		12. 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		○	○
	② [별표]의 유형1에 해당하는 개인정보처리자는 제1항에 따른 내부 관리계획을 수립하지 아니할 수 있고, [별표]의 유형2에 해당하는 개인정보처리자는 제1항제12호부터 제14호까지를 내부 관리계획에 포함하지 아니할 수 있다.				
	③ 개인정보처리자는 제1항 각 호의 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부 관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 한다.			○	○
	④ 개인정보 보호책임자는 연 1회 이상으로 내부 관리계획의 이행 실태를 점검·관리 하여야 한다.			○	○

조	항	호	유형1 (완화)	유형2 (표준)	유형3 (강화)
제5조 (접근권한의 관리)	① 개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.			○	○
	② 개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하여야 한다.		○	○	○
	③개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.		○	○	○
	④ 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자 별로 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.		○	○	○
	⑤ 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다.		○	○	○
	⑥ 개인정보처리자는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다.			○	○
	⑦ [별표]의 유형1에 해당하는 개인정보처리자는 제1항 및 제6항을 아니할 수 있다.				
제6조 (접근통제)	① 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 조치를 하여야 한다.	1. 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol)주소 등으로 제한하여 인가받지 않은 접근을 제한	○	○	○
		2. 개인정보처리시스템에 접속한 IP (Internet Protocol) 주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응	○	○	○
	② 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN: Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다.			○	○
	③ 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 하여야 한다.		○	○	○
	④ 고유식별정보를 처리하는 개인정보처리자는 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하고 필요한 보완 조치를 하여야 한다.			○	○
	⑤ 개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하여야 한다.			○	○
	⑥ 개인정보처리자가 별도의 개인정보처리시스템을 이용하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 제1항을 적용하지 아니할 수 있으며, 이 경우 업무용 컴퓨터 또는 모바일 기기의 운영체제(OS: Operating System)나 보안프로그램 등에서 제공하는 접근 통제 기능을 이용할 수 있다.		○	○	○
	⑦ 개인정보처리자는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.		○	○	○
	⑧ [별표]의 유형1에 해당하는 개인정보처리자는 제2항, 제4항부터 제5항까지의 조치를 아니할 수 있다.				

조	항	호	유형1 (완화)	유형2 (표준)	유형3 (강화)
제7조 (개인정보의 암호화)	① 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.		○	○	○
	② 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.		○	○	○
	③ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ: Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.		○	○	○
	④ 개인정보처리자가 내부망에 고유식별정보를 저장하는 경우에는 다음 각 호의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.	1. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과	○	○	○
		2. 암호화 미적용시 위험도 분석에 따른 결과	○	○	○
	부칙 제2조(적용례) 영 제21조의2제2항에 따른 주민등록번호의 암호화 적용시기 이후에는 고유식별정보 중 주민등록번호는 제7조제4항을 적용하지 아니한다.				
	⑤ 개인정보처리자는 제1항, 제2항, 제3항, 또는 제4항에 따라 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.		○	○	○
	⑥ 개인정보처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.				○
	⑦ 개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.		○	○	○
	⑧ [별표]의 유형1 및 유형2에 해당하는 개인정보처리자는 제6항을 아니할 수 있다.				
제8조 (접속기록의 보관 및 점검)	① 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 6개월 이상 보관·관리하여야 한다.		○	○	○
	② 개인정보처리자는 개인정보의 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 반기별로 1회 이상 점검하여야 한다.		○	○	○
	③ 개인정보처리자는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.		○	○	○
제9조 (악성프로그램 등 방지)	개인정보처리자는 악성프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.	1. 보안 프로그램의 자동 업데이트 기능을 사용하거나, 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지	○	○	○
		2. 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트를 실시	○	○	○
		3. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치	○	○	○
제10조 (관리용 단말기의 안전조치)	개인정보처리자는 개인정보 유출 등 개인정보 침해사고 방지를 위하여 관리용 단말기에 대해 다음 각 호의 안전조치를 하여야 한다.	1. 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치	○	○	○
		2. 본래 목적 외로 사용되지 않도록 조치	○	○	○
		3. 악성프로그램 감염 방지 등을 위한 보안조치 적용	○	○	○

조	항	호	유형1 (완화)	유형2 (표준)	유형3 (강화)
제11조 (물리적 안전조치)	① 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다.		○	○	○
	② 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.		○	○	○
	③ 개인정보처리자는 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하여야 한다. 다만, 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있다.		○	○	○
제12조 (재해·재난 대비 안전조치)	① 개인정보처리자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검하여야 한다.				○
	② 개인정보처리자는 재해·재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하여야 한다.				○
	③ [별표]의 유형1 및 유형2에 해당하는 개인정보처리자는 제1항부터 제2항까지 조치를 이행하지 아니할 수 있다.				
제13조 (개인 정보의 파기)	① 개인정보처리자는 개인정보를 파기할 경우 다음 각 호 중 어느 하나의 조치를 하여야 한다.	1. 완전파괴(소각·파쇄 등)	○	○	○
		2. 전용 소자장비를 이용하여 삭제	○	○	○
		3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행	○	○	○
	② 개인정보처리자가 개인정보의 일부만을 파기하는 경우, 제1항의 방법으로 파기하는 것이 어려울 때에는 다음 각 호의 조치를 하여야 한다.	1. 전자적 파일 형태인 경우: 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독	○	○	○
		2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우: 해당 부분을 마스킹, 천공 등으로 삭제	○	○	○