요양기관
개인정보 자율보호 표준가이드

HIRA 건강보험심사평가원
HEALTH INSURANCE REVIEW & ASSESSMENT SERVICE

목 차

III. 개인정보의 안전한 관리

서식 모음

관련 규정

표준가이드 변경 이력

연번	일자	주요내용	비고
1	2015.	▪ 최초 작성	
2	2020.02.	▪ (3.2.10) 업무용 모바일 기기 비밀번호 설정 ⇒ (3.2.3) 안전한 비밀번호 작성규칙 적용으로 통합 ▪ (3.8.2) 전담조직, 적정인력 운영 (3.8.4) 필요예산 반영 ⇒ (3.8.1) 개인정보 보호책임자 역할 정의로 통합 * (3.8.3) 개인정보 보호책임자 관리·감독 → (3.8.2) 변경 ▪ (3.2.7) 홈페이지 노출진단 서비스 내용 삭제 ▪ (3.4.1) 접속기록 2년 이상 보관, 기록항목 추가 등 * 「개인정보의 안전성 확보조치 기준」('19.6.7.) 개정사항 반영 ▪ 용어·서식 표준화, 기타 내용 현행화(파란색 표시)	(삭제) 3.2.10 3.8.2 3.8.4
3.	2020.11.	▪ 「개인정보 보호법」 통합 및 개인정보보호위원회(이하 '보호위원회') 출범(8.5.) 등 변경사항 반영 ▪ 항목번호 1.1.3 → 1.1.2로 변경 ▪ 항목 증빙자료 명확화 및 인쇄물 제작에 따른 뒷표지 추가	(삭제) 1.1.3
4	2022.11.	▪ 항목번호 1.5. → 1.4 로 변경(개인정보의 파기) ▪ 개인정보보호위원회 표준 개인정보 보호지침 반영 (별지 양식, 라벨링 등) ▪ 사전질문 변경(청구SW 점검 연계, 3.3.3 추가) ▪ 점검기준, 증빙자료, 근거규정 보완 및 지표설명 일반화	
5	2023.4.	▪ (3.3.6) 암호 키 항목 추가 ▪ (3.6.2) 용어 변경	

지표별 가이드

사전 질문 및 응답 요령

Ⅰ. 개인정보의 처리

사전질문(점검항목 선택정보) 답변에 따른 점검항목 점검/제외

사전질문	점검항목	답변	
		예	아니오
조제, 복약지도 목적 외로 개인정보수집 및 이용(홍보용 SMS 발송 등)을 하고 있습니까?	1.1.1 1.1.2 1.2.1 1.2.2 1.2.3 2.1.1 2.2.1	점검	점검항목 제외
영상정보처리기기(CCTV)를 설치, 운영하고 있습니까?	2.3.1 2.3.2 2.3.3 2.3.4	점검	점검항목 제외
개인정보를 수집하는(회원가입 등) 홈페이지를 보유하고 있습니까?	3.2.7 3.3.5	점검	점검항목 제외
청구프로그램 외 개인정보를 처리하는 프로그램을 사용하고 있습니까?(예:고객관리프로그램 등)	3.2.8 3.2.9 3.3.1 3.3.3 3.3.4	점검	점검항목 제외

점검결과 선택 방법

점검결과	선택방법
양호	점검항목이 약국에 해당되며, 요구하는 기준에 부합한 조치가 마련되고 증빙을 할 수 있는 경우 선택
미흡	점검항목이 약국에 해당되나 관리실태가 부실하거나, 대책마련이 안된 경우 선택
해당없음	점검항목이 약국에 해당사항이 없는 경우 선택

1.1.1	진료(조제, 복약지도 포함) 목적 외로 서면(오프라인) 및 홈페이지(온라인) 등을 통한 개인정보수집 시 동의를 받고 있는가?
점검기준	☑ 필수항목(5개)을 환자(정보주체)에게 고지하고 동의를 받았는지 여부 확인 ☑ 동의 시 명시한 항목과 실제 수집하는 항목간의 일치 여부 확인
증빙자료	☑ 개인정보수집동의서, 회원가입신청서 등 개인정보수집 양식 ☑ 개인정보 목적 외 이용 및 제3자 제공 내역(요청서 등 관련 증적 포함)
관련근거	「개인정보 보호법」 제15조(개인정보의 수집· 이용) 제18조(개인정보의 목적 외 이용·제공 제한)
세부설명	□ 개인정보 목적 외 이용·제공이 가능한 경우(공공기관 외) 1. 정보주체(이용자)로부터 별도의 동의를 받는 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 □ 개인정보를 목적 외 용도로 이용·제공하기 위하여 동의를 받을 경우 고지사항 1. 개인정보를 제공받는 자 2. 개인정보의 이용 목적(제공 시에는 제공받는 자의 이용목적) 3. 이용 또는 제공하는 개인정보의 항목 4. 개인정보의 보유 및 이용 기간 (제공 시에는 제공받는 자의 보유 및 이용기간) 5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에 그 불이익의 내용

1.1.2	진료(조제, 복약지도 포함) 목적 외로 만 14세 미만 아동의 개인정보를 수집·처리 시, 법정대리인의 동의를 받았는가?
점검기준	☑ 진료(조제, 복약지도 포함) 목적 외 14세 미만 아동의 개인정보를 수집·처리 시, 법정대리인의 동의 여부 확인
증빙자료	☑ 개인정보수집동의서, 회원가입신청서 등 개인정보수집 양식
관련근거	「개인정보 보호법」 제22조(동의를 받는 방법)
세부설명	□ 진료(조제, 복약지도 포함) 목적 외로 수집한 개인정보 중 만 14세 미만 아동의 개인정보가 있을 경우, 해당 개인정보 수집 시 법정대리인으로부터 동의를 받아야하며, 증빙자료를 통해 확인 □ 법정대리인의 동의를 받기 위해 법정대리인의 성명·연락처를 수집할 때에는 해당 아동에게 자신의 신분과 연락처, 법정대리인의 성명과 연락처를 수집하고자 하는 이유를 알려야 함 □ 개인정보처리자는 법 제22조제5항에 따라 수집한 법정대리인의 개인정보를 법정대리인의 동의를 얻기 위한 목적으로만 이용하여야 하며, 법정대리인의 동의 거부가 있거나 법정대리인의 동의 의사가 확인되지 않는 경우 수집일로부터 5일 이내에 파기해야 함

1.2.1	목적에 필요한 최소한의 개인정보만 수집하고 있는가?
점검기준	☑ 목적달성을 위한 최소한의 개인정보(필수정보) 수집여부 확인 ☑ 환자(정보주체)에게 최소한의 정보 외의 개인정보(선택정보) 수집에는 동의하지 않을 수 있다는 사실을 고지하는지 여부 확인
증빙자료	☑ 개인정보수집동의서, 회원가입신청서 등 개인정보수집 양식
관련근거	「개인정보 보호법」 제16조(개인정보의 수집 제한)
세부설명	□ 수집 목적에 필요한 범위 내에서 최소한의 개인정보(필수정보)만 수집 • 서면(오프라인) 또는 홈페이지(온라인)등에서 개인정보를 수집하는 경우, 목적 달성을 위해 반드시 수집하여야 하는 최소한의 개인정보만을 수집 – 필수정보는 아니나, 추가적인 서비스 제공 등을 위해 필요한 정보(선택정보)를 수집하는 경우에도 목적 달성을 위한 최소한의 정보를 수집 • 필요한 최소한의 정보(필수정보) 외의 개인정보(선택정보) 수집에는 동의하지 아니할 수 있다는 사실을 명확하게 알려야 함 예시) 홈페이지 회원가입을 통한 정보를 수집하고자 하는 경우 – 동의 필요(필수정보): 성명, 전화번호 – 동의거부 가능(선택정보): 성별, 나이 【참고】 최소한의 개인정보 수집 여부에 대한 입증 책임은 요양기관(개인정보처리자)에 있음

1.2.2	최소한의 개인정보 수집 외에 선택정보에 대한 미 동의를 이유로 재화 또는 부가서비스 제공을 거부하고 있지 않는가?
점검기준	☑ 필수정보가 아닌 선택정보 미동의 시에도 회원가입 등 기본적인 서비스를 제공하는지 여부 확인
증빙자료	☑ 개인정보수집동의서, 회원가입신청서 등 개인정보수집 양식
관련근거	「개인정보 보호법」 제16조(개인정보의 수집 제한)
세부설명	□ 환자(정보주체)의 동의를 받아 개인정보를 수집하는 경우, 진료(조제, 복약지도 포함) 목적에 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 않을 수 있음을 구체적으로 알리고 수집하여야 함 • 최소한의 개인정보(필수정보) 외의 개인정보(선택정보) 수집에 동의하지 않아도 기본적인 서비스 제공(회원가입 등)이 가능하여야 함 • 환자(정보주체)에게 동의를 받을 시 선택정보에 대한 동의를 거부할 경우 재화 또는 부가서비스의 이용이 제한됨을 알리는 것은 가능

1.2.3	개인정보 수집 시, 포괄 동의를 받고 있지 않은가?
점검기준	☑ 각각의 개인정보 처리 동의 사항을 구분하여 각각 동의를 받는지 여부
증빙자료	☑ 개인정보수집동의서, 회원가입신청서 등 개인정보수집 양식
관련근거	「개인정보 보호법」 제22조(동의를 받는 방법)
세부설명	□ 개인정보의 처리에 대하여 환자(정보주체)의 동의를 받을 때에는 환자가 동의사항을 명확하게 인지할 수 있도록 구분하고 각각 동의를 받아야 함 【참고】 <구분 동의가 필요한 경우> ① 개인정보 수집·이용 동의 ② 마케팅 목적 처리 동의 ③ 제3자 제공 동의 ④ 목적 외 이용·제공 동의 ⑤ 법정대리인 동의 ⑥ 민감정보 처리 동의 ⑦ 고유식별정보 처리 동의 ⑧ 국외 제3자 제공 동의 ※ 위의 ②, ④와 같은 경우에는 목적별로 각각 동의를 받아야 함

1.3.1	제3자에게 개인정보 제공 및 목적 외 이용 시 환자(정보주체)의 별도 동의를 받고 있는가?
점검기준	☑ 법령(「의료법」, 「약사법」 등)에 근거한 제3자 제공의 경우 해당 법령 준수여부 확인 ☑ 법령에 근거하지 않은 제3자 제공의 경우, 필수 고지항목(①~⑤)을 환자(정보주체)에게 고지하고 동의를 받았는지 여부 확인
증빙자료	☑ 법령에 근거하지 않은 제3자 제공 사례가 있는 경우 • 제3자 개인정보 제공 동의서(필수고지내용 ①~⑤ 포함된 동의서)
관련근거	「개인정보 보호법」 제17조(개인정보의 제공) 제18조(개인정보의 목적 외 이용·제공 제한)
세부설명	□ 법령에서 정한 제3자 제공이 가능한 경우에는 법령 준수와 별도로 환자(정보주체)에게 고지 후 동의 받을 필요 없음 예시1) 「의료법」 제21조(기록 열람 등)에 의해 건강보험 급여비용 청구를 위한 개인정보 제공은 환자의 동의 없이 가능함 예시2) 「의료법」 제21조(기록 열람 등)에 의해 환자의 대리인이 환자의 동의서 및 위임장, 환자의 신분증 사본 및 대리인의 신분증 사본을 제출하는 경우에는 개인정보를 제공 가능함 □ 법령의 근거 없이 개인정보 수집 목적을 넘어 이용하거나 제3자에게 제공하는 경우, 다른 개인정보의 처리에 대한 동의와 분리하여 다음 사항을 고지하고 목적 외 이용·제공에 대한 별도의 동의를 받아야 함 ① 개인정보를 제공받는 자 ② 개인정보를 제공받는 자의 개인정보 이용 목적 ③ 제공하는 개인정보의 항목 ④ 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간 ⑤ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우 그 불이익의 내용

<table>
<tr><td>1.4.1</td><td>수집한 진료정보 및 개인정보의 보유기간 경과, 처리 목적(제공받는 경우 제공받는 목적) 달성 후 지체 없이 개인정보를 파기하고 있는가?</td></tr>
<tr><td>점검기준</td><td>☑ 법령에 규정된 보존기간이 지난 진료정보 및 기타 목적으로 수집한 개인정보를 목적 달성 이후 파기하였는지 여부 확인</td></tr>
<tr><td>증빙자료</td><td>☑ 개인정보 파기 관리대장</td></tr>
<tr><td>관련근거</td><td>「개인정보 보호법」 제21조(개인정보의 파기)</td></tr>
<tr><td>세부설명</td><td>□ 「의료법」, 「약사법」 등 법령에 규정된 보존기한 준수 파기
다만, 계속적인 진료를 위하여 필요한 경우에는 1회에 한정하여 동일 기간만큼 연장 가능함(「의료법 시행규칙」 제15조)

□ 진료(조제, 복약지도 포함) 목적 외로 수집한 개인정보는 보유기간의 경과 및 처리목적 달성 시 지체 없이(5일 이내) 파기하여야 함

□ 개인정보 파기 시 ‘개인정보 파기 관리대장’과 파기한 증빙자료를 함께 보관·관리하는 것을 권장함(「표준 개인정보 보호지침」 제10조)

□ 다만, 5명 미만의 상시근로자가 있는 의료기관이 개인정보의 파기를 독립적으로 수행하기 어려운 때에는 협회의 중앙회 또는 지부에서 공동으로 파기할 수 있음

<table>
<tr><th>근거</th><th>의료법(시행규칙 제15조)</th><th>약사법(제29조, 30조)</th></tr>
<tr><td>기록물
(보존기간)</td><td>환자명부(5년), 진료기록부(10년), 처방전(2년, 건강보험 청구건 5년), 수술기록(10년), 검사소견기록(5년), 방사선 사진 및 그 소견서(5년), 간호기록부(5년), 조산기록부(5년), 진단서 등의 부본(3년)</td><td>처방전(2년, 건강보험 청구건 3년)
조제기록부(5년)</td></tr>
</table>
</td></tr>
</table>

1.4.2	개인정보 파기 시 복구 또는 재생되지 않도록 조치하고 있는가?
점검기준	☑ 개인정보의 파기 시 복원 불가능한 방법으로 파기 여부 확인
증빙자료	☑ 개인정보 파기 관리대장
관련근거	「개인정보 보호법」 제21조(개인정보의 파기)
세부설명	□ 개인정보(파일)의 당초 수집목적이 달성되었거나, 보유기간이 경과되어 파기 시 복원이 불가능한 방법으로 영구 삭제하여야 함 □ 개인정보 파기 또는 연장 후 개인정보 파기관리대장에 파기사실 확인서와 함께 보관·관리하는 것을 권장함 (「표준 개인정보 보호지침」 제10조) □ '복원이 불가능한 방법' 이란 현재의 기술수준에서 사회통념상 적정한 비용으로 파기한 개인정보의 복원이 불가능하도록 조치하는 방법을 말함 • 전자 파일: 청구S/W 파기기능을 이용, 영구삭제S/W, 포맷 등 • 비전자 파일: 소각, 파쇄, 천공, 마스킹 등

1.4.3	임시파일 및 출력자료 등은 목적달성 후 즉시 파기 하고 있는가?
점검기준	☑ 임시로 출력하거나 PC에 보관하고 있는 개인정보 포함 자료는 사용 후 즉시 파기하는지 여부 확인
증빙자료	☑ 임시파일 및 출력자료를 즉시 파기 가능하도록 소형 파쇄기 등 설치 여부
관련근거	「개인정보 보호법」 제21조(개인정보의 파기)
세부설명	□ 업무 수행 상 보존 필요성은 없으나, 임시적으로 생성한 파일이나 출력자료는 사용 후 즉시 파기하여야 함 • 출력자료를 불필요하게 생산하지 말아야 하며 환자의 정보가 담긴 문서(접수증, 진료기록부 사본, 처방전 등)가 대기실, 접수대에 방치되지 않도록 관리해야 함 • 업무용 PC에 보관중인 개인정보가 포함된 임시파일(한글문서, 워드, 엑셀, 환자사진 등) 또한 목적 달성 후 즉시 파기해야 함 – 임시 저장이 필요한 경우 반드시 암호화(비밀번호 설정)하여 저장 – 주기적으로 임시파일 존재여부 점검 및 삭제

1.4.4	법령(전자상거래법, 형사소송법, 민사소송법 등)에 따라 개인정보를 파기하지 않고 보존하는 경우 별도로 분리 보관하고 있는가?
점검기준	☑ 파기대상임에도 불구하고 법령에 따라 보존하는 개인정보를 적절한 방법으로 분리 보관하는지 여부 확인
증빙자료	☑ 타 법령의 근거에 따라 별도 분리 보관하는 개인정보가 있는 경우, 개인정보처리시스템 내 분리 저장된 화면캡처 또는 물리적 보관사진 등
관련근거	「개인정보 보호법」 제21조(개인정보의 파기)
세부설명	□ 수집목적이 달성된 개인정보나 보존기한이 지난 진료기록의 경우에도 전자상거래법, 형사소송법, 민사소송법 등의 법령에 근거하여 개인정보 전부 또는 일부를 파기하지 않고 보존한다면, 그 개인정보를 별도로 분리하여 보관하여야 함 • 서면: 물리적 장소 분리 • 전자파일: 별도의 DB, Table, 파일 등으로 분리 □ 접근권한은 해당업무 담당자 등의 필수직원으로 엄격히 제한 • 법령에 따라 분리 보관한다는 의미는 소송, 민원 등 특정한 상황이 아니면 접근할 필요가 없다는 의미 □ 법원·경찰 등에서 법률에 의해서 보존요청이 올 경우 요청기간에 따라 보존하여야함

지표별 가이드

Ⅱ. 개인정보의 처리 제한

2.1. 민감정보의 처리제한

2.2. 고유식별정보의 처리제한

2.3. 영상정보처리기기 설치운영 제한

2.4. 업무위탁에 따른 개인정보의 처리제한

2.5. 개인정보 취급자 감독

2.1.1	진료(조제, 복약지도 포함)목적 외로 민감정보를 수집할 경우, 별도 동의를 받고 있는가?
점검기준	☑ 목적 외 개인정보 수집 시 별도 동의를 받는지 여부 확인
증빙자료	☑ 개인정보수집동의서, 민감정보 수집 동의서 등 민감정보 수집 양식
관련근거	「개인정보 보호법」 제23조(민감정보의 처리 제한)
세부설명	□ 진료(조제, 복약지도 포함) 목적의 민감정보 처리는 법령에 의해 환자(정보주체)의 별도 동의 없이 처리 가능함 □ 진료(조제, 복약지도 포함)목적 외 또는 법령에 근거하지 않고 민감정보를 처리하고자 하는 경우 환자(정보주체)에게 아래 사항을 고지하고 별도의 동의를 받아야 함 • 민감정보 수집·이용 시 고지사항 – 민감정보의 수집·이용 목적 – 수집하려는 민감정보의 항목 – 민감정보의 보유 및 이용기간 – 동의거부권 및 동의 거부에 따른 불이익 안내

2.2.1	관련법령에 의거하여 고유식별정보를 수집 및 처리하고 있는가?
점검기준	☑ 관련법령에 의거하여 고유식별정보를 수집하는지 여부 확인
증빙자료	☑ 「의료법」, 「약사법」 등 법령에 근거한 고유식별정보 수집 및 처리만 하는 경우 별도의 증빙자료 없이 점검결과 '양호' 선택
관련근거	「개인정보 보호법」 제24조(고유식별정보의 처리 제한) 제24조의2(주민등록번호 처리의 제한)
세부설명	□ 고유식별정보: 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호 □ 진료(조제, 복약지도 포함)목적의 고유식별정보 처리는 법령에 의해 환자(정보주체)의 별도 동의 없이 처리 가능함 □ 진료(조제, 복약지도 포함)목적 외 또는 법령에 근거하지 않고 고유식별정보를 처리할 경우 환자(정보주체)에게 별도의 동의를 받아야 함 ※ 단, 주민등록번호는 법률에서 구체적으로 처리를 요구하거나 허용한 경우*에 한하여 처리가능 * 법률, 대통령령, 국회규칙, 대법원규칙, 헌법재판소규칙, 중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우 • 고유식별정보(주민등록번호 제외) 수집·이용 시 고지사항 – 고유식별정보의 수집·이용 목적 – 수집하려는 고유식별정보의 항목 – 고유식별정보의 보유 및 이용기간 – 동의거부권 및 동의 거부에 따른 불이익 안내

2.3.1	영상정보처리기기(CCTV) 운영·관리방침을 수립하고 있는가?
점검기준	☑ 영상정보처리기기(CCTV) 운영·관리방침 수립 여부 확인 ☑ 영상정보처리기기(CCTV) 운영·관리방침 공개 여부 확인
증빙자료	☑ 영상정보처리기기(CCTV) 운영 · 관리 방침(필수 기재사항 ①~⑧ 포함 수립)
관련근거	「개인정보 보호법」 제25조(영상정보처리기기의 설치운영 제한), 「개인정보 보호법 시행령」 제25조(영상정보처리기기의 운영·관리 방침) 「표준 개인정보 보호지침」 제36조(영상정보처리기기 운영·관리 지침)
세부설명	□ 영상정보처리기기(CCTV) 운영자는 아래 내용이 포함된 영상정보처리기기(CCTV) 운영·관리방침을 마련하고, 이를 공개하여야 함 <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, 보관장소 및 처리방법 ⑤ 영상정보처리기기운영자의 영상정보 확인 방법 및 장소 ⑥ 정보주체의 영상정보 열람 등 요구에 대한 조치 ⑦ 영상정보 보호를 위한 기술적·관리적 및 물리적 조치 ⑧ 그 밖에 영상정보처리기기의 설치·운영 및 관리에 필요한 사항 <영상정보처리기기(CCTV) 운영·관리 방침 공개 방법> • 영상정보처리기기 운영·관리 방침은 개인정보 처리방침과 동일하게 인터넷 홈페이지 또는 보기 쉬운 장소(접수대 등)에 게시하여야 함 ※ 개인정보 처리방침에 포함하여 수립·공개 가능 【참고】 영상정보처리기기 운영·관리 방침은 영상정보처리기기(CCTV)의 운영책임기관에서 수립하여 관리 함(위탁 운영하는 경우에는 위탁자가 운영·관리 방침을 수립·관리)

2.3.2	영상정보처리기기(CCTV)를 설치한 장소에 정보주체가 영상정보 처리기기(CCTV) 설치 사실을 인지할 수 있도록 필수기재 사항을 포함한 안내판을 설치하고 있는가?
점검기준	☑ 안내판 설치(필수 기재사항 ①~④ 포함) 여부 확인
증빙자료	☑ 안내판 설치 장소 및 내용
관련근거	「개인정보 보호법」 제25조(영상정보처리기기의 설치운영 제한) 「표준 개인정보 보호지침」 제39조(안내판의 설치)
세부설명	□ 요양기관 내 공개된 장소에 영상정보처리기기(CCTV)를 설치·운영하는 경우 환자(정보주체)가 쉽게 인식할 수 있도록 안내판을 설치하여야 함 • 안내판에 필수기재 하여야 할 사항 ① 설치 목적 및 장소 ② 촬영 범위 및 시간 ③ 관리책임자의 성명(또는 직책) 및 연락처 ④ (설치·운영을 위탁한 경우) 수탁자의 명칭 및 연락처 □ 요양기관의 진료실, 처치실, 수술실, 입원실 등의 공간에 영상정보처리기기(CCTV)를 설치하여 개인영상 등을 수집하고자 하는 경우에는 정보주체의 수집·이용 동의를 받아야 함 (단, 정신보건법에 의한 수용시설을 갖춘 정신의료기관, 정신질환자사회복귀시설, 정신요양시설은 제외) [인터넷 홈페이지를 운영하고 있지 않아 게재가 불가능한 경우 게시방법] 1. 영상정보처리기기운영자의 사업장·영업소·사무소·점포 등 보기 쉬운 장소에 게시하는 방법 2. 영상정보처리기기운영자의 사업장 등이 있는 특별시·광역시·도 또는 특별자치도(이하 “시·도”라 한다)이상의 지역을 주된 보급지역으로 하는 「신문 등의 진흥에 관한 법률」 제2조제1호가목·다목 및 같은 조 제2호에 따른 일반일간신문, 일반주간신문 또는 인터넷신문에 싣는 방법

2.3.3	영상정보처리기기(CCTV)에 대한 이용 · 제공 · 열람 · 파기 내역을 기록하고 관리 하는가?
점검기준	☑ 개인영상정보 관리대장 작성·관리 여부 확인
증빙자료	☑ 개인영상정보 관리대장
관련근거	「표준 개인정보 보호지침」 제42조(이용·제3자 제공·파기의 기록 및 관리) 「표준 개인정보 보호지침」 제44조(정보주체의 열람등 요구) 「표준 개인정보 보호지침」 제45조(개인영상정보 관리대장)
세부설명	□ 영상정보처리기기(CCTV) 운영자는 개인영상정보를 ① 수집 목적 이외로 이용하거나 제3자에게 제공하는 경우, ② 파기하는 경우, ③ 열람 요청이 있는 경우에는 아래 사항을 기록하고 관리하여야 함 <이용 또는 제공하는 경우> ① 개인영상정보 파일의 명칭 ② 이용 하거나 제공받은 자(공공기관 또는 개인)의 명칭 ③ 이용 또는 제공의 목적 ④ 법령상 이용 또는 제공 근거가 있는 경우 그 근거 ⑤ 이용 또는 제공의 기간이 정하여져 있는 경우에는 그 기간 ⑥ 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 보관기간은 개인영상정보 수집 후 30일 이내로 파기하는 것을 권장함 (제41조(보관 및 파기) <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

2.3.4	영상정보처리기기(CCTV)가 분실·도난·유출·변조 또는 훼손되지 아니하도록 안전성 확보조치를 하고 있는가?
점검기준	☑ 영상정보처리기기(CCTV)보관 시설 마련 또는 잠금장치 설치 여부 확인 ☑ 영상정보처리기기(CCTV)에 대한 접근통제 여부 확인
증빙자료	☑ 영상정보처리기기(CCTV) 녹화장비(DVR) 등 물리적 시건장치 사진 또는 접속계정(ID) 등록화면 캡처
관련근거	「개인정보 보호법」 제25조(영상정보처리기기의 설치운영 제한) 제29조(안전조치의무) 「표준 개인정보 보호지침」 제47조(개인영상정보의 안전성 확보를 위한 조치) 개인정보보호위원회 영상정보처리기기 설치운영 가이드라인
세부설명	□ 개인영상정보가 분실·도난·유출·변조 또는 훼손되지 않도록 개인영상정보의 안전성 확보에 필요한 조치를 하여야 함 • 개인영상정보의 안전한 물리적 보관을 위한 별도 보관시설 마련 또는 잠금장치 설치 • 영상정보처리기기(CCTV)에 대한 접근 통제 및 접근 권한 제한

<table>
<tr><td>2.4.1</td><td>위탁 계약 시 문서(계약서)에 의한 계약을 하였는가?</td></tr>
<tr><td>점검기준</td><td>☑ 위탁사업자별 계약서에 필수사항(7개)이 포함되었는지 여부 확인</td></tr>
<tr><td>증빙자료</td><td>☑ 위탁사업자별 계약서(필수사항이 포함된 위·수탁 계약서, 협약서, 특약서 등)
• 개인정보 처리방침(개인정보 처리업무 위탁 관련 공개 내역)
• 개인정보 수집 양식
• 개인정보 처리위탁 계약서
• 재화 또는 서비스 홍보·판매 권유 업무 위탁 관련 정보주체 통지 내역</td></tr>
<tr><td>관련근거</td><td>「개인정보 보호법」 제26조(업무위탁에 따른 개인정보의 처리제한)</td></tr>
<tr><td>세부설명</td><td>□ 개인정보 위탁업무 예시
• 진료신청서 처리사무, 진료비 수납사무, 연말정산 사무, 각종 증명서 발급 사무 등 개인정보 처리업무 위탁
• 전자차트 및 청구S/W 등의 유지보수, 혈액검사, CCTV 운영, 홈페이지 운영, 처방전 보관/폐기 등

□ 개인정보 처리 위탁문서(계약서)에 포함되어야 할 내용
① 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
② 개인정보의 기술적·관리적 보호조치에 관한 사항
③ 위탁하는 업무의 목적 및 범위
④ 재위탁 제한에 관한 사항
⑤ 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
⑥ 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항
⑦ 수탁자가 준수해야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

【참고】 업무위탁과 제3자 제공 비교
<table><tr><th>구분</th><th>업무위탁</th><th>제3자 제공</th></tr><tr><td>관련조항</td><td>「개인정보 보호법」 제26조</td><td>「개인정보 보호법」 제17조</td></tr><tr><td>예시</td><td>배송업무 위탁, TM 위탁 등</td><td>사업제휴, 개인정보 판매 등</td></tr><tr><td>이전목적</td><td>위탁자의 이익을 위해 처리</td><td>제3자의 이익을 위해 처리</td></tr><tr><td>예측가능성</td><td>정보주체가 사전 예측 가능
(정보주체의 신뢰 범위 내)</td><td>정보주체가 사전예측 곤란
(정보주체의 신뢰 범위 밖)</td></tr><tr><td>이전방법</td><td>원칙: 위탁사실 공개
예외: 위탁사실 고지
(마케팅 업무 위탁)</td><td>제공목적 등 고지 후 정보주체 동의 획득</td></tr><tr><td>관리·감독책임</td><td>위탁자 책임</td><td>제공받는 자 책임</td></tr><tr><td>손해배상책임</td><td>위탁자 부담(사용자 책임)</td><td>제공받는 자 부담</td></tr></table></td></tr>
</table>

2.4.2	수탁업체에 대한 교육 및 처리현황 점검 등 관리 감독을 실시하고 있는가?
점검기준	☑ 수탁업체에 대한 개인정보보호 교육 실시 여부 ☑ 수탁업체가 위탁한 개인정보처리 업무를 적절하게 처리하고 있는지 점검·확인 여부
증빙자료	☑ 수탁업체 대상 관리·감독 및 개인정보보호 교육 결과 등
관련근거	「개인정보 보호법」 제26조(업무위탁에 따른 개인정보의 처리제한)
세부설명	□ 수탁업체 교육 • 환자(정보주체)의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 수탁자를 교육 ※ 수탁업체를 대상으로 교육이 현실적으로 어려운 경우 수탁업체의 자체 개인정보보호 교육 실시 증빙서류를 받아 보관하는 것으로 대신할 수 있음 □ 수탁업체 관리·감독 • 수탁자(위탁받는 업체)의 개인정보 처리현황 및 실태, 목적 외 이용·제공 여부, 재위탁 여부, 안전성 확보조치 여부 등을 정기적으로 관리·감독하고 그 결과를 '수탁업체 개인정보보호 실태 점검표'를 이용하여 기록·보관할 수 있음 • 수탁업체를 대상으로 직접 관리·감독이 어려운 경우 수탁업체 자체적으로 개인정보의 안전성 확보조치 등에 대한 점검 등을 실시하여 그 결과를 '수탁업체 개인정보보호 실태 점검표'를 제출 받아 보관하는 것으로 대신할 수 있음 □ 수탁자가 상시적으로 위탁업무를 처리하지 않는 경우, 계약서에 자체 교육 및 감독에 관한 사항을 명시하고 위탁업무 발생 시 보안서약서, 확인서 등 증빙자료를 확보해 놓을 수 있음

2.4.3	위탁에 관한 사실을 인터넷 홈페이지 또는 사보, 접수실, 대기실 등에 공개하고 있는가?
점검기준	☑ 위탁에 관한 사실 공개(필수사항을 포함)여부 확인
증빙자료	☑ 위탁에 관한 사실을 공개한 증빙자료(개인정보 처리방침 등)
관련근거	「개인정보 보호법」 제26조(업무위탁에 따른 개인정보의 처리제한)
세부설명	□ 요양기관(개인정보처리자)은 위탁하는 업무의 내용과 수탁자를 정보주체가 언제든지 쉽게 확인 할 수 있도록 공개해야함 • 공개 필수사항(수탁기관명, 위탁업무내용) • 공개 방법 ① 인터넷 홈페이지(운영 요양기관만 해당)공개내역 화면 ② 사업자의 보기 쉬운 장소인 접수실, 대기실 등에 게재 □ 개인정보 처리방침의 '위탁에 관한 사실' 항목에 포함하여 작성 후 공개 가능함 □ 진료를 목적으로 다른 요양기관 또는 검사기관에 검사를 위탁하는 등 개인정보 처리를 위탁하는 경우 정보주체인 환자의 동의를 받을 필요는 없으나, '표준 개인정보처리위탁 계약서'를 작성하여 보관 필요

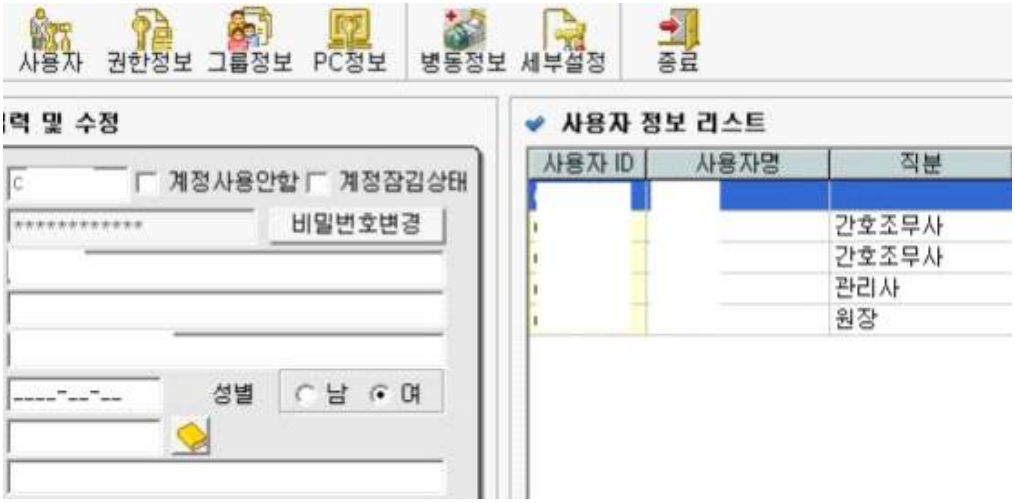
2.5.1	개인정보취급자에 대한 보안서약서를 제출토록 하였는가?
점검기준	☑ 개인정보취급자로부터 보안서약서 수령 여부 확인
증빙자료	☑ 개인정보취급자 보안서약서(임직원, 외부인력) ☑ 비밀유지서약서(퇴직자)
관련근거	「개인정보 보호법」 제28조(개인정보취급자에 대한 감독) 표준 개인정보 보호지침 제15조(개인정보취급자에 대한 감독)
세부설명	□ 정보자산을 취급하거나 접근권한이 부여된 임직원·임시직원·외부자 등이 내부 정책 및 관련 법규, 비밀유지 의무 등 준수사항을 명확히 인지할 수 있도록 업무 특성에 따른 정보보호 서약을 받아야함 • 신규 인력 채용 시 정보보호 및 개인정보보호 책임이 명시된 정보보호 및 개인정보 보호 서약서를 받고 있는가? • 임시직원, 외주용역직원 등 외부자에게 정보자산에 대한 접근권한을 부여할 경우 정보보호 및 개인정보보호에 대한 책임, 비밀유지 의무 등이 명시된 서약서를 받고 있는가? • 임직원 퇴직 시 별도의 비밀유지에 관련한 서약서를 받고 있는가? • 정보보호, 개인정보보호 및 비밀유지 서약서는 안전하게 보관하고 필요 시 쉽게 찾아볼 수 있도록 관리하고 있는가?

2.5.2	개인정보취급자에 대한 정기적인 교육은 실시하고 있는가?
점검기준	☑ 내부관리계획 또는 연간 개인정보보호 교육계획에 따른 교육 실시 여부 확인 (연 1회 이상 교육 실시하여야 함)
증빙자료	☑ 개인정보보호 교육 결과(교육 수료증, 교육 참석 서명록 등)
관련근거	개인정보 보호법 제26조(업무위탁에 따른 개인정보의 처리 제한) 제28조(개인정보 취급자에 대한 감독) 제29조(안전조치의무) 개인정보의 안전성 확보조치 기준 제4조(내부관리계획의 수립·시행) 개인정보의 기술적·관리적 보호조치 기준 제3조(내부관리계획의 수립·시행)
세부설명	□ 직원(개인정보취급자)을 대상으로 매년 정기적으로 개인정보보호 교육을 실시하여야 함 ※ 교육내용 및 방법은 요양기관 자체 내부관리계획(3.1.1 항목)에 따라 시행 • 교육방법: 기관의 환경을 고려하여 집합교육, 인터넷 교육, 외부교육과정 참석, 전문 강사초빙 등 다양한 방법을 활용 • 교육대상: 개인정보 및 관련설비(서버, PC, CCTV등)에 직·간접적으로 접근하는 내부직원 및 외주용역업체 직원 등 모든 인력 포함

지표별 가이드

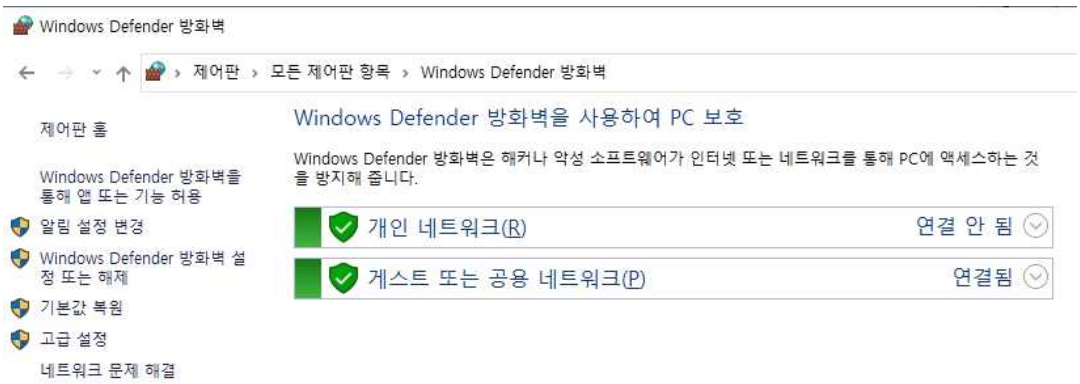
Ⅲ. 개인정보의 안전한 관리

<table>
<tr><td>3.1.1</td><td colspan="6">내부관리 계획을 수립하고 필수사항을 포함하고 있는가?</td></tr>
<tr><td>점검기준</td><td colspan="6">☑ 필수 사항을 포함한 내부관리계획(필수사항 ①~⑮) 수립 여부 확인
<table>
<tr><td colspan="2" rowspan="2">구 분</td><td colspan="4">개인정보처리자의 개인정보 보유량 (전체 총합)</td></tr>
<tr><td>1만명 미만</td><td>1만명~10만명 미만</td><td>10만명~100만명 미만</td><td>100만명 이상</td></tr>
<tr><td rowspan="8">개인정보처리자유형</td><td>공공기관</td><td colspan="2" rowspan="3">유형2(표준)</td><td colspan="2" rowspan="3">유형3(강화)</td></tr>
<tr><td>대기업</td></tr>
<tr><td>중견기업</td></tr>
<tr><td>중소기업</td><td colspan="3">유형2(표준)</td><td>유형3(강화)</td></tr>
<tr><td>소상공인</td><td rowspan="2">유형1(완화)</td><td colspan="3" rowspan="2">유형2(표준)</td></tr>
<tr><td>개인</td></tr>
<tr><td>단체</td><td>유형1(완화)</td><td colspan="2">유형2(표준)</td><td>유형3(강화)</td></tr>
</table>
※ 유형1 : 내부관리계획 의무사항 아님
※ 유형2 : 내부관리계획의 필수 사항 중 12, 13, 14번을 포함하지 아니할 수 있음
※ 유형3 : 내부관리계획 내 15개 사항 모두를 포함하여야 함</td></tr>
<tr><td>증빙자료</td><td colspan="6">☑ 내부관리계획서(필수 반영 사항 포함)</td></tr>
<tr><td>관련근거</td><td colspan="6">「개인정보 보호법」 제29조(안전조치 의무)
「개인정보보호법 시행령」 제30조(개인정보의 안전성 확보 조치)
「개인정보의 안전성 확보조치 기준」 제4조(내부 관리 계획의 수립·시행)
「개인정보의 기술적·관리적 보호조치 기준」 제3조(내부관리계획의 수립·시행)</td></tr>
<tr><td>세부설명</td><td colspan="6">☐ 내부관리계획의 필수 사항
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. 접근통제에 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</td></tr>
</table>

3.2.1	개인정보처리시스템(전자차트, 청구S/W 등)에 대한 접근 권한을 최소한의 범위로 업무담당자에 따라(1인 1계정) 차등 부여하였는가?
점검기준	☑ 업무담당자별 1인1계정 부여 (*계정공유금지) 여부 확인 ☑ 개인정보처리시스템 업무담당자별 접근권한 관리 여부 확인
증빙자료	☑ 접속계정(ID) 등록 현황 및 부여된 권한내역 자료(사용자ID관리대장) 또는 화면 캡처 (예시) 
관련근거	「개인정보 보호법」 제29조(안전조치 의무) 「개인정보의 안전성 확보조치 기준」 제5조(접근 권한의 관리) 「개인정보의 기술적·관리적 보호조치 기준」 제4조(접근통제)
세부설명	□ 요양기관(개인정보처리자)은 개인정보처리시스템에 대한 접근권한을 각 업무담당자별 1계정을 부여하여야 함 □ 요양기관이 관리하는 환자(정보주체)의 개인정보가 1만 명 이상인 경우 개인정보처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 업무담당자에 따라 차등 부여하여야 함

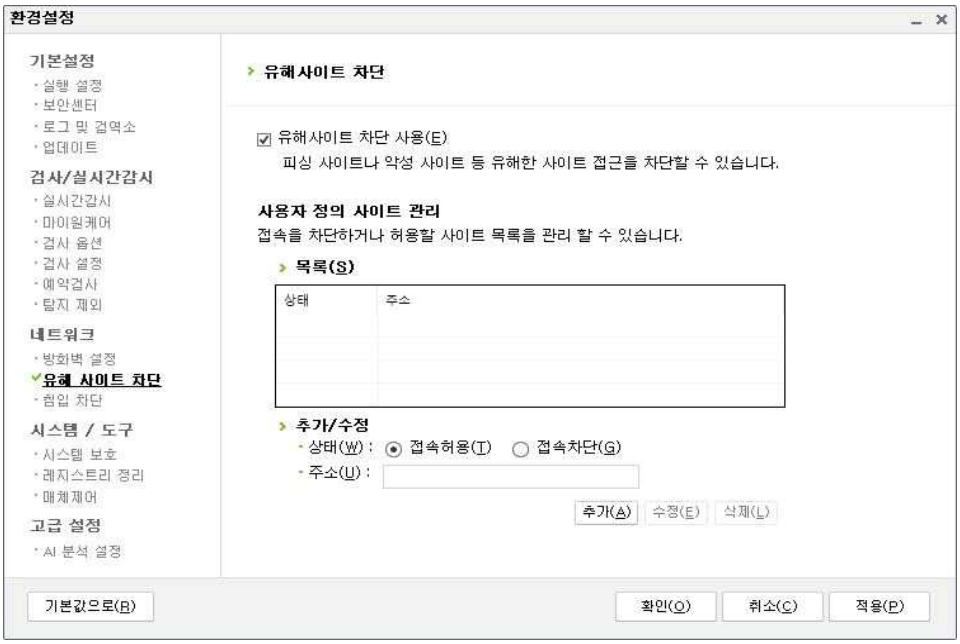
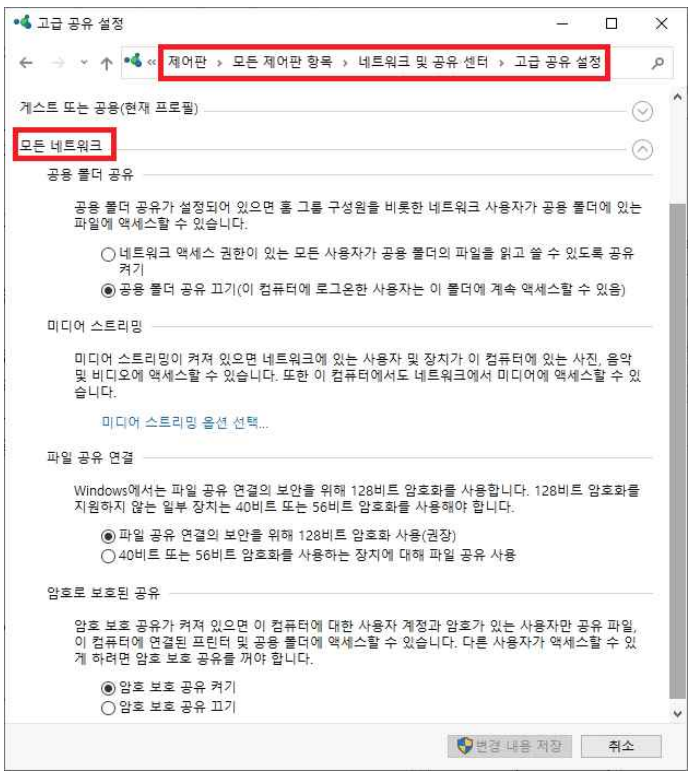
3.2.2	개인정보처리시스템(전자차트, 청구S/W 등) 접근 권한의 부여·변경·말소 내역의 기록 관리를 최소 3년간 보관하고 있는가?
점검기준	☑ 업무별 접근권한관리 기록 보관(3년 이상) 여부 확인
증빙자료	☑ 업무별 권한의 부여, 변경, 말소내역을 확인할 수 있는 관리 기록 (사용자ID 관리대장)
관련근거	「개인정보 보호법」 제29조(안전조치 의무) 「개인정보의 안전성 확보조치 기준」 제5조(접근 권한의 관리) 「개인정보의 기술적·관리적 보호조치 기준」 제4조(접근통제)
세부설명	□ 권한 부여·변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 함 □ 전보 또는 퇴직 등 인사이동이 발생하여 직원(개인정보취급자)이 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여야 함

<table>
<tr><td>3.2.3</td><td>안전한 비밀번호 작성규칙을 적용하고 있는가?</td></tr>
<tr><td>점검기준</td><td>☑ 안전한 비밀번호 작성규칙(PC, 개인정보처리시스템 등) 준수 여부 확인</td></tr>
<tr><td>증빙자료</td><td>☑ 웹페이지, 정보시스템 및 개인정보처리시스템 비밀번호 설정 화면
☑ 비밀번호 관리 정책 및 절차</td></tr>
<tr><td>관련근거</td><td>「개인정보 보호법」 제29조(안전조치 의무)
「개인정보의 안전성 확보조치 기준」 제5조(접근 권한의 관리)
「개인정보의 기술적·관리적 보호조치 기준」 제4조(접근통제)</td></tr>
<tr><td>세부설명</td><td>□ 비밀번호 설정방법
<table>
<tr><th>비밀번호 길이</th><th>문자 종류</th><th>혼합 종류</th></tr>
<tr><td>10자리 이상인 경우</td><td rowspan="2">알파벳 대문자, 알파벳 소문자, 특수문자, 숫자</td><td>두 종류 이상</td></tr>
<tr><td>8자 이상인 경우</td><td>세 종류 이상</td></tr>
</table>
※ 비밀번호는 최소 6개월마다 변경해야 함
※ 비밀번호는 쉬운 단어*를 제외하고, 유추하기 어렵게 설정해야 함
* 일련번호(12345678), 전화번호, 잘 알려진 단어(love, happy), 키보드 상 나란히 있는 문자열(qwer) 등</td></tr>
</table>

3.2.4	개인정보처리시스템(전자차트, 청구S/W 등)에 대하여 불법적인 접근 및 침해사고를 방지하기 위한 접근통제시스템을 설치/운영하고 있는가?
점검기준	☑ (업무용 PC) 백신, 방화벽 기능을 가진 SW 설치 및 점검 여부 확인 ☑ (서버급 이상) 접근통제 관련 HW 및 SW 설치 및 운영 여부 확인
증빙자료	☑ (업무용 PC) 컴퓨터 운영체제(Windows OS 등) 및 백신프로그램에서 제공하는 방화벽 설정 화면 캡처 ☑ (서버급 이상) 침입통제시스템을 도입한 경우 정책적용 내역 (예시) 윈도우 방화벽  (예시) 백신 방화벽 

관련근거	「개인정보 보호법」 제29조(안전조치 의무) 「개인정보의 안전성 확보조치 기준」 제6조(접근통제) 「개인정보의 기술적·관리적 보호조치 기준」 제4조(접근통제)
세부설명	□ **3가지 중 반드시 1가지 이상 적용해야 함** ① 컴퓨터의 운영체제(윈도우 등)의 기본 기능을 이용하여 방화벽 사용 ※ 윈도우의 [설정] – [제어판] – [Windows방화벽] '사용' 클릭 ② 보안프로그램(알약, V3 등)의 방화벽 사용 ③ 보안업체에서 제공하는 보안 서비스 (침입방지시스템 등)

3.2.5	외부에서 정보통신망을 통한 접속 시 가상 사설망, 전용선 등 안전한 접속수단 혹은 안전한 인증수단을 제공하고 있는가?
점검기준	☑ 외부망과 연결된 서버에 가상사설망(VPN: Virtual Private Network), 전용선 등의 안전한 접속 수단 제공
증빙자료	☑ 전자차트, 청구S/W 등 개인정보처리시스템 로그인 방식 화면 캡처 ▪ 정보시스템 운영체제 계정 목록 ▪ 서버 보안 설정 ▪ 서버접근제어 정책(SecureOS 관리화면 등) ▪ 서버 및 네트워크 구성도 ▪ 정보자산 목록
관련근거	「개인정보 보호법」 제29조(안전조치 의무) 「개인정보의 안전성 확보조치 기준」 제6조(접근통제) 「개인정보의 기술적·관리적 보호조치 기준」 제4조(접근통제)
세부설명	□ 개인정보처리시스템은 외부망(인터넷 되는 PC)에서 원칙적으로 차단이 되어야 함 – 단, 개인정보취급자가 외부망으로 개인정보처리시스템에 접속해야 한다면 다음 **2가지 중 1가지 이상 적용해야 함** ① 안전한 접속수단 적용: 가상사설망(VPN)이나 전용선 등 ② 안전한 인증수단 적용: 공동인증서, 일회용 비밀번호(OTP), 보안토큰 등 【참고】 외부와 접속가능한 통신망 확인 후 VPN 또는 전용선 사용여부 확인 혹은 안전한 인증수단 사용여부 확인 ※ 외부망과 연결된 서버 운용 시 전용선, VPN 외 IP, MAC, 공동인증서 등을 통해서 접속을 제한하여 처리가능

3.2.6	P2P(peer to peer), 웹하드 등 비인가프로그램의 접속을 차단하고 있는가?
점검기준	(업무용 PC) ☑ 공유폴더 제거 및 비인가 프로그램 접속 차단여부 확인 (서버급 이상) ☑ 침입차단 시스템의 설치 및 운영여부 확인 ☑ 공유폴더 제거 여부 확인
증빙자료	☑ (업무용 PC) 기업용 백신SW 설정 화면 캡처 (예시) 백신 유해사이트 차단  (예시) 공유폴더 제거 ([설정] – [제어판] – [네트워크 및 공유 센터]) 

	☑ 서버급 이상 ▪ 비업무사이트(P2P 등) 차단정책(비업무사이트 차단시스템 관리화면 등) ▪ 인터넷 접속내역 모니터링 이력 ▪ 망분리 대상자 목록 ▪ 망간 자료 전송 절차 및 처리내역(신청·승인내역 등) ▪ 네트워크 구성도
관련근거	「개인정보 보호법」 제29조(안전조치 의무) 「개인정보의 안전성 확보조치 기준」 제6조(접근통제) 「개인정보의 기술적·관리적 보호조치 기준」 제4조(접근통제)
세부설명	□ 취급중인 개인정보가 외부경로를 통해 유출되거나 권한없는 사람에게 공개되지 않도록 조치해야 함 – 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망(Wifi) 이용 등 외부경로에서 개인정보가 유출되지 않도록 조치 필요 – 개인정보처리시스템, 업무용 컴퓨터 및 모바일 기기 등에 조치 필요 □ 기업용 백신SW 등 보안 프로그램을 이용하여 유해사이트 접속 차단 가능함 – 방화벽(V3), 브라우저(IE) 등 □ 차단이 어려운 경우 해당 비인가 프로그램을 삭제 조치 후 다시 설치되지 않도록 관리하면 됨 – (윈도우OS) [시작>제어판>성능 및 유지관리>관리도구>컴퓨터관리] 공유폴더 확인 ※ 공유폴더 이용하는 업무 진행 시 공유폴더 암호 설정 및 사용 후 공유폴더를 해제해야 함 □ 공유기를 이용한 무선망을 사용하는 경우 안전한 비밀번호 적용해야 함

3.2.7	인터넷 홈페이지의 개인정보 노출 방지를 위한 보안 조치를 실시하고 있는가?
점검기준	☑ 홈페이지 개인정보 노출방지 점검 및 보완조치 여부 확인 ☑ 홈페이지 웹 취약점 점검 여부 확인
증빙자료	☑ 홈페이지 개인정보 노출방지 점검, 웹 취약점 점검 수행 결과
관련근거	「개인정보 보호법」 제29조(안전조치 의무) 「개인정보의 안전성 확보조치 기준」 제6조(접근통제) 「개인정보의 기술적·관리적 보호조치 기준」 제4조(접근통제)
세부설명	□ 인터넷 홈페이지를 통해 개인정보가 유출되지 않도록 **연 1회 이상 홈페이지를 점검하는 것**을 권장함 - 홈페이지 개인정보 노출 진단 모니터링 방법 □ 인터넷 홈페이지에서 고유식별정보(여권번호, 운전면허번호, 외국인등록번호)를 처리하고 환자(정보주체)의 개인정보가 1만명 이상인 경우, 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하여야 함 - KISA 보호나라(www.boho.or.kr) 홈페이지를 통해 웹 취약점을 점검 가능

3.2.8	계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 접근을 제한하고 있는가?
점검기준	☑ 개인정보처리시스템(전자차트, 청구 S/W, 홈페이지 등)에 접속하는 계정 또는 비밀번호를 일정 횟수 이상 잘못 입력 시 접근 제한 여부 확인
증빙자료	☑ 일정 횟수 이상의 접속계정(ID), 비밀번호 오류 시 안내되는 메시지 화면 캡처 등
관련근거	「개인정보 보호법」 제29조(안전조치 의무) 「개인정보의 안전성 확보조치 기준」 제5조(접근 권한의 관리) 제6조(접근통제) 「개인정보의 기술적·관리적 보호조치 기준」 제4조(접근통제)
세부설명	□ 요양기관 담당자(개인정보처리자)는 아래 2가지를 방지해야 함 ① 개인정보처리시스템(전자차트, 청구 S/W, 홈페이지 등)에 권한 없는 자의 비정상적인 접근한 경우 – (예시) 권한없는 사용자의 접속을 차단하는 보안프로그램 사용 ② 계정 정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 – (예시) 5회이상 잘못 입력 시 계정 잠금, 계정 해제 시 추가적인 인증수단(공동인증서, OTP 등)을 통하여 사용자 확인 후 계정 잠금 해제

3.2.9	일정시간 이상 업무처리를 하지 않을 시 자동으로 시스템 접속이 차단되도록 하고 있는가?
점검기준	☑ 개인정보처리시스템(전자차트, 청구 S/W, 홈페이지 등)에서 일정시간 이상 업무처리를 하지 않을 시 자동으로 시스템 접속 차단 여부 확인
증빙자료	☑ 개인정보처리시스템에 접속 후 일정시간 활동이 없는 경우, 자동 로그아웃 처리되는 화면 또는 기능적용 화면 캡처
관련근거	「개인정보 보호법」 제29조(안전조치 의무) 「개인정보의 안전성 확보조치 기준」 제6조(접근통제) 「개인정보의 기술적·관리적 보호조치 기준」 제4조(접근통제)
세부설명	□ 개인정보 유출 방지를 위해 요양기관 담당자(개인정보처리자)가 일정시간 이상 업무처리 하지 않는 경우 자동으로 시스템을 차단해야 함 – (예시) 개인정보처리시스템에 접속 후 30분 이상 업무처리를 하지 않는 경우, 자동으로 로그아웃되며 재접속 시 최초 로그인할 때와 동일한 방법으로 접속해야 함 【참고】 시스템 접속차단은 개인정보처리시스템 연결해제를 의미하며, 업무용 컴퓨터의 화면보호기 등은 접속차단에 해당하지 않음

3.3.1	고유식별정보, 비밀번호 및 생체정보를 개인정보처리시스템(전자차트, 홈페이지, 청구S/W 등)에 저장 시 암호화 하고 있는가?
점검기준	☑ 개인정보처리시스템(전자차트, 홈페이지, 청구S/W 등)에 저장된 고유식별정보, 비밀번호 및 생체정보의 암호화 적용여부 확인
증빙자료	☑ 개인정보처리시스템 내 고유식별정보, 비밀번호, 생체정보의 암호화 저장된 화면 캡처 등
관련근거	「개인정보 보호법」 제29조(안전조치 의무) 「개인정보의 안전성 확보조치 기준」 제7조(개인정보의 암호화) 「개인정보의 기술적·관리적 보호조치 기준」 제6조(개인정보의 암호화)
세부설명	□ 고유식별정보, 비밀번호 및 생체정보를 개인정보처리시스템(전자차트, 홈페이지, 청구S/W 등)에 저장 시 암호화 조치를 취해야 함

3.3.2	고유식별정보, 비밀번호 및 생체정보를 컴퓨터(업무용PC) 및 모바일기기에 저장 시 암호화하고 있는가?
점검기준	☑ 업무용 PC 및 모바일기기에 저장된 고유식별정보, 비밀번호 및 생체정보의 암호화 여부 확인 ☑ 개인정보처리시스템에서 파일 다운로드 기능이 있는 경우
증빙자료	☑ 업무용 컴퓨터(모바일기기 포함)에 저장된 파일 더블클릭 시 비밀번호를 물어보는 화면 캡처 등
관련근거	「개인정보 보호법」 29조(안전조치 의무) 「개인정보의 안전성 확보조치 기준」 제7조(개인정보의 암호화) 「개인정보의 기술적·관리적 보호조치 기준」 제6조(개인정보의 암호화)
세부설명	□ 업무용 컴퓨터 또는 모바일 기기에 고유식별정보, 비밀번호 및 생체정보를 저장하여 관리하는 경우 아래와 같이 암호화시켜 안전하게 보관해야 함 – 문서편집기(한글, MS-Office 등): 비밀번호 설정기능 사용 – 압축프로그램 이용한 파일 압축 및 비밀번호 설정 – 암호화 알고리즘이 적용된 암호화 소프트웨어를 사용 ※ 비밀번호 설정 시 단순 숫자 또는 문자열 사용 금지 (3.2.3 참고)

3.3.3	고유식별정보, 비밀번호 및 생체정보를 정보통신망을 통하여 송·수신하거나 보조저장매체를 통하여 전달 시 암호화하고 있는가?
점검기준	☑ 고유식별정보, 비밀번호 및 생체정보를 정보통신망(이메일, 메신저 등)을 통하여 송·수신하거나 보조저장매체 등을 통해 전달하는 경우 이를 암호화 여부 확인 ☑ (보조기억매체) 보안USB 등 사용 여부 확인
증빙자료	☑ (보조기억매체 활용시) 보안USB 비밀번호 입력 화면 캡처 등
관련근거	「개인정보 보호법」 제29조(안전조치 의무) 「개인정보의 안전성 확보조치 기준」 제7조(개인정보의 암호화) 「개인정보의 기술적·관리적 보호조치 기준」 제6조(개인정보의 암호화)
세부설명	□ 고유식별정보, 비밀번호 및 생체정보를 정보통신망을 통하여 송·수신하거나 보조저장매체 등을 통해 전달하는 경우 아래와 같이 암호화시켜 안전하게 보관해야 함 – 암호화 알고리즘이 적용된 암호화 소프트웨어를 사용 □ 홈페이지에서 개인정보를 수집하는 기관의 경우 SSL/TLS 등의 통신 암호화를 적용하여야 함

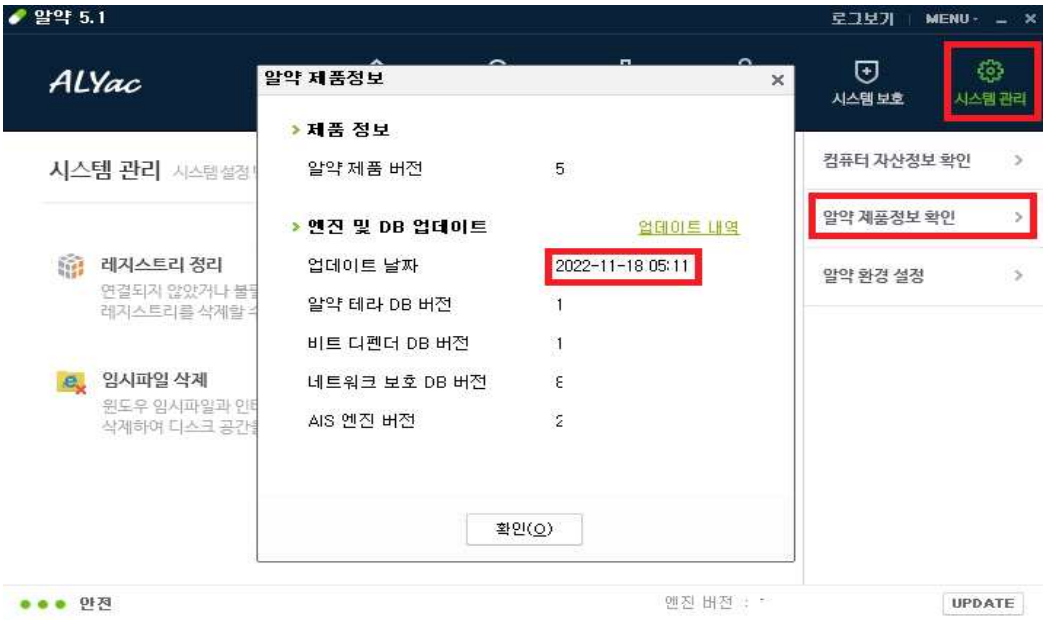
3.3.4	고유식별정보, 비밀번호 및 생체정보를 암호화하여 저장 시 안전한 암호 알고리즘 사용을 하였는가?
점검기준	☑ 암호화 시 안전한 암호 알고리즘을 사용 여부 확인
증빙자료	☑ 개인정보처리시스템내 데이터베이스(DB)에 저장된 값 또는 알고리즘 적용을 위한 프로그램 소스 화면 캡처 등
관련근거	「개인정보 보호법」 제29조(안전조치 의무) 「개인정보의 안전성 확보조치 기준」 제7조(개인정보의 암호화) 「개인정보의 기술적·관리적 보호조치 기준」 제6조(개인정보의 암호화)
세부설명	□ 개인정보처리시스템에 고유식별정보, 비밀번호, 생체정보를 암호화하여 저장 시, 안전한 암호알고리즘을 사용해야함 【참고】 안전한 암호알고리즘, 암호화 방식 등은 “개인정보 암호화 조치 안내서” 참조 ※ 보호위원회 홈페이지(www.pipc.go.kr)에서 다운로드 가능

3.3.5	고유식별정보를 인터넷과 내부망의 중간지점(DMZ)에 저장 시 암호화하고 있는가?
점검기준	☑ 홈페이지 운영 시 고유식별정보를 인터넷 구간 및 인터넷 구간과 내부망의 중간지점(DMZ)에 저장하는 경우 암호화하여 저장하는지 확인
증빙자료	☑ 중간지점(DMZ) 구간에서 운영하는 개인정보처리시스템내 데이터베이스(DB)에 저장된 값 등 캡처
관련근거	「개인정보 보호법」 제29조(안전조치 의무) 「개인정보의 안전성 확보조치 기준」 제7조(개인정보의 암호화) 「개인정보의 기술적·관리적 보호조치 기준」 제6조(개인정보의 암호화)
세부설명	□ 고유식별정보를 인터넷PC·서버(DMZ)에 저장하는 경우 암호화 하여 저장하는지 확인하여야 함 - DMZ는 인터넷PC와 업무PC(인트라넷) 사이 침입차단시스템 등 중간지점의 서버를 말하며, 인터넷PC에서 직접 접근이 가능한 영역임

3.3.6	안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립하고 있는가?
점검기준	☑ 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차 수립 여부
증빙자료	☑ 암호 키 관리 절차서
관련근거	「개인정보 보호법」 29조(안전조치 의무) 「개인정보의 안전성 확보조치 기준」 제7조(개인정보의 암호화) 「개인정보의 기술적·관리적 보호조치 기준」 제6조(개인정보의 암호화)
세부설명	□ 안전한 암호 키 생성, 저장, 분배, 백업, 복구, 파기 등에 관한 절차 수립·시행 여부 확인 1. 암호 키와 관련된 절차를 수립하고 시행 2. 암호 키는 암호화된 데이터를 복호화 할 수 있는 정보이므로 암호 키의 안전한 사용과 관리는 매우 중요하며 라이프사이클 단계별 암호 키 관리 절차를 수립 시행 【참고】 - 개인정보보호위원회, 한국인터넷진흥원, 『개인정보의 안전성 확보조치 기준 해설서(2020.12)』

3.4.1	개인정보취급자의 접속기록을 최소 2년 이상 보관하여 관리하고 있는가?
점검기준	☑ 개인정보취급자의 접속기록을 최소 2년 이상 보관 및 관리여부 확인
증빙자료	☑ 접속기록 생성일자를 확인할 수 있는 자료 또는 화면 캡처 등
관련근거	「개인정보 보호법」 제29조(안전조치 의무) 「개인정보의 안전성 확보조치 기준」 제8조(접속기록의 보관 및 점검) 「개인정보의 기술적·관리적 보호조치 기준」 제5조(접속기록의 위·변조 방지)
세부설명	□ 개인정보처리시스템(전자차트, 청구S/W 등)에 접속한 기록이 위 · 변조 및 도난, 분실되지 않도록 접속기록*을 최소 2년 이상 보관 · 관리하여야 함 * 개인정보처리시스템 수행한 업무내역(개인정보취급자 계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등)이 전자적으로 기록된 것 □ 개인정보처리시스템을 위탁·운영하는 경우 수탁업체에 2년 이상 접속기록 보관 여부를 확인하여야 함 ※ 해당 기능이 불가능한 개인정보처리시스템인 경우, 수탁업체에 기능 추가를 요청하여야 함 □ 개인정보의 유출·변조·훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 함 – 이와 함께, 개인정보를 다운로드한 것이 발견되었을 경우에는 내부관리계획으로 정하는 바에 따라 그 사유를 반드시 확인 ※ 접속기록의 필수 항목(5개) ① 계정 ② 접속일시 ③ 접속지 정보 ④ 처리한 정보주체 정보: 처리자 성명, ID 등 ⑤ 수행업무: 열람, 수정, 삭제, 인쇄, 입력 등

3.4.2	접속기록의 위·변조 및 도난, 분실되지 않도록 접속 기록을 안전하게 보관하고 있는가?
점검기준	☑ 개인정보처리시스템(전자차트, 청구S/W 등)에 접속한 기록을 위·변조 및 도난, 분실되지 않도록 안전하게 보관하는지 여부
증빙자료	☑ 접속기록을 별도의 저장매체(외장형 하드디스크, USB메모리 등)에 저장하여 보관하고 있는 사진 또는 별도 지정된 장소에 보관하고 있는 사진
관련근거	「개인정보 보호법」 제29조(안전조치 의무) 「개인정보의 안전성 확보조치 기준」 제8조(접속기록의 보관 및 점검) 「개인정보의 기술적·관리적 보호조치 기준」 제5조(접속기록의 위·변조 방지)
세부설명	□ 대표자(원장, 약국장)은 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 함 【참고】 보관방법 ① 접속기록 위·변조 방지 방법 – 접속기록을 백업하여 개인정보처리시스템 이외의 별도의 저장매체(USB, 외장하드, CD, DVD 등)에 보관 ▪ (예시) 개인정보처리시스템(전자 차트, 청구 S/W 등)의 데이터 및 접속기록을 일괄 백업하여 보조저장매체(USB, 외장하드 등)에 보관 ② 접속기록을 안전하게 보관하는 방법 – 별도 지정된 장소(통제구역), 금고 또는 잠금 장치가 있는 캐비넷(보관함) 등에 보관

3.5.1	개인정보처리시스템이 설치된 업무용 PC에 백신 프로그램 등의 보안 프로그램의 설치 및 업데이트, 악성프로그램 삭제 등 지속적으로 관리하고 있는가?
점검기준	☑ 발견된 악성프로그램 등에 대한 대응 조치여부 확인 ☑ 최신 보안 프로그램 설치 여부 확인 – 자동업데이트 혹은 일 1회 이상의 업데이트 실시
증빙자료	☑ 업무용 PC에 설치된 기업용 백신프로그램의 최근 업데이트 날짜 화면 캡처 
관련근거	「개인정보 보호법」 제29조(안전조치 의무) 「개인정보의 안전성 확보조치 기준」 제9조(악성프로그램 등 방지) 「개인정보의 기술적·관리적 보호조치 기준」 제7조(악성프로그램 방지)
세부설명	□ 악성프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 함 – 업무용 PC에는 개인용 백신S/W가 아닌 기업용 백신S/W를 사용하여야 함 ※ 기업용 백신S/W가 없을 시: 심평원 제공 DUR모듈에 포함된 백신 S/W(AhnLab Online Security) 사용 가능 – 백신S/W는 항상 활성화 시켜두고, **월 1회 이상 정기적으로 검사**하는 것을 권장 □ 보안 프로그램의 자동 업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지하여야 함

3.6.1	개인정보 등 중요자료가 보관된 물리적 장소에 대한 출입통제 절차를 수립하여 운영하고 있는가?
점검기준	☑ 물리적 보관장소에 대한 출입통제 절차 수립 여부 확인 ☑ 출입관리 대장을 작성·관리여부 확인
증빙자료	☑ 출입통제 절차서, 출입관리대장
관련근거	「개인정보 보호법」 제29조(안전조치의무) 「개인정보의 안전성 확보조치 기준」 제11조(물리적 안전조치) 「개인정보의 기술적·관리적 보호조치 기준」 제8조(물리적 접근방지)
세부설명	□ 요양기관에 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 함(가이드 86페이지 참조) □ 출입 통제방법 – 통제구역 설정, 통제구역 잠금장치 및 지정된 자만 출입, 출입자 명부 작성 등

3.6.2	개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하고 있는가?
점검기준	☑ 개인정보가 포함된 서류, 보조저장매체를 별도 지정된 통제구역, 금고, 잠금장치가 있는 보관함에 보관 여부 확인
증빙자료	☑ 통제구역, 금고, 잠금장치가 있는 보관함 사진
관련근거	「개인정보 보호법」 제29조(안전조치 의무) 「개인정보의 안전성 확보조치 기준」 제10조(관리용 단말기의 안전조치) 제11조(물리적안전조치) 「개인정보의 기술적·관리적 보호조치 기준」 제8조(물리적 접근방지) 제9조(출력·복사 시 보호조치)
세부설명	□ 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 함 – 개인정보가 포함된 서류, 보조저장매체 등의 보관 시, 별도 보관 장소가 없는 경우나 임시로 보관이 필요한 경우에는 잠금장치가 있는 보관시설(캐비닛, 금고 등)에 보관하여야 함 □ 개인정보가 포함된 서류(진료기록부, 처방전 등)을 안전한 장소에 보관하지 않고 책상 등 공개된 장소에 방치 금지

<table>
<tr><td>3.7.1</td><td>개인정보 처리방침을 수립하고 있는가?</td></tr>
<tr><td>점검기준</td><td>☑ 필수항목(8개)을 포함한 개인정보 처리방침 수립 여부</td></tr>
<tr><td>증빙자료</td><td>☑ 개인정보 처리방침</td></tr>
<tr><td>관련근거</td><td>「개인정보 보호법」 제30조(개인정보 처리방침의 수립 및 공개)</td></tr>
<tr><td>세부설명</td><td>□ 다음 각 호의 사항이 포함된 개인정보 처리방침을 정하여야 함
<table>
<tr><th>구분</th><th>기재사항</th><th></th></tr>
<tr><td>1</td><td>제목 및 서문</td><td>의무</td></tr>
<tr><td>2</td><td>개인정보의 처리 목적</td><td>의무</td></tr>
<tr><td>3</td><td>개인정보의 처리 및 보유 기간</td><td>의무</td></tr>
<tr><td>4</td><td>처리하는 개인정보의 항목</td><td>의무</td></tr>
<tr><td>5</td><td>개인정보파일 등록 현황</td><td>의무 해당시</td></tr>
<tr><td>6</td><td>개인정보 영향평가 수행 결과</td><td>권장 해당시</td></tr>
<tr><td>7</td><td>개인정보의 제3자 제공에 관한 사항</td><td>의무 해당시</td></tr>
<tr><td>8</td><td>개인정보처리의 위탁에 관한 사항</td><td>의무 해당시</td></tr>
<tr><td>9</td><td>개인정보의 파기절차 및 파기방법</td><td>의무</td></tr>
<tr><td>10</td><td>정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항</td><td>의무</td></tr>
<tr><td>11</td><td>개인정보의 안전성 확보조치에 관한 사항</td><td>의무</td></tr>
<tr><td>12</td><td>개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항</td><td>의무 해당시</td></tr>
<tr><td>13</td><td>가명정보를 처리하는 경우 가명정보 처리에 관한 사항</td><td>의무 해당시</td></tr>
<tr><td>14</td><td>개인정보 보호책임자에 관한 사항</td><td>의무</td></tr>
<tr><td>15</td><td>개인정보의 열람청구를 접수·처리하는 부서</td><td>의무</td></tr>
<tr><td>16</td><td>정보주체의 권익침해에 대한 구제방법</td><td>의무</td></tr>
<tr><td>17</td><td>개인정보 관리수준진단 결과</td><td>권장</td></tr>
<tr><td>18</td><td>영상정보처리기기 운영·관리에 관한 사항</td><td>권장 해당시</td></tr>
<tr><td>19</td><td>개인정보 처리방침의 변경에 관한 사항</td><td>의무</td></tr>
<tr><td>20</td><td>그밖에 개인정보처리자가 개인정보 처리 기준 및 보호조치 등에 관하여 자율적으로 개인정보 처리방침에 포함하여 정한 사항</td><td>권장 해당시</td></tr>
</table>
【참고】 개인정보보호 포털(www.privacy.go.kr)의 ‘개인정보 처리방침 만들기’ 활용방법 참조</td></tr>
</table>

3.7.2	개인정보 처리방침을 홈페이지 또는 보기 쉬운 장소(접수대, 대기실 등)에 공개하고 있는가?
점검기준	☑ 개인정보 처리방침 공개여부 확인
증빙자료	☑ 개인정보 처리방침 공개 사실을 확인할 수 있는 자료
관련근거	「개인정보 보호법」 제30조(개인정보 처리방침의 수립 및 공개)
세부설명	□ 개인정보 처리방침은 인터넷 홈페이지, 대기실 등을 통하여 환자(정보주체)가 언제든지 쉽게 확인할 수 있도록 공개하여야 함 □ 개인정보 처리방침을 변경하는 경우에는 변경 및 시행시기, 변경된 내용을 보기 쉬운 장소(인터넷 홈페이지 등)를 통해 지속적으로 공개하여야 함

3.8.1	개인정보 보호책임자가 지정되고 그 역할이 정의되어 있는가?
점검기준	☑ 개인정보 보호책임자가 자격요건에 맞게 문서로 지정되었는지 여부
증빙자료	☑ 개인정보 보호책임자 지정 및 역할 확인이 가능한 문서 – 내부관리계획, 업무 분장표, 직제표, 개인정보 처리방침 등
관련근거	「개인정보 보호법」 제31조(개인정보 보호책임자의 지정)
세부설명	□ 대표자(원장·약국장)은 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 지정하여야 함 또한, 적절한 책임·권한·역할을 아래와 같은 문서를 통하여 정의하여야 함 – 내부관리계획, 업무 분장표, 직제표, 개인정보 처리방침 등 □ 개인정보 보호책임자의 지정요건 ① 사업주 또는 대표자 ② 정보주체의 개인정보 보호업무를 위해 조직된 부서의 장 또는 개인정보보호에 관한 소양이 있는 사람 □ 개인정보 보호책임자는 다음 각 호의 업무를 수행함 ① 개인정보보호 계획의 수립 및 시행 ② 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선 ③ 개인정보 처리와 관련한 불만의 처리 및 피해구제 ④ 개인정보 유출 및 오용·남용방지를 위한 내부통제시스템의 구축 ⑤ 개인정보 보호 교육 계획의 수립 및 시행 ⑥ 개인정보 파일의 보호 및 관리 · 감독 ⑦ 그 밖에 개인정보의 적절한 처리를 위하여 대통령령으로 정한 업무 – 개인정보 처리방침의 수립·변경 및 시행 – 개인정보 보호 관련 자료의 관리 – 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기 □ 기타 개인정보 보호책임자의 활동(권장) – 개인정보보호 전담조직 구성 및 전담인력 확보 – 개인정보보호 활동을 수행하는데 필요한 예산 확보 및 반영 (교육비·출장비, 진료차트S/W 등 도입·운영, 백신S/W 등 예산)

3.8.2	개인정보 보호책임자는 개인정보보호 교육을 이수하고 관리·감독을 수행하고 있는가?
점검기준	☑ 개인정보 보호책임자의 교육이수 여부 확인 ☑ 관리 · 감독 활동 수행여부 확인
증빙자료	☑ 개인정보 보호책임자 관리 · 감독 및 제도개선 활동 실적 ☑ 개인정보 보호책임자 교육 이수 실적 – 교육 참석확인증, 수료증 등
관련근거	「개인정보 보호법」 제31조(개인정보 보호책임자의 지정) 제26조(업무위탁에 따른 개인정보의 처리 제한) 제28조(개인정보취급자에 대한 감독) 제29조(안전조치의무) 「개인정보의 안전성 확보조치 기준」 제4조(내부관리계획의 수립·시행) 「개인정보의 기술적·관리적 보호조치 기준」 제3조(내부관리계획의 수립·시행)
세부설명	□ 개인정보 보호책임자 역할 – 개인정보 보호책임자는 기관(사업자)의 개인정보보호 총괄 업무를 수행할 수 있어야 함 【참고】 동법 시행령 제32조 제1항(개인정보 보호책임자의 업무 및 지정요건 등) □ **개인정보 보호책임자 교육이수** – 기관의 환경을 고려하여 집합교육, 인터넷 교육, 외부교육과정 참석, 전문 강사초빙 등 다양한 방법을 활용하여 교육 이수 □ **개인정보 보호책임자 관리 · 감독 활동: (예시)** 개인정보 정기점검 체크리스트 – 각종 관리대장 기록·관리 여부 – 개인정보처리시스템 접속기록 점검 – 운영체제, 백신, 문서편집 프로그램 최신 보안 패치 적용 – 직원변경에 따른 ID, 보안서약서 관리 등

3.9.1	개인정보 유·노출 등 침해사고 발생 시 대응절차를 숙지하고 있는가?
점검기준	☑ 침해사고 대응절차 숙지여부 확인
증빙자료	☑ 동 항목은 별도의 증빙자료가 없어도 점검기준을 준수하는 경우 양호
관련근거	「개인정보 보호법」 제34조(개인정보 유출통지 등)
세부설명	□ 개인정보 침해사고 대응 범위, 절차, 신고방법 등 침해사고 대응절차를 숙지해야 함 【참고】 □ **1천명 이상의 환자(정보주체)의 개인정보가 유출된 경우** 신고절차 – **개인정보보호위원회** 또는 전문기관(한국인터넷진흥원)에 유출 통지 결과를 신고해야 함 – 추가적으로 홈페이지 혹은 대기실 등 원내 보기 쉬운 장소에 **7일 이상** 게시하여야 함

서식 모음

서식(증빙자료) 리스트

연번	서 식 명	지표번호
1	개인정보 수집·이용 동의서	1.1.1 1.1.2 1.2.1 1.2.2 1.2.3 1.3.1
2	개인정보 파기 관리대장	1.5.1 1.5.2
3	민감정보 수집·이용 동의서	2.1.1
4	영상정보 처리기기(CCTV) 운영방침	2.3.1
5	영상정보 처리기기(CCTV) 설치 안내	2.3.2
6	개인영상정보 관리대장	2.3.3
7	표준 개인정보처리위탁 계약서	2.4.1
8	수탁업체 개인정보보호 실태점검표	2.4.2
9	개인정보취급 보안서약서 / 비밀유지서약서	2.5.1
10	개인정보보호 교육 서명록	2.5.2
11	개인정보 내부관리 계획	3.1.1
12	사용자 ID관리대장	3.2.1 3.2.2
13	출입통제절차 / 출입관리대장	3.6.1
14	개인정보 처리방침	3.7.1
15	개인정보 정기점검 체크리스트	3.8.2
16	개인정보 유출시 필수 조치요령 / 개인정보 유출신고서	3.9.1

개인정보 수집·이용 동의서 예시(요양기관)

1.1.1	1.1.2	1.2.1
1.2.2	1.2.3	1.3.1

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

*[요양기관명]*은 *○○○서비스 제공*을 위하여 아래와 같이 개인정보를 수집·이용하고 제3자에게 제공하고자 합니다.

내용을 자세히 읽으신 후 동의 여부를 결정하여 주십시오.

☐ **선택적 개인정보 수집·이용 내역 (선택사항, 동의거부 가능)**

항 목	수집목적	보유기간
☐ 성명 ☐ 전화번호 ☐ 성별 ☐ 결혼 여부 ☐ 연령 ☐ 관심 분야	*예방접종 안내, 최신의학정보*	*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
oo연구소	*맞춤형 의학정보 수집*	*성별, 결혼 여부, 연령, 관심분야*	*1년*

※ 위의 개인정보 제공에 대한 동의를 거부할 권리가 있습니다. 그러나 동의를 거부할 경우 *맞춤형 의학정보 이용에* 제한을 받을 수 있습니다.

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

<기타 고지 사항>

개인정보 보호법 제15조 제1항 제2호에(의료법) 따라 진료목적인 경우 환자(정보주체)의 동의 없이 개인정보를 수집·이용합니다.

개인정보 수집·이용 목적	개인정보 항목	수집 근거
진료기록부 작성	주소·성명·연락처·주민등록번호 등 인적사항, 주된 증상, 진단결과, 진료경과, 치료내용, 진료일시	「의료법」 제22조, 동법 시행규칙 제14조

년 월 일

본인 성명 (서명 또는 인)

법정대리인 성명 (서명 또는 인)

[요양기관명]장 귀중

개인정보 수집·이용 동의서 예시(약국)

1.1.1 1.1.2 1.2.1
1.2.2 1.2.3 1.3.1

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

*[○○약국]*은 *○○○서비스 제공*을 위하여 아래와 같이 개인정보를 수집·이용하고 제3자에게 제공하고자 합니다.

내용을 자세히 읽으신 후 동의 여부를 결정하여 주십시오.

☐ **선택적 개인정보 수집·이용 내역 (선택사항, 동의거부 가능)**

항 목	수집목적	보유기간
☐ 성명 ☐ 전화번호 ☐ 성별 ☐ 결혼 여부 ☐ 연령 ☐ 관심 분야	*예방접종 안내, 최신의학정보*	*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
○○연구소	*맞춤형 의학정보 수집*	*성별, 결혼 여부, 연령, 관심분야*	*1년*

※ 위의 개인정보 제공에 대한 동의를 거부할 권리가 있습니다. 그러나 동의를 거부할 경우 *맞춤형 의학정보 이용에* 제한을 받을 수 있습니다.

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

<기타 고지 사항>

개인정보 보호법 제15조 제1항 제2호에(약사법) 따라 조제, 복약지도 등 진료목적인 경우 환자(정보주체)의 동의 없이 개인정보를 수집·이용 할 수 있습니다.

개인정보 수집·이용 목적	개인정보 항목	수집 근거
진료기록부 작성	주소·성명·연락처·주민등록번호 등 인적사항, 주된 증상, 진단결과, 진료경과, 치료내용, 진료일시	「의료법」 제22조, 동법 시행규칙 제14조

년 월 일

본인 성명 (서명 또는 인)

법정대리인 성명 (서명 또는 인)

[요양기관명]장 귀중

1.5.1
1.5.2

개인정보 파기 관리대장(예시)

번호	개인정보 파일명	자료의 종류	생성일	폐기일	폐기사유	처리담당자	처리부서장
1	환자 종이 청구 정보	종이처방전	2010.9.8	2015.9.8	보존기간 경과	○○○	○○○
2	환자 조제 내역 정보	전산데이터	2010.3.12	2015.3.12	보존기간 경과	○○○	○○○

2.1.1

○○○을 위한 민감정보 수집·이용 동의서(예시)

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

항 목	수집목적	보유기간
민감정보 항목 기재	*수집목적 기재*	*보유기간 기재*

※ 위와 같이 개인정보를 처리하는데 동의를 거부할 권리가 있습니다.
그러나 동의를 거부할 경우 관련 서비스 제공이 제한 될 수 있습니다.

위와 같이 민감정보를 처리하는데 동의하십니까? (예, 아니오)

년 월 일

본인 성명 (서명 또는 인)

※ 정보주체가 만14세 미만의 아동인 경우

위와 같이 민감정보를 처리하는데 동의하십니까? (예, 아니오)

년 월 일

본 인 성명 (서명 또는 인)
법정대리인 성명 (서명 또는 인)

[요양기관명]장 귀중

2.3.1

영상정보처리기기(CCTV) 운영·관리 방침(예시)

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

1. 영상정보처리기기의 설치 근거 및 설치 목적

본 사는 개인정보보호법 제25조 제1항에 따라 다음과 같은 목적으로 영상정보처리기기를 설치·운영 합니다.

- 시설안전 및 화재 예방

- 고객의 안전을 위한 범죄 예방

(주차장에 설치하는 경우)

- 차량도난 및 파손방지

※ 주차대수 30대를 초과하는 규모의 경우 「주차장법 시행규칙」 제6조제1항을 근거로 설치·운영 가능

2. 설치 대수, 설치 위치 및 촬영범위

설치 대수	설치 위치 및 촬영 범위
00대	*건물로비, 주차장 입구*

3. 관리책임자 및 접근권한자

귀하의 영상정보를 보호하고 개인영상정보와 관련한 불만을 처리하기 위하여 아래와 같이 개인영상정보 보호책임자를 두고 있습니다.

구분	성명	직위	소속	연락처
관리책임자	*홍길동*	*과장*	*0000과*	*00-0000-0000*
접근권한자				

4. 영상정보의 촬영시간, 보관기간, 보관장소 및 처리방법

촬영시간	보관기간	보관장소
24시간	*촬영일로부터 30일*	*000실 (보관시설 명)*

- 처리방법: 개인영상정보의 목적 외 이용, 제3자 제공, 파기, 열람 등 요구에 관한 사항을 기록·관리하고, 보관기간 만료 시 복원이 불가능한 방법으로 영구 삭제(출력물의 경우 파쇄 또는 소각)합니다.

5. 영상정보처리기기 설치 및 관리 등의 위탁에 관한 사항 *(해당하는 경우만)*

본 사는 아래와 같이 영상정보처리기기 설치 및 관리 등을 위탁하고 있으며, 관계 법령에 따라 위탁계약 시 개인정보가 안전하게 관리될 수 있도록 필요한 사항을 규정하고 있습니다.

수탁업체	담당자	연락처
OO시스템	*홍길동*	*00-000-0000*

6. 개인영상정보의 확인 방법 및 장소에 관한 사항

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

- 확인 장소: OO부서 OO팀

7. 정보주체의 영상정보 열람 등 요구에 대한 조치

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

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

8. 영상정보의 안전성 확보조치

본 사는 처리하는 영상정보는 암호화 조치 등을 통하여 안전하게 관리되고 있습니다. 또한 본 사는 개인영상정보보호를 위한 관리적 대책으로서 개인정보에 대한 접근 권한을 차등부여하고 있고, 개인영상정보의 위·변조 방지를 위하여 개인영상정보의 생성 일시, 열람 시 열람 목적·열람자·열람 일시 등을 기록하여 관리하고 있습니다.

이 외에도 개인영상정보의 안전한 물리적 보관을 위하여 잠금장치를 설치하고 있습니다.

9. 영상정보처리기기 운영·관리방침 변경에 관한 사항

이 영상정보처리기기 운영·관리방침은 2012년 O월 OO일에 제정되었으며 법령·정책 또는 보안기술의 변경에 따라 내용의 추가·삭제 및 수정이 있을 시에는 시행하기 최소 7일전에 본 사 홈페이지를 통해 변경사유 및 내용 등을 공지하도록 하겠습니다.

- 공고일자: 2000년 O월 OO일 / 시행일자: 2000년 O월 OO일

안내판 및 홈페이지 게재 내용 예시

2.3.2

CCTV 설치 안내

◈ 설치 목적: *범죄예방 및 시설안전*

◈ 설치 장소: *출입구의 벽면/천장,*
엘리베이터/각층의 천장

◈ 촬영 범위: *출입구, 엘리베이터 및 각층 복도(360°회전)*

◈ 촬영 시간: *24시간 연속 촬영*

◈ 관리책임자: *OO과 홍길동 (00-000-0000)*

(설치·운영을 위탁한 경우)

◈ 위탁관리자: *OO업체 박길동 (00-000-0000)*

※ 안내판에 CCTV 그림을 표시하여 정보주체가 쉽게 인식할 수 있도록 하는 것이 바람직함

2.3.3

개인영상정보 관리대장

번호	구분	일시	파일명 /형태	담당자/	목적/ 사유	이용·제공받는 제3자 /열람 등 요구자	이용·제공·열람 거부 시 구체적 사유	사본 제공 사유
1	□ 이용 □ 제공 □ 열람 □ 파기							
2	□ 이용 □ 제공 □ 열람 □ 파기							
3	□ 이용 □ 제공 □ 열람 □ 파기							
4	□ 이용 □ 제공 □ 열람 □ 파기							
5	□ 이용 □ 제공 □ 열람 □ 파기							
6	□ 이용 □ 제공 □ 열람 □ 파기							

2.4.1

※ 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

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

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

제2조 (용어의 정의) 본 계약에서 별도로 정의되지 아니한 용어는「개인정보 보호법」, 같은 법 시행령 및 고시,「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2021-2호) 및「표준 개인정보 보호지침」(개인정보보호위원회 고시 제2020-1호)에서 정의된 바에 따른다.

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

1. 개인정보의 암호화 *2. 프로그램의 유지보수*

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

계약 기간 : 년 월 일 ~ 년 월 일

제5조 (재위탁 제한) ① "수탁자"는 "위탁자"의 사전 승낙을 얻은 경우를 제외하고 "위탁자"와의 계약상의 권리와 의무의 전부 또는 일부를 제3자에게 양도하거나 재위탁할 수 없다.

② "수탁자"가 다른 제3의 회사와 수탁계약을 할 경우에는 "수탁자"는 해당 사실을 계약 체결 7일 이전에 "위탁자"에게 통보하고 협의하여야 한다.

1) 각호의 업무 예시: 고객만족도 조사 업무, 회원가입 및 운영 업무, 사은품 배송을 위한 이름, 주소, 연락처 처리 등

제6조 (개인정보의 안전성 확보조치) "수탁자"는「개인정보 보호법」제23조제2항 및 제24조제3항 및 제29조, 같은 법 시행령 제21조 및 제30조, 「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2021-2호)에 따라 개인정보의 안전성 확보에 필요한 관리적·기술적 조치를 취하여야 한다.

제7조 (개인정보의 처리제한) ① "수탁자"는 계약기간은 물론 계약 종료 후에도 위탁업무 수행 목적 범위를 넘어 개인정보를 이용하거나 이를 제3자에게 제공 또는 누설하여서는 안 된다.

② "수탁자"는 계약이 해지되거나 또는 계약기간이 만료된 경우 위탁업무와 관련하여 보유하고 있는 개인정보를 「개인정보 보호법」시행령 제16조 및「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2021-2호)에 따라 즉시 파기하거나 "위탁자"에게 반납하여야 한다.

③ 제2항에 따라 "수탁자"가 개인정보를 파기한 경우 지체없이 "위탁자"에게 그 결과를 통보하여야 한다.

제8조 (수탁자에 대한 관리·감독 등) ① "위탁자"는 "수탁자"에 대하여 다음 각 호의 사항을 감독할 수 있으며, "수탁자"는 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 "위탁자"는 "수탁자"에 대하여 제1항 각 호의 사항에 대한 실태를 점검하여 시정을 요구할 수 있으며, "수탁자"는 특별한 사유가 없는 한 이행하여야 한다.

③ "위탁자"는 처리위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 1년에 *( )회* "수탁자"를 교육할 수 있으며, "수탁자"는 이에 응하여야 한다.[2)]

④ 제1항에 따른 교육의 시기와 방법 등에 대해서는 "위탁자"는 "수탁자"와 협의하여 시행한다.

제9조 (정보주체 권리보장) ① "수탁자"는 정보주체의 개인정보 열람, 정정·삭제, 처리정지 요청 등에 대응하기 위한 연락처 등 민원 창구를 마련해야 한다.

제10조 (개인정보의 파기) ① "수탁자"는 제4조의 위탁업무기간이 종료되면 특별한 사유가 없는 한 지체 없이 개인정보를 파기하고 이를 "위탁자"에게 확인받아야 한다.

---

2)「개인정보 안전성 확보조치 기준 고시」(개인정보보호위원회 고시 제2021-2호) 및「개인정보 보호법」제26조에 따라 개인정보처리자 및 취급자는 개인정보보호에 관한 교육을 의무적으로 시행하여야 한다.

제11조 (손해배상) ① “수탁자” 또는 “수탁자”의 임직원 기타 “수탁자”의 수탁자가 이 계약에 의하여 위탁 또는 재위탁 받은 업무를 수행함에 있어 이 계약에 따른 의무를 위반하거나 “수탁자” 또는 “수탁자”의 임직원 기타 “수탁자”의 수탁자의 귀책사유로 인하여 이 계약이 해지되어 “위탁자” 또는 개인정보주체 기타 제3자에게 손해가 발생한 경우 “수탁자”는 그 손해를 배상하여야 한다.

② 제1항과 관련하여 개인정보주체 기타 제3자에게 발생한 손해에 대하여 “위탁자”가 전부 또는 일부를 배상한 때에는 “위탁자”는 이를 “수탁자”에게 구상할 수 있다.

본 계약의 내용을 증명하기 위하여 계약서 2부를 작성하고, “위탁자”와 “수탁자”가 서명 또는 날인한 후 각 1부씩 보관한다.

20 . . .

위탁자
주 소 :
기관(회사)명 :
대표자 성명 : (인)

수탁자
주 소 :
기관(회사)명 :
대표자 성명 : (인)

2.4.2

수탁업체 개인정보보호 실태 점검표

○ 업 체 명: *○○정보기술*

○ 점검일자: *20XX년 XX월 XX일*

연번	점검항목	점검결과		해당 없음	비고
		예	아니오		
1	*개인정보 목적 외 이용제공 여부*				
2	*재위탁 여부*				
3	*안전성 확보조치 여부*				

※『개인정보의 안전성 확보조치 기준』제26조 참조

※ 위탁업무내용에 따라 점검항목 조정 가능함

2.5.1

보안 서약서(예시)

□ 성　명:
□ 소　속:
□ 직　책:

본인은 *OOO* 업무 중에 알게 된 환자의 개인정보에 대하여 업무 수행 중이나 업무 수행 후에도 비밀을 지킬 것을 서약합니다.

또한 환자의 개인정보의 보호를 위해 *OOO*에서 정하는 개인정보 처리방침 또는 내부관리계획을 준수할 것이며, 적법한 절차 없이 환자의 개인정보를 무단으로 조회하거나 유출하지 않을 것을 서약합니다.

본인은 개인정보 보호책임자로부터 개인정보 처리 및 보호의 법적 근거가 되는「개인정보보호법」관련 규정을 충분히 설명을 듣고 숙지하였습니다.

만약, 이러한 서약에도 불구하고 업무상 알게 된 사항에 대하여 비밀을 누설하거나 정당한 사유 없이 조회, 유출, 오용할 경우 민·형사상 처벌은 물론 징계처분을 받을 수 있음을 통고 받았으며, 이러한 제재에 대하여 이의를 제기하지 않을 것을 본인의 자의로 서약합니다.

년　　월　　일

성 명:　　(인)

2.5.1

비밀유지 서약서(예시)

소 속 :
직 명 :
성 명 :

위 본인은 재직 중 직무상 지득한 모든 비밀을 퇴직 후에도 절대로 누설하지 않을 것이며 공무상 비밀을 누설하였을 경우에는 형사상의 처벌 등 어떠한 경우에도 이의를 제기하지 않겠음

20 년 월 일

성 명 (인)

○○○ 의원 원장 ○○○ 귀하

2.5.2

개인정보보호 교육 서명록

○ 교육일자:
○ 교육장소:
○ 교육내용(예시)
- *정보보호 및 개인정보보호의 기본 개요, 관리체계 구축 및 방법, 관련 법률*
- *정보보호 및 개인정보보호 관련 내부규정, 관리적·기술적·물리적 조치사항*
- *중요정보 및 개인정보 침해(유출)사고 사례 및 대응방안, 규정 위반 시 법적 책임 등*

연번	부서명	직급	성명	서명
1	*○○과*	*과장*	*○○○*	*○○○*
2	*○○과*	*대리*	*○○○*	*○○○*

개인정보보호 교육 수료증 예시

3.1.1

개인정보 내부관리 계획

제1장 총칙

제1조(목적)

개인정보보호 내부관리계획은 개인정보보호법 제29조(안전조치의무) 내부관리계획의 수립 및 시행 의무에 따라 제정된 것으로 *[요양기관명]*에 근무하는 직원들이 취급하는 개인정보를 체계적으로 관리하여 개인정보가 분실, 도난, 누출, 변조, 훼손, 오·남용 등이 되지 아니하도록 함을 목적으로 한다.

제2조(적용범위)

본 계획은 홈페이지 등의 온라인을 통하여 수집, 이용, 제공 또는 관리되는 개인정보뿐만 아니라 오프라인(*인적사항신청서, 챠트, 진료사진, 전화, 팩스 등*)을 통해 수집, 이용, 제공 또는 관리되는 개인정보에 대해서도 적용되며, 이러한 개인정보를 취급하는 내부 직원 및 외부업체 직원에 대해 적용된다.

제3조(용어 정의)

1. “개인정보”란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.
2. “처리”란 개인정보의 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.
3. “정보주체”란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
4. “개인정보처리자”란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
5. “개인정보 보호책임자”란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지는 자로서, 「개인정보 보호법 시행령」 제32조(개인정보 보호책임자의 업무 및 지정요건 등)제2항에 해당하는 자를 말한다.
6. “개인정보취급자”란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을 말한다.
7. “개인정보처리시스템”이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한

데이터베이스시스템을 말한다.

8. “위험도 분석”이란 개인정보 유출에 영향을 미칠 수 있는 다양한 위험요소를 식별·평가하고 해당 위험요소를 적절하게 통제할 수 있는 방안 마련을 위한 종합적으로 분석하는 행위를 말한다.
9. "비밀번호"라 함은 이용자 및 개인정보취급자 등이 시스템 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 말한다.
10. "접속기록"이라 함은 이용자 또는 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 식별자, 접속일시, 접속지를 알 수 있는 정보, 수행업무 등 접속한 사실을 전자적으로 기록한 것을 말한다.
11. "생체정보"라 함은 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 인증·식별하거나 개인에 관한 특징을 알아보기 위해 일정한 기술적 수단을 통해 처리되는 정보를 말한다.
12. "생체인식정보"라 함은 생체정보 중 특정 개인을 인증 또는 식별할 목적으로 일정한 기술적 수단을 통해 처리되는 정보를 말한다.
13. "P2P(Peer to Peer)"라 함은 정보통신망을 통해 서버의 도움 없이 개인과 개인이 직접 연결되어 파일을 공유하는 것을 말한다.
14. "공유설정"이라 함은 컴퓨터 소유자의 파일을 타인이 조회·변경·복사 등을 할 수 있도록 설정하는 것을 말한다.
15. "보안서버"라 함은 정보통신망에서 송·수신하는 정보를 암호화하여 전송하는 웹서버를 말한다.
16. "인증정보"라 함은 개인정보처리시스템 또는 정보통신망을 관리하는 시스템 등이 요구한 식별자의 신원을 검증하는데 사용되는 정보를 말한다.
17. "모바일 기기"란 스마트폰, 태블릿PC 등 무선망을 이용할 수 있는 휴대용 기기를 말한다.
18. "보조저장매체"란 이동형 하드디스크(HDD), USB메모리, CD(Compact Disk) 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 쉽게 분리·접속할 수 있는 저장매체를 말한다.
19. “대기업”이란 「독점규제 및 공정거래에 관한 법률」 제14조에 따라 공정거래위원회가 지정한 기업집단을 말한다.
20. “중견기업”이란 「중견기업 성장촉진 및 경쟁력 강화에 관한 특별법」 제2조에 해당하는 기업을 말한다.
21. “중소기업”이란 「중소기업기본법」 제2조 및 동법 시행령 제3조에 해당하는 기업을 말한다.
22. “소상공인”이란 「소상공인 보호 및 지원에 관한 법률」 제2조에 해당하는 자를 말한다.

제2장(내부관리계획의 수립 및 시행)

제4조(내부관리계획의 수립 및 승인)

1. 개인정보 보호책임자는 *개인정보처리자명([요양기관명] 임직원 OOO)*이 개인정보보호와 관련한 법령 및 규정 등을 준수할 수 있도록 내부 의사결정 절차를 통하여 내부관리계획을 수립하여야 한다.
2. 개인정보 보호책임자는 내부관리계획의 각 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부 관리계획을 수정하여야 한다.
3. 개인정보 보호책임자는 내부관리계획을 수립하거나 수정하는 경우에는 *[최고경영층 OOO]*으로부터 내부결재 등의 승인을 받아야 하며, 그 이력을 보관·관리하여야 한다.
4. 개인정보처리자는 내부 관리계획의 세부 이행을 위한 각종 지침 등을 마련하여 시행할 수 있다.
5. 개인정보 보호책임자는 연 1회 이상으로 내부 관리계획의 이행 실태를 점검·관리 하고 그 결과에 따라 적절한 조치를 취하여야 한다.

제5조(내부관리계획의 공표)

1. 개인정보 보호책임자는 4조에 따라 승인한 내부관리계획을 *[요양기관명]* 전 임직원 및 관련자에게 알림으로써 이를 준수하도록 하여야 한다.
2. 내부관리계획은 임직원 등이 언제든지 열람할 수 있는 방법으로 비치하거나 제공하여야 하며, 변경사항이 있는 경우에는 이를 공지하여야 한다.

제3장 개인정보 보호책임자의 의무와 책임

제6조(개인정보 보호책임자의 지정)

1. *개인정보처리자명([요양기관명] 임직원 OOO)*다음 각 목의 어느 하나에 해당하는 자를 개인정보 보호책임자로 임명한다.(개인정보보호법 시행령 제32조제2항)

가. *[요양기관명]*의 사업주 또는 대표자 *[OOO]*

나. 임원(임원이 없는 경우 개인정보 처리 관련 업무를 담당하는 부서의 장 *[OOO]*

제7조(개인정보 보호책임자의 역할 및 책임)

1. 개인정보 보호책임자는 정보주체의 개인정보 보호를 위하여 다음 각 목의 업무를 수행한다.

가. 개인정보 보호 계획의 수립 및 시행

나. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선

다. 개인정보 처리와 관련한 불만의 처리 및 피해 구제

라. 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축

마. 개인정보 보호 교육 계획의 수립 및 시행
바. 개인정보파일의 보호 및 관리 감독
사. 법 제30조에 따른 개인정보 처리방침의 수립·변경 및 시행
아. 개인정보 보호 관련 자료의 관리
자. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기

2. 개인정보 보호책임자는 업무를 수행함에 있어서 필요한 경우 개인정보의 처리 현황, 처리 체계 등에 대하여 수시로 조사하거나 관계 당사자로부터 보고를 받을 수 있다.
3. 개인정보 보호책임자는 개인정보 보호와 관련하여 이 법 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 하며, 필요하면 *[요양기관명] 최고경영층*에게 개선조치를 보고하여야 한다.

제8조(개인정보취급자의 역할 및 책임)

1. 개인정보취급자는 *개인정보처리자명([요양기관명] 임직원 OOO)*의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을 말한다.
2. 개인정보취급자는 개인정보를 처리함에 있어서 개인정보가 안전하게 관리될 수 있도록 동 계획은 물론, 개인정보 보호와 관련한 법령 및 규정 등을 준수하여야 한다.

제4장 개인정보보호 교육

제9조(개인정보취급자의 교육)

1. 개인정보 보호책임자는 다음 각 호의 사항을 포함하는 연간 개인정보보호 교육계획을 수립하고 실시하여야 한다.
   가. 교육목적 및 대상: *[전 직원을 대상으로 개인정보보호 교육]*
   나. 교육내용: *[개인정보보호 동영상교육 이수 등]*
   다. 교육 일정 및 방법: *[정기 또는 수시, 온라인, 오프라인(연수과정 등) 교육 이수]*
2. 개인정보 보호책임자는 정보주체정보보호에 대한 직원들의 인식제고를 위해 노력해야 하며, 개인정보의 오·남용 또는 유출 등을 적극 예방하기 위해 임·직원을 대상으로 매년 정기적으로 *연1회 이상*의 개인정보보호 교육을 실시한다.
3. 교육 방법은 집체 교육뿐만 아니라, 인터넷 교육, 그룹웨어 교육 등 다양한 방법을 활용하여 실시하고, 필요한 경우 외부 전문기관이나 전문요원에 위탁하여 교육을 실시한다.
4. 개인정보보호에 대한 중요한 전파 사례가 있거나 개인정보보호 업무와 관련하여 변경된 사항이 있는 경우, 개인정보 보호책임자는 *직원 회의* 등을 통해 수시 교육을 실시할 수 있다.
5. 개인정보 보호책임자는 제4장에 따라 개인정보 보호 교육을 실시한 결과 또는 이를 입증할 수 있는 관련 자료 등을 기록·보관하여야 한다.

제5장 개인정보의 기술적 · 관리적 보호조치

제10조(개인정보취급자 접근권한 관리 및 인증)

1. *개인정보처리자명([요양기관명] 임직원 OOO)*은 개인정보처리시스템(청구 S/W)에 대한 접근권한을 업무수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.
2. 개인정보처리자는 휴직 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여야 하며, 또한 비밀유지의무 등에 대한 보안서약서를 받아야 한다.
3. *개인정보처리자명([요양기관명] 임직원 OOO)*은 1, 2에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.
4. *개인정보처리자명([요양기관명] 임직원 OOO)*은 개인정보처리시스템에 접속할 수 있는 사용자 계정을 발급하는 경우, 개인정보취급자 별로 한 개의 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.
5. *개인정보처리자명([요양기관명] 임직원 OOO)*은 개인정보처리시스템(청구S/W), 접근통제시스템, 인터넷 홈페이지 등에 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 다음의 사항을 적용하여야 한다.
   ① 문자, 숫자의 조합·구성에 따라 최소 8자리 또는 10자리 이상의 길이로 구성
   - 최소 8자리 이상 : 두 종류 이상의 문자를 이용하여 구성한 경우
     ※ 문자 종류 : 알파벳 대문자와 소문자, 특수문자, 숫자
   - 최소 10자리 이상 : 하나의 문자종류로 구성한 경우
     ※ 단, 숫자로만 구성할 경우 취약할 수 있음

   ② 비밀번호는 추측하거나 유추하기 어렵도록 설정
   - 동일한 문자 반복(aaabbb, 123123 등), 키보드 상에서 나란히 있는 문자열(qwer 등), 일련번호(12345678 등), 가족이름, 생일, 전화번호 등은 사용하지 않음

   ③ 비밀번호가 제3자에게 노출되었을 경우 지체 없이 새로운 비밀번호로 변경해야 함
6. *개인정보처리자명([요양기관명] 임직원 OOO)*은 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.

제11조(접근통제)

1. 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 시스템을 설치·운영하여야 한다.
   가. 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol)주소 등으로 제한하여 인가받지 않은 접근을 제한 *[백신 및 윈도우 방화벽을 이용하여 접근통제 설정]*

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

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

제12조(개인정보의 암호화)

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

제13조(접속기록의 위·변조 방지)

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

제14조(보안프로그램 설치 및 운영)

1. 개인정보처리자는 개인정보처리시스템 또는 업무용 컴퓨터에 악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 한다.
2. 보안 프로그램의 자동 업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 적용하여야 한다.
3. 악성 프로그램관련 경보가 발령된 경우 또는 사용 중인 응용프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 적용하여야 한다.

제15조(물리적 접근제한 및 접근통제 방법)

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

제6장 개인정보 침해대응 및 피해구제

제16조(개인정보 유출사고 대응)

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

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

제17조(권익침해 구제방법)

1. 개인정보주체는 개인정보침해로 인한 구제를 받기 위하여 개인정보분쟁조정위원회, 한국인터넷진흥원 개인정보침해신고센터 등에 분쟁해결이나 상담 등을 신청한다. 이 밖에 기타 개인정보침해의 신고 및 상담에 대하여는 아래의 기관에 문의한다.

가. 개인정보 침해신고센터: (국번없이) 118 privacy.kisa.or.kr

나. 대검찰청 사이버범죄수사단: (국번없이) 1301 privacy@spo.go.kr(www.spo.go.kr)

다. 경찰청 사이버테러대응센터: (국번없이) 182 cyberbureau.police.go.kr

라. 개인분쟁조정위원회: 1833-6972 www.kopico.go.kr

3.2.1
3.2.2

사용자 ID 관리대장

연번	처리일시	사용자 ID	소속	직급	성명	접근권한	유형	사유	처리자ID (성명)
1	*20XX.XX.XX 00:00*	*ABCD*	*○○과*	*과장*	*○○○*	*건강보험 청구업무*	*부여*	*입사*	*○○○○ (○○○)*
2	*20XX.XX.XX 00:00*	*ABCD*	*○○과*	*과장*	*○○○*	*접수업무*	*변경*	*부서 변경*	*○○○○ (○○○)*
3	*20XX.XX.XX 00:00*	*ABCD*	*○○과*	*과장*	*○○○*	*접수업무*	*말소*	*퇴사*	*○○○○ (○○○)*

※ 개인정보처리시스템에 ID별 권한 부여·변경 기능이 없는 경우 본 서식을 사용할 수 있음
※ 위의 서식을 참고하여 요양기관의 환경에 맞게 수정하여 사용

출입통제 절차 수립 예시

3.6.1

방문자 신분확인

⬇

출입관리대장 작성
(방문자명 및 소속, 입실시간, 방문목적)

⬇

담당직원 동행 입실

⬇

출입관리대장 작성
(퇴실시간)

⬇

업무종료 후 잠금 확인

3.6.1

출 입 관 리 대 장

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

개인정보 처리방침 예시(의료기관) 3.7.1

【 개인정보 처리방침 】

OO의료기관(**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 알려드리기 위하여 다음과 같이 개인정보 처리방침을 수립·공개합니다.

[주요 개인정보 처리 표시(라벨링)]

 개인정보	*성명, 주민등록번호, 연락처, 주소 등*	 개인정보 처리목적	*의료법에 근거한 진료행위 등*
 개인정보 처리위탁	*위탁기관: **A** 수탁기관 (위탁수행): **AAA, BBB, CCC, DDD***	 고충 처리 안내	*담당자: **홍길동** 연락처: **<전화번호>***

개인정보 처리방침의 순서는 다음과 같습니다.

1. 개인정보의 처리목적, 수집항목, 보유 및 이용기간
2. 개인정보의 제 3자 제공
3. 개인정보의 보유 및 이용기간 및 파기절차 및 파기방법
4. 이용자 및 법정대리인의 권리와 그 행사방법
5. 개인정보 처리의 위탁
6. 개인정보 보호책임자 및 열람청구
7. 권익침해 구제방법
8. 개인정보의 안전성 확보조치
9. 추가적인 이용·제공 판단 기준
10. 개인정보 자동 수집 장치의 설치·운영 및 거부에 관한 사항
11. 행태정보의 수집·이용 및 거부 등에 관한 사항
12. 정책 변경에 따른 공지의무

1. 개인정보의 처리목적, 수집항목, 보유 및 이용기간(해당되는 부분만 작성)

처리목적	수집항목	보유 및 이용기간
진료서비스 제공 및 환자 명부 관리	*(필수) 주소, 성명, 주민등록번호, 전화번호*	*5년 (의료법 시행규칙 제15조)*
진료기록부 관리	*(필수) 주소, 성명 연락처, 주민등록번호, 병력 및 가족력, 주된 증상, 진단 결과 또는 진단명, 진료 경과, 치료내용, 진료일시*	*10년 (의료법 시행규칙 제15조)*
진료 예약 등 서비스 제공	*(필수) 성명, 주민등록번호, 휴대폰번호*	*의료법 시행규칙 제15조에 준하여 관리*
진료비 수납 등 원무서비스	*(필수) 카드사명, 카드번호 등 결제 승인정보*	*의료법 시행규칙 제15조에 준하여 관리*
홈페이지 회원가입 (홈페이지가 있는 경우)	*(필수) 성명, 생년월일, ID, 비밀번호, 이메일 주소, 만 14세 미만 아동의 경우 법정대리인 정보(성명, 생년월일, 성별, 휴대전화번호)* *(선택) 자택전화번호*	*회원 탈퇴 시까지*

수집하는 개인정보는 「의료법」, 「국민건강보험법」에 따른 *업무(진료정보의 보관 등)* 및 건강보험급여의 청구에만 사용하며 이용 목적이 변경될 시에는 사전 동의를 구할 것입니다.

2. 개인정보의 제3자 제공

*A*는 정보주체의 개인정보를 명시한 범위 내에서만 처리하며, 정보주체의 동의, 법률의 특별한 규정 등『개인정보 보호법』제17조 및 제18조에 해당하는 경우에만 개인정보를 제3자에게 제공하고 그 외에는 정보주체의 개인정보를 제3자에게 제공하지 않습니다.

*A*는 의료법 제21조 제3항 각 호에 해당하는 경우 환자에 관한 기록을 열람하게 하거나 사본을 내주는 등 내용을 확인할 수 있도록 하고 있습니다.

*A*는 응급의료에 관한 법류 제11조에 따라 응급환자를 다른 의료기관으로 이송할 경우 이송받는 의료기관에 진료에 필요한 의무기록을 제공할 수 있습니다.

*A*는 생명윤리 및 안전에 관한 법률 제18조에 따라 인간대상연구를 수행하는 경우 정보주체의 서면동의와 동법에 따른 기관위원회의 심의를 거쳐참여자의 개인정보를 제3자에게 제공할 수 있습니다.

*A*는 정보주체의 동의를 얻어 다음과 같이 개인정보를 제공할 수 있습니다.(해당되는 경우 작성)

제공받는 자	제공목적	제공항목	제공 근거 / 보유 및 이용기간
건강보험 심사평가원	*급여비용 심사·지급·대상여부 확인 및 적정성 평가*	*성명, 주민등록번호, 진단명, 진료내역 등*	*국민건강보험법 제 13조, 제43조, 제56조*
국민건강 보험공단	*건강보험 자격득실*	*성명, 주민등록번호, 국적, 체류자격(외국인), 연락처 등*	*국민건강보험법 제7조, 제8조, 제9조, 제10조 등*
<제3자명>	*<제공목적>*	*<제공항목>*	*<제공받는자의 법적 근거 / 보유 및 이용기간*

3. 개인정보의 보유 및 이용기간 및 파기절차 및 파기방법

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

정보주체로부터 동의받은 개인정보 보유기간이 경과하거나 처리목적이 달성되었음에도 불구하고 다른 법령에 따라 개인정보를 계속 보존하여야 하는 경우에는, 해당 개인정보를 별도의 데이터베이스(DB)로 옮기거나 보관장소를 달리하여 보존합니다.

또한 A는 폐업 또는 휴업 신고를 할 때에는 기록·보존하고 있는 진료기록부, 조산기록부, 간호기록 등 진료에 관한 기록을 관할 보건소장에게 이관합니다.

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

4. 이용자 및 법정대리인의 권리와 그 행사방법

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

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

또한 정보주체의 위임을 받은 자 등 대리인이 보건복지부령으로 정하는 요건을 갖추어 요청한 경우에도 기록 열람 등 정보주체의 권리를 행사할 수 있습니다.

5. 개인정보 처리의 위탁(해당하는 부분만 작성)

개인정보를 정보시스템을 통해 관리하기 위해 다음의 회사에 개인정보를 위탁하고 있습니다.

위탁받는 자(수탁자)	위탁업무	보유 및 이용기간
AAA	*청구프로그램 (업무 및 기록의 전산관리)*	*위탁계약 종료시까지*
BBB	*진료기록부 등 폐기*	*위탁계약 종료시까지*
CCC	*CCTV 프로그램*	*위탁계약 종료시까지*
DDD	*CT/팍스(파노라마) 프로그램*	*위탁계약 종료시까지*
EEE	*홈페이지 유지보수*	*위탁계약 종료시까지*
FFF	*기공소(치과의원만 해당)*	*위탁계약 종료시까지*
GGG	*혈액검사*	*위탁계약 종료시까지*
HHH	*PC 유지보수*	*위탁계약 종료시까지*

6. 개인정보 보호책임자 및 열람청구

정보주체는 *A*의 서비스를 이용하시면서 발생한 모든 개인정보보호 관련 문의, 불만처리, 피해구제 등에 관한 사항을 개인정보 보호책임자에게 문의할 수 있습니다. *A*는 정보주체의 문의에 대해 지체없이 답변 및 처리해드릴 것입니다.

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

정보주체는「개인정보 보호법」제35조에 따른 개인정보의 열람 청구를 아래의 부서에 할 수 있습니다. *A*는 정보주체의 개인정보 열람청구가 신속하게 처리되도록 노력하겠습니다.

부서명: *A*
담당자: *홍길동*
연락처: *<전화번호>, <이메일>, <팩스번호>*

정보주체는 *A*의 서비스를 이용하시면서 발생한 모든 개인정보보호 문의, 불만처리, 피해구제 등에 관한 사항을 개인정보 보호책임자 및 담당부서로 문의할 수 있습니다. *A*는 정보주체의 문의에 대해 지체없이 답변 및 처리해드릴 것입니다.

7. 권익침해 구제방법

정보주체는 개인정보침해로 인한 구제를 받기 위하여 개인정보분쟁조정위원회, 한국인터넷진흥원 개인정보침해신고센터 등에 분쟁해결이나 상담 등을 신청할 수 있습니다. 이 밖에 기타 개인정보침해의 신고, 상담에 대하여는 아래의 기관에 문의하시기 바랍니다.

1. 개인정보분쟁조정위원회: (국번없이) 1833-6972 (www.kopico.go.kr)
2. 개인정보침해신고센터: (국번없이) 118 (privacy.kisa.or.kr)
3. 대검찰청: (국번없이) 1301 (www.spo.go.kr)
4. 경찰청: (국번없이) 182 (ecrm.cyber.go.kr)

A는 정보주체의 개인정보자기결정권을 보장하고 개인정보침해로 인한 상담 및 피해 구제를 위해 노력하고 있으며, 신고나 상담이 필요한 경우 아래의 담당부서로 연락해 주시기 바랍니다.

담당자: *홍길동*
연락처: *<전화번호>, <이메일>, <팩스번호>*

「개인정보 보호법」 제35조(개인정보의 열람), 제36조(개인정보의 정정·삭제), 제37조(개인정보의 처리정지 등)의 규정에 의한 요구에 대 하여 공공기관의 장이 행한 처분 또는 부작위로 인하여 권리 또는 이익의 침해를 받은 자는 행정심판법에 정하는 바에 따라 행정심판을 청구할 수 있습니다.

1. 중앙행정심판위원회: (국번없이) 110 (www.simpan.go.kr)

8. 개인정보의 안전성 확보조치

A는 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 접근권한 관리, 접근통제시스템 설치, 보안프로그램 설치 및 갱신 등의 방법으로 안전하게 관리합니다.

9. 추가적인 이용·제공 판단 기준(해당되는 경우에만 작성)

*A*는 「개인정보 보호법」 제15조제3항 및 제17조제4항에 따라 「개인정보 보호법」 시행령 제14조의2에 따른 사항을 고려하여 정보주체의 동의 없이 개인정보를 추가적으로 이용·제공할 수 있습니다.

항목	이용·제공 목적	보유 및 이용기간
이름, 연락처, 주소	*조제약을 잘못 수령한 사실을 알리기 위한 연락*	*목적 달성 즉시 파기*

이에 따라 *A*는 정보주체의 동의 없이 추가적인 이용·제공을 하기 위해서 다음과 같은 사항을 고려하였습니다.

▶ 개인정보를 추가적으로 이용·제공하려는 목적이 당초 수집 목적과 관련성이 있는지 여부
▶ 개인정보를 수집한 정황 또는 처리 관행에 비추어 볼 때 추가적인 이용·제공에 대한 예측 가능성이 있는지 여부
▶ 개인정보의 추가적인 이용·제공이 정보주체의 이익을 부당하게 침해하는지 여부

10. 개인정보 자동 수집 장치의 설치·운영 및 거부에 관한 사항(홈페이지가 없는 경우 해당없음)

*A*는 이용자에게 개별적인 맞춤서비스를 제공하기 위해 이용 정보를 제공하고 수시로 불러오는 '쿠키(cookie)'를 사용합니다. 웹사이트를 운영하는데 이용되는 서버(http)가 이용자의 컴퓨터 브라우저에게 보내는 소량의 정보이며 이용자들의 PC 컴퓨터내의 하드디스크에 저장되기도 합니다.

가. 쿠키의 사용목적: 이용자가 방문한 각 서비스와 웹 사이트들에 대한 방문 및 이용형태, 인기 검색어, 보안접속 여부 등을 파악하여 이용자에게 최적화된 정보 제공을 위해 사용됩니다.
나. 쿠키의 설치·운영 및 거부: 웹브라우저 상단의 도구>인터넷 옵션>개인정보 메뉴의 옵션 설정을 통해 쿠키 저장을 거부 할 수 있습니다.
다. 쿠키 저장을 거부할 경우 맞춤형 서비스 이용에 어려움이 발생할 수 있습니다.

11. 행태정보의 수집·이용 및 거부 등에 관한 사항(홈페이지가 없는 경우 해당없음)

*A*는 서비스 이용과정에서 정보주체에게 최적화된 맞춤형 서비스 및 혜택, 온라인 맞춤형 광고 등을 제공하기 위하여 행태정보를 아래와 같이 행태정보를 수집·이용합니다.

수집하는 행태정보의 항목	행태정보 수집 방법	행태정보 수집 목적	보유·이용기간 및 이후 정보처리 방법
이용자의 웹사이트/앱 서비스 방문이력, 검색이력, 구매이력,	*이용자의 웹 사이트 및 앱 방문/실행 시 자동 수집*	*이용자의 관심, 성향에 기반한 개인 맞춤형 상품추천 서비스를 제공*	*수집일로부터 00일 후 파기*

*A*는 다음과 같이 온라인 맞춤형 광고 사업자가 행태정보를 수집·처리하도록 허용하고 있습니다.

- 행태정보를 수집 및 처리하려는 광고 사업자: ○○○
- 행태정보 수집 방법: 이용자가 당사 웹사이트를 방문하거나 앱을 실행할 때 자동 수집 및 전송
- 수집·처리되는 행태정보 항목: 이용자의 웹/앱 방문이력, 검색이력, 구매이력

- 보유·이용기간: 00일

*A*는 온라인 맞춤형 광고 등에 필요한 최소한의 행태정보만을 수집하며, 사상, 신념, 가족 및 친인척관계 학력·병력, 기타 사회활동 경력 등 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 민감한 행태정보를 수집하지 않습니다.

A는 만 14세 미만임을 알고 있는 아동이나 만14세 미만의 아동을 주 이용자로 하는 온라인 서비스로부터 맞춤형 광고 목적의 행태정보를 수집하지 않고, 만 14세 미만임을 알고 있는 아동에게는 맞춤형 광고를 제공하지 않습니다.

A는 모바일 앱에서 온라인 맞춤형 광고를 위하여 광고식별자를 수집·이용합니다. 정보주체는 모바일 단말기의 설정 변경을 통해 앱의 맞춤형 광고를 차단·허용할 수 있습니다.

▶ 스마트폰의 광고식별자 차단/허용

1. (안드로이드) ① 설정 → ② 개인정보보호 → ③ 광고 → ③광고 ID 재설정 또는 광고ID 삭제
2. (아이폰) ① 설정 → ② 개인정보보호 → ③ 추적 → ④ 앱이 추적을 요청하도록 허용 끔

※ 모바일 OS 버전에 따라 메뉴 및 방법이 다소 상이할 수 있습니다.

정보주체는 웹브라우저의 쿠키 설정 변경 등을 통해 온라인 맞춤형 광고를 일괄적으로 차단·허용할 수 있습니다. 다만, 쿠키 설정 변경은 웹사이트 자동로그인 등 일부 서비스의 이용에 영향을 미칠 수 있습니다.

12. 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.

이전의 개인정보 처리방침은 홈페이지 확인 또는 접수창구에 문의주시면 확인하실 수 있습니다.

- 20XX. X. X. ~ 20XX. X. X. 적용

- 20XX. X. X. ~ 20XX. X. X. 적용

개인정보 처리방침 예시(약국)

3.7.1

【 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 알려드리기 위하여 다음과 같이 개인정보 처리방침을 수립·공개합니다.

[주요 개인정보 처리 표시(라벨링)]

 개인정보	*(조제)* *성명, 주민등록 번호, 연락처 등* *(청구)* *성명, 주민등록 번호, 연락처 등*	 개인정보 처리목적	*의약품 조제, 처방전 관리 및 요양급여 청구*
 개인정보 처리위탁	*위탁기관:* ***A*** *수탁기관* *(위탁수행):* ***AAA, BBB, CCC, DDD***	 고충 처리 안내	*담당자: 홍길동* *연락처:* *<전화번호>*

개인정보 처리방침의 순서는 다음과 같습니다.

1. 개인정보의 처리목적, 수집항목, 보유 및 이용기간(해당되는 부분만 작성)

처리목적	수집항목	보유 및 이용기간
의약품 조제 및 처방전 관리	*(필수) 성명, 주민등록번호, 전화번호 의료기관 명칭, 질병분류기호, 의료인의 성명 및 면허종류, 처방의약품, 발급연원일, 사용기간*	*2년 (약사법 제 29조) ※보험급여청구 처방전은 3년간 보관*
조제기록부 관리 및 요양급여 청구	*(필수) 성명, 연락처, 주민등록번호, 질병명, 요양급여비용, 본인부담금 및 비용청구액, 처방전 내용 및 가입자 성명, 건강보험증 번호*	*5년 (약사법 제30조 1항)*
홈페이지 회원가입 (홈페이지가 있는 경우)	*(필수) 성명, 생년월일, ID, 비밀번호, 이메일 주소, 만 14세 미만 아동의 경우 법정대리인 정보(성명, 생년월일, 성별, 휴대전화번호) (선택) 자택전화번호*	*회원 탈퇴 시까지*

※ 수집하는 개인정보는 「의료법」, 「약사법」, 「국민건강보험법」에 따른 *업무(처방전의 보관 조제 정보의 보관 등)*, 건강보험급여의 청구에만 사용하며 이용 목적이 변경될 시에는 사전 동의를 구할 것입니다.

2. 개인정보의 제3자 제공(요양기관 환경에 맞게 가감하여 작성)

*A*는 정보주체의 개인정보를 명시한 범위 내에서만 처리하며, 정보주체의 동의, 법률의 특별한 규정 등『개인정보 보호법』제17조 및 제18조에 해당하는 경우에만 개인정보를 제3자에게 제공하고 그 외에는 정보주체의 개인정보를 제3자에게 제공하지 않습니다.

*A*는 약사법 제30조 제3항 각 호에 해당하는 경우 조제기록부를 열람하게 하거나 사본을 내주는 등 내용을 확인할 수 있도록 하고 있습니다.

*A*는 응급의료에 관한 법류 제11조에 따라 응급환자를 다른 의료기관으로 이송할 경우 이송받는 의료기관에 진료에 필요한 의무기록을 제공할 수 있습니다.

제공받는 자	제공목적	제공항목	제공 근거 / 보유 및 이용기간
건강보험 심사평가원	*요양급여비용의 청구*	*성명, 건강보험증 번호, 주민등록번호, 질병명, 요양급여비용의 내용, 본인부담금 및 비용청구액, 처방전 내용*	*국민건강보험법 제47조*
한국의약품 안전관리원	*부작용 등의 확인*	*성명, 성별, 생년월일, 체중, 신장, 임신기간, 월경일, 과거 병력 및 치료 정보, 부모정보, 사망정보*	*약사법 제68조의8*

3. 개인정보의 보유 및 이용기간 및 파기절차 및 파기방법

「약사법」, 「국민건강보험법」에서 정한 보유기간 동안 개인정보를 보유하며 개인정보가 불필요하게 되었을 때에는 지체 없이 개인정보를 파기합니다.

정보주체로부터 동의받은 개인정보 보유기간이 경과하거나 처리목적이 달성되었음에도 불구하고 다른 법령에 따라 개인정보를 계속 보존하여야 하는 경우에는, 해당 개인정보를 별도의 데이터베이스(DB)로 옮기거나 보관장소를 달리하여 보존합니다.

- 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.

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

또한 정보주체의 위임을 받은 자 등 대리인이 보건복지부령으로 정하는 요건을 갖추어 요청한 경우에도 기록 열람 등 정보주체의 권리를 행사할 수 있습니다.

5. 개인정보 처리의 위탁(요양기관 환경에 맞게 가감하여 작성)

개인정보를 정보시스템을 통해 관리하기 위해 다음의 회사에 개인정보를 위탁하고 있습니다.

위탁받는 자(수탁자)	위탁업무	보유 및 이용기간
AAA	*청구프로그램 (업무 및 기록의 전산관리)*	*위탁계약 종료시까지*
BBB	*조제기록부 등 폐기*	*위탁계약 종료시까지*
CCC	*CCTV 프로그램 및 내부 보안*	*위탁계약 종료시까지*
DDD	*홈페이지 유지보수*	*위탁계약 종료시까지*

6. 개인정보 보호책임자 및 열람청구

정보주체는 *A*의 서비스를 이용하시면서 발생한 모든 개인정보보호 관련 문의, 불만처리, 피해구제 등에 관한 사항을 개인정보 보호책임자에게 문의할 수 있습니다. *A*는 정보주체의 문의에 대해 지체없이 답변 및 처리해드릴 것입니다.

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

정보주체는 「개인정보 보호법」 제35조에 따른 개인정보의 열람 청구를 아래의 담당자에 할 수 있습니다. *A*는 정보주체의 개인정보 열람청구가 신속하게 처리되도록 노력하겠습니다.

담당자: *홍길동*

연락처: *<전화번호>, <이메일>, <팩스번호>*

7. 권익침해 구제방법

정보주체는 개인정보침해로 인한 구제를 받기 위하여 개인정보분쟁조정위원회, 한국인터넷진흥원 개인정보침해신고센터 등에 분쟁해결이나 상담 등을 신청할 수 있습니다. 이 밖에 기타 개인정보침해의 신고, 상담에 대하여는 아래의 기관에 문의하시기 바랍니다.

1. 개인정보분쟁조정위원회: (국번없이) 1833-6972 (www.kopico.go.kr)
2. 개인정보침해신고센터: (국번없이) 118 (privacy.kisa.or.kr)
3. 대검찰청: (국번없이) 1301 (www.spo.go.kr)
4. 경찰청: (국번없이) 182 (ecrm.cyber.go.kr)

*A*는 정보주체의 개인정보자기결정권을 보장하고 개인정보침해로 인한 상담 및 피해 구제를 위해 노력하고 있으며, 신고나 상담이 필요한 경우 아래의 담당부서로 연락해 주시기 바랍니다.

담당자: *홍길동*
연락처: *<전화번호>, <이메일>, <팩스번호>*

「개인정보 보호법」 제35조(개인정보의 열람), 제36조(개인정보의 정정·삭제), 제37조(개인정보의 처리정지 등)의 규정에 의한 요구에 대 하여 공공기관의 장이 행한 처분 또는 부작위로 인하여 권리 또는 이익의 침해를 받은 자는 행정심판법에 정하는 바에 따라 행정심판을 청구할 수 있습니다.

1. 중앙행정심판위원회: (국번없이) 110 (www.simpan.go.kr)

8. 개인정보의 안전성 확보조치

*A*는 이용자의 개인정보보호를 위한 기술적 대책으로서 여러 보안장치를 마련하고 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 접근권한 관리, 접근통제시스템 설치, 보안프로그램 설치 및 갱신 등의 방법으로 안전하게 관리합니다.

9. 추가적인 이용·제공 판단 기준

*A*는 「개인정보 보호법」 제15조제3항 및 제17조제4항에 따라 「개인정보 보호법」 시행령 제14조의2에 따른 사항을 고려하여 정보주체의 동의 없이 개인정보를 추가적으로 이용·제공할 수 있습니다.

항목	이용·제공 목적	보유 및 이용기간
이름, 연락처, 주소	*조제약을 잘못 수령한 사실을 알리기 위한 연락*	*목적 달성 즉시 파기*

이에 따라 *A*는 정보주체의 동의 없이 추가적인 이용·제공을 하기 위해서 다음과 같은 사항을 고려하였습니다.

- ▶ 개인정보를 추가적으로 이용·제공하려는 목적이 당초 수집 목적과 관련성이 있는지 여부
- ▶ 개인정보를 수집한 정황 또는 처리 관행에 비추어 볼 때 추가적인 이용·제공에 대한 예측 가능성이 있는지 여부
- ▶ 개인정보의 추가적인 이용·제공이 정보주체의 이익을 부당하게 침해하는지 여부

10. 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.

이전의 개인정보 처리방침은 홈페이지 확인 또는 접수창구에 문의주시면 확인하실 수 있습니다.

- 20XX. X. X. ~ 20XX. X. X. 적용
- 20XX. X. X. ~ 20XX. X. X. 적용

3.8.2

개인정보 정기점검 체크리스트

○ 점 검 자: _____

○ 점검일자: *20XX년 XX월 XX일(매월 1회 점검)*

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

[요양기관명] 개인정보 보호책임자: _____(인)

개인정보 유출시 필수 조치요령 | 3.9.1

개인정보 유출 사고 발생 시 이것만은 꼭 조치하세요!

1

유출된 정보주체 개개인에게 지체 없이 통지

⇨ **「개인정보 보호법」 제34조 제1항**

✓ 시 한: 유출되었음을 알게 되었을 경우 지체 없이(5일 이내)
✓ 통지 항목: ① 유출된 개인정보의 항목 ② 유출 시점과 및 그 경위
③ 피해 최소화를 위한 정보주체의 조치방법
④ 기관의 대응조치 및 피해구제 절차
⑤ 피해 신고 접수 담당부서 및 연락처

* 「개인정보 보호법」 제75조 제2항 제8호(**3천만원 이하의 과태료**)
정보주체에게 같은 항 각 호의 사항을 알리지 아니한 자

2

피해 최소화를 위한 대책 마련 및 필요한 조치 실시

⇨ **「개인정보 보호법」 제34조 제2항**

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

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

3

1천명 이상 유출된 경우 유출 통지 결과를 신고

⇨ **「개인정보 보호법」 제34조 제3항**

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

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

4

1천명 이상 유출된 경우에는 추가적으로 홈페이지에 공지

⇨ **「개인정보 보호법 시행령」 제40조 제3항**

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

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

표준 개인정보 보호지침 제28조(개인정보 유출신고 등) 별지 제1호 서식

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">유출신고접수기관</td><td>기관명</td><td>담당자명</td><td>연락처</td></tr>
<tr><td></td><td></td><td></td></tr>
</table>

관련 규정

개인정보보호법

표준 개인정보 보호지침

개인정보의 안전성 확보조치 기준

개인정보의 기술적 · 관리적 보호조치 기준

개인정보 보호법

[시행 2020. 8. 5.] [법률 제16930호, 2020. 2. 4., 일부개정]

제1장 총칙

제1조(목적) 이 법은 개인정보의 처리 및 보호에 관한 사항을 정함으로써 개인의 자유와 권리를 보호하고, 나아가 개인의 존엄과 가치를 구현함을 목적으로 한다. <개정 2014. 3. 24.>

제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. <개정 2014. 3. 24., 2020. 2. 4.>

1. “개인정보”란 살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다.
   가. 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보
   나. 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보. 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다.
   다. 가목 또는 나목을 제1호의2에 따라 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보(이하 “가명정보”라 한다)
1의2. “가명처리”란 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것을 말한다.
2. “처리”란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.
3. “정보주체”란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
4. “개인정보파일”이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.
5. “개인정보처리자”란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
6. “공공기관”이란 다음 각 목의 기관을 말한다.
   가. 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관, 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다) 및 그 소속 기관, 지방자치단체
   나. 그 밖의 국가기관 및 공공단체 중 대통령령으로 정하는 기관
7. “영상정보처리기기”란 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등

을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 대통령령으로 정하는 장치를 말한다.

8. “과학적 연구”란 기술의 개발과 실증, 기초연구, 응용연구 및 민간 투자 연구 등 과학적 방법을 적용하는 연구를 말한다.

제3조(개인정보 보호 원칙) ① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.

② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.

③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.

④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다.

⑤ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다.

⑥ 개인정보처리자는 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.

⑦ 개인정보처리자는 개인정보를 익명 또는 가명으로 처리하여도 개인정보 수집목적을 달성할 수 있는 경우 익명처리가 가능한 경우에는 익명에 의하여, 익명처리로 목적을 달성할 수 없는 경우에는 가명에 의하여 처리될 수 있도록 하여야 한다. <개정 2020. 2. 4.>

⑧ 개인정보처리자는 이 법 및 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.

제4조(정보주체의 권리) 정보주체는 자신의 개인정보 처리와 관련하여 다음 각 호의 권리를 가진다.

1. 개인정보의 처리에 관한 정보를 제공받을 권리
2. 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리
3. 개인정보의 처리 여부를 확인하고 개인정보에 대하여 열람(사본의 발급을 포함한다. 이하 같다)을 요구할 권리
4. 개인정보의 처리 정지, 정정·삭제 및 파기를 요구할 권리
5. 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리

제5조(국가 등의 책무) ① 국가와 지방자치단체는 개인정보의 목적 외 수집, 오용·남용 및 무분별한 감시·추적 등에 따른 폐해를 방지하여 인간의 존엄과 개인의 사생활 보호를 도모하기 위한 시책을 강구하여야 한다.

② 국가와 지방자치단체는 제4조에 따른 정보주체의 권리를 보호하기 위하여 법령의 개선 등 필요한 시책을 마련하여야 한다.

③ 국가와 지방자치단체는 개인정보의 처리에 관한 불합리한 사회적 관행을 개선하기 위하여 개인정보처리자의 자율적인 개인정보 보호활동을 존중하고 촉진·지원하여야 한다.
④ 국가와 지방자치단체는 개인정보의 처리에 관한 법령 또는 조례를 제정하거나 개정하는 경우에는 이 법의 목적에 부합되도록 하여야 한다.

제6조(다른 법률과의 관계) 개인정보 보호에 관하여는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따른다. <개정 2014. 3. 24.>

제2장 개인정보 보호정책의 수립 등

제7조(개인정보 보호위원회) ① 개인정보 보호에 관한 사무를 독립적으로 수행하기 위하여 국무총리 소속으로 개인정보 보호위원회(이하 "보호위원회"라 한다)를 둔다. <개정 2020. 2. 4.>
② 보호위원회는 「정부조직법」 제2조에 따른 중앙행정기관으로 본다. 다만, 다음 각 호의 사항에 대하여는 「정부조직법」 제18조를 적용하지 아니한다. <개정 2020. 2. 4.>
1. 제7조의8제3호 및 제4호의 사무
2. 제7조의9제1항의 심의·의결 사항 중 제1호에 해당하는 사항
③ 삭제 <2020. 2. 4.>
④ 삭제 <2020. 2. 4.>
⑤ 삭제 <2020. 2. 4.>
⑥ 삭제 <2020. 2. 4.>
⑦ 삭제 <2020. 2. 4.>
⑧ 삭제 <2020. 2. 4.>
⑨ 삭제 <2020. 2. 4.>

제7조의2(보호위원회의 구성 등) ① 보호위원회는 상임위원 2명(위원장 1명, 부위원장 1명)을 포함한 9명의 위원으로 구성한다.
② 보호위원회의 위원은 개인정보 보호에 관한 경력과 전문지식이 풍부한 다음 각 호의 사람 중에서 위원장과 부위원장은 국무총리의 제청으로, 그 외 위원 중 2명은 위원장의 제청으로, 2명은 대통령이 소속되거나 소속되었던 정당의 교섭단체 추천으로, 3명은 그 외의 교섭단체 추천으로 대통령이 임명 또는 위촉한다.
1. 개인정보 보호 업무를 담당하는 3급 이상 공무원(고위공무원단에 속하는 공무원을 포함한다)의 직에 있거나 있었던 사람
2. 판사·검사·변호사의 직에 10년 이상 있거나 있었던 사람
3. 공공기관 또는 단체(개인정보처리자로 구성된 단체를 포함한다)에 3년 이상 임원으로 재직하였거나 이들 기관 또는 단체로부터 추천받은 사람으로서 개인정보 보호 업무를 3년 이상 담당하였던 사람
4. 개인정보 관련 분야에 전문지식이 있고 「고등교육법」 제2조제1호에 따른 학교에서 부교수 이상으로 5년 이상 재직하고 있거나 재직하였던 사람

③ 위원장과 부위원장은 정무직 공무원으로 임명한다.

④ 위원장, 부위원장, 제7조의13에 따른 사무처의 장은 「정부조직법」 제10조에도 불구하고 정부위원이 된다.

[본조신설 2020. 2. 4.]

제7조의3(위원장) ① 위원장은 보호위원회를 대표하고, 보호위원회의 회의를 주재하며, 소관 사무를 총괄한다.

② 위원장이 부득이한 사유로 직무를 수행할 수 없을 때에는 부위원장이 그 직무를 대행하고, 위원장·부위원장이 모두 부득이한 사유로 직무를 수행할 수 없을 때에는 위원회가 미리 정하는 위원이 위원장의 직무를 대행한다.

③ 위원장은 국회에 출석하여 보호위원회의 소관 사무에 관하여 의견을 진술할 수 있으며, 국회에서 요구하면 출석하여 보고하거나 답변하여야 한다.

④ 위원장은 국무회의에 출석하여 발언할 수 있으며, 그 소관 사무에 관하여 국무총리에게 의안 제출을 건의할 수 있다.

[본조신설 2020. 2. 4.]

제7조의4(위원의 임기) ① 위원의 임기는 3년으로 하되, 한 차례만 연임할 수 있다.

② 위원이 궐위된 때에는 지체 없이 새로운 위원을 임명 또는 위촉하여야 한다. 이 경우 후임으로 임명 또는 위촉된 위원의 임기는 새로이 개시된다.

[본조신설 2020. 2. 4.]

제7조의5(위원의 신분보장) ① 위원은 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 그 의사에 반하여 면직 또는 해촉되지 아니한다.

1. 장기간 심신장애로 인하여 직무를 수행할 수 없게 된 경우
2. 제7조의7의 결격사유에 해당하는 경우
3. 이 법 또는 그 밖의 다른 법률에 따른 직무상의 의무를 위반한 경우

② 위원은 법률과 양심에 따라 독립적으로 직무를 수행한다.

[본조신설 2020. 2. 4.]

제7조의6(겸직금지 등) ① 위원은 재직 중 다음 각 호의 직(職)을 겸하거나 직무와 관련된 영리업무에 종사하여서는 아니 된다.

1. 국회의원 또는 지방의회의원
2. 국가공무원 또는 지방공무원
3. 그 밖에 대통령령으로 정하는 직

② 제1항에 따른 영리업무에 관한 사항은 대통령령으로 정한다.

③ 위원은 정치활동에 관여할 수 없다.

[본조신설 2020. 2. 4.]

제7조의7(결격사유) ① 다음 각 호의 어느 하나에 해당하는 사람은 위원이 될 수 없다.

1. 대한민국 국민이 아닌 사람

2. 「국가공무원법」 제33조 각 호의 어느 하나에 해당하는 사람
3. 「정당법」 제22조에 따른 당원

② 위원이 제1항 각 호의 어느 하나에 해당하게 된 때에는 그 직에서 당연 퇴직한다. 다만, 「국가공무원법」 제33조제2호는 파산선고를 받은 사람으로서 「채무자 회생 및 파산에 관한 법률」에 따라 신청기한 내에 면책신청을 하지 아니하였거나 면책불허가 결정 또는 면책 취소가 확정된 경우만 해당하고, 같은 법 제33조제5호는 「형법」 제129조부터 제132조까지, 「성폭력범죄의 처벌 등에 관한 특례법」 제2조, 「아동·청소년의 성보호에 관한 법률」 제2조제2호 및 직무와 관련하여 「형법」 제355조 또는 제356조에 규정된 죄를 범한 사람으로서 금고 이상의 형의 선고유예를 받은 경우만 해당한다.

[본조신설 2020. 2. 4.]

제7조의8(보호위원회의 소관 사무) 보호위원회는 다음 각 호의 소관 사무를 수행한다.

1. 개인정보의 보호와 관련된 법령의 개선에 관한 사항
2. 개인정보 보호와 관련된 정책·제도·계획 수립·집행에 관한 사항
3. 정보주체의 권리침해에 대한 조사 및 이에 따른 처분에 관한 사항
4. 개인정보의 처리와 관련한 고충처리·권리구제 및 개인정보에 관한 분쟁의 조정
5. 개인정보 보호를 위한 국제기구 및 외국의 개인정보 보호기구와의 교류·협력
6. 개인정보 보호에 관한 법령·정책·제도·실태 등의 조사·연구, 교육 및 홍보에 관한 사항
7. 개인정보 보호에 관한 기술개발의 지원·보급 및 전문인력의 양성에 관한 사항
8. 이 법 및 다른 법령에 따라 보호위원회의 사무로 규정된 사항

[본조신설 2020. 2. 4.]

제7조의9(보호위원회의 심의·의결 사항 등) ① 보호위원회는 다음 각 호의 사항을 심의·의결한다.

1. 제8조의2에 따른 개인정보 침해요인 평가에 관한 사항
2. 제9조에 따른 기본계획 및 제10조에 따른 시행계획에 관한 사항
3. 개인정보 보호와 관련된 정책, 제도 및 법령의 개선에 관한 사항
4. 개인정보의 처리에 관한 공공기관 간의 의견조정에 관한 사항
5. 개인정보 보호에 관한 법령의 해석·운용에 관한 사항
6. 제18조제2항제5호에 따른 개인정보의 이용·제공에 관한 사항
7. 제33조제3항에 따른 영향평가 결과에 관한 사항
8. 제28조의6, 제34조의2, 제39조의15에 따른 과징금 부과에 관한 사항
9. 제61조에 따른 의견제시 및 개선권고에 관한 사항
10. 제64조에 따른 시정조치 등에 관한 사항
11. 제65조에 따른 고발 및 징계권고에 관한 사항
12. 제66조에 따른 처리 결과의 공표에 관한 사항
13. 제75조에 따른 과태료 부과에 관한 사항

14. 소관 법령 및 보호위원회 규칙의 제정·개정 및 폐지에 관한 사항
15. 개인정보 보호와 관련하여 보호위원회의 위원장 또는 위원 2명 이상이 회의에 부치는 사항
16. 그 밖에 이 법 또는 다른 법령에 따라 보호위원회가 심의·의결하는 사항

② 보호위원회는 제1항 각 호의 사항을 심의·의결하기 위하여 필요한 경우 다음 각 호의 조치를 할 수 있다.

1. 관계 공무원, 개인정보 보호에 관한 전문 지식이 있는 사람이나 시민사회단체 및 관련 사업자로부터의 의견 청취
2. 관계 기관 등에 대한 자료제출이나 사실조회 요구

③ 제2항제2호에 따른 요구를 받은 관계 기관 등은 특별한 사정이 없으면 이에 따라야 한다.

④ 보호위원회는 제1항제3호의 사항을 심의·의결한 경우에는 관계 기관에 그 개선을 권고할 수 있다.

⑤ 보호위원회는 제4항에 따른 권고 내용의 이행 여부를 점검할 수 있다.

[본조신설 2020. 2. 4.]

제7조의10(회의) ① 보호위원회의 회의는 위원장이 필요하다고 인정하거나 재적위원 4분의 1 이상의 요구가 있는 경우에 위원장이 소집한다.

② 위원장 또는 2명 이상의 위원은 보호위원회에 의안을 제의할 수 있다.

③ 보호위원회의 회의는 재적위원 과반수의 출석으로 개의하고, 출석위원 과반수의 찬성으로 의결한다.

[본조신설 2020. 2. 4.]

제7조의11(위원의 제척·기피·회피) ① 위원은 다음 각 호의 어느 하나에 해당하는 경우에는 심의·의결에서 제척된다.

1. 위원 또는 그 배우자나 배우자였던 자가 해당 사안의 당사자가 되거나 그 사건에 관하여 공동의 권리자 또는 의무자의 관계에 있는 경우
2. 위원이 해당 사안의 당사자와 친족이거나 친족이었던 경우
3. 위원이 해당 사안에 관하여 증언, 감정, 법률자문을 한 경우
4. 위원이 해당 사안에 관하여 당사자의 대리인으로서 관여하거나 관여하였던 경우
5. 위원이나 위원이 속한 공공기관·법인 또는 단체 등이 조언 등 지원을 하고 있는 자와 이해관계가 있는 경우

② 위원에게 심의·의결의 공정을 기대하기 어려운 사정이 있는 경우 당사자는 기피 신청을 할 수 있고, 보호위원회는 의결로 이를 결정한다.

③ 위원이 제1항 또는 제2항의 사유가 있는 경우에는 해당 사안에 대하여 회피할 수 있다.

[본조신설 2020. 2. 4.]

제7조의12(소위원회) ① 보호위원회는 효율적인 업무 수행을 위하여 개인정보 침해 정도가

경미하거나 유사·반복되는 사항 등을 심의·의결할 소위원회를 둘 수 있다.
② 소위원회는 3명의 위원으로 구성한다.
③ 소위원회가 제1항에 따라 심의·의결한 것은 보호위원회가 심의·의결한 것으로 본다.
④ 소위원회의 회의는 구성위원 전원의 출석과 출석위원 전원의 찬성으로 의결한다.
[본조신설 2020. 2. 4.]

제7조의13(사무처) 보호위원회의 사무를 처리하기 위하여 보호위원회에 사무처를 두며, 이 법에 규정된 것 외에 보호위원회의 조직에 관한 사항은 대통령령으로 정한다.
[본조신설 2020. 2. 4.]

제7조의14(운영 등) 이 법과 다른 법령에 규정된 것 외에 보호위원회의 운영 등에 필요한 사항은 보호위원회의 규칙으로 정한다.
[본조신설 2020. 2. 4.]

제8조 삭제 <2020. 2. 4.>

제8조의2(개인정보 침해요인 평가) ① 중앙행정기관의 장은 소관 법령의 제정 또는 개정을 통하여 개인정보 처리를 수반하는 정책이나 제도를 도입·변경하는 경우에는 보호위원회에 개인정보 침해요인 평가를 요청하여야 한다.
② 보호위원회가 제1항에 따른 요청을 받은 때에는 해당 법령의 개인정보 침해요인을 분석·검토하여 그 법령의 소관기관의 장에게 그 개선을 위하여 필요한 사항을 권고할 수 있다.
③ 제1항에 따른 개인정보 침해요인 평가의 절차와 방법에 관하여 필요한 사항은 대통령령으로 정한다.
[본조신설 2015. 7. 24.]

제9조(기본계획) ① 보호위원회는 개인정보의 보호와 정보주체의 권익 보장을 위하여 3년마다 개인정보 보호 기본계획(이하 “기본계획”이라 한다)을 관계 중앙행정기관의 장과 협의하여 수립한다. <개정 2013. 3. 23., 2014. 11. 19., 2015. 7. 24.>
② 기본계획에는 다음 각 호의 사항이 포함되어야 한다.
1. 개인정보 보호의 기본목표와 추진방향
2. 개인정보 보호와 관련된 제도 및 법령의 개선
3. 개인정보 침해 방지를 위한 대책
4. 개인정보 보호 자율규제의 활성화
5. 개인정보 보호 교육·홍보의 활성화
6. 개인정보 보호를 위한 전문인력의 양성
7. 그 밖에 개인정보 보호를 위하여 필요한 사항
③ 국회, 법원, 헌법재판소, 중앙선거관리위원회는 해당 기관(그 소속 기관을 포함한다)의 개인정보 보호를 위한 기본계획을 수립·시행할 수 있다.

제10조(시행계획) ① 중앙행정기관의 장은 기본계획에 따라 매년 개인정보 보호를 위한 시행

계획을 작성하여 보호위원회에 제출하고, 보호위원회의 심의·의결을 거쳐 시행하여야 한다.

② 시행계획의 수립·시행에 필요한 사항은 대통령령으로 정한다.

제11조(자료제출 요구 등) ① 보호위원회는 기본계획을 효율적으로 수립하기 위하여 개인정보처리자, 관계 중앙행정기관의 장, 지방자치단체의 장 및 관계 기관·단체 등에 개인정보처리자의 법규 준수 현황과 개인정보 관리 실태 등에 관한 자료의 제출이나 의견의 진술 등을 요구할 수 있다. <개정 2013. 3. 23., 2014. 11. 19., 2015. 7. 24.>

② 보호위원회는 개인정보 보호 정책 추진, 성과평가 등을 위하여 필요한 경우 개인정보처리자, 관계 중앙행정기관의 장, 지방자치단체의 장 및 관계 기관·단체 등을 대상으로 개인정보관리 수준 및 실태파악 등을 위한 조사를 실시할 수 있다. <신설 2015. 7. 24., 2017. 7. 26., 2020. 2. 4.>

③ 중앙행정기관의 장은 시행계획을 효율적으로 수립·추진하기 위하여 소관 분야의 개인정보처리자에게 제1항에 따른 자료제출 등을 요구할 수 있다. <개정 2015. 7. 24.>

④ 제1항부터 제3항까지에 따른 자료제출 등을 요구받은 자는 특별한 사정이 없으면 이에 따라야 한다. <개정 2015. 7. 24.>

⑤ 제1항부터 제3항까지에 따른 자료제출 등의 범위와 방법 등 필요한 사항은 대통령령으로 정한다. <개정 2015. 7. 24.>

제12조(개인정보 보호지침) ① 보호위원회는 개인정보의 처리에 관한 기준, 개인정보 침해의 유형 및 예방조치 등에 관한 표준 개인정보 보호지침(이하 “표준지침”이라 한다)을 정하여 개인정보처리자에게 그 준수를 권장할 수 있다. <개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>

② 중앙행정기관의 장은 표준지침에 따라 소관 분야의 개인정보 처리와 관련한 개인정보 보호지침을 정하여 개인정보처리자에게 그 준수를 권장할 수 있다.

③ 국회, 법원, 헌법재판소 및 중앙선거관리위원회는 해당 기관(그 소속 기관을 포함한다)의 개인정보 보호지침을 정하여 시행할 수 있다.

제13조(자율규제의 촉진 및 지원) 보호위원회는 개인정보처리자의 자율적인 개인정보 보호활동을 촉진하고 지원하기 위하여 다음 각 호의 필요한 시책을 마련하여야 한다. <개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>

1. 개인정보 보호에 관한 교육·홍보
2. 개인정보 보호와 관련된 기관·단체의 육성 및 지원
3. 개인정보 보호 인증마크의 도입·시행 지원
4. 개인정보처리자의 자율적인 규약의 제정·시행 지원
5. 그 밖에 개인정보처리자의 자율적 개인정보 보호활동을 지원하기 위하여 필요한 사항

제14조(국제협력) ① 정부는 국제적 환경에서의 개인정보 보호 수준을 향상시키기 위하여 필요한 시책을 마련하여야 한다.

② 정부는 개인정보 국외 이전으로 인하여 정보주체의 권리가 침해되지 아니하도록 관련

시책을 마련하여야 한다.

제3장 개인정보의 처리

제1절 개인정보의 수집, 이용, 제공 등

제15조(개인정보의 수집·이용) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.

1. 정보주체의 동의를 받은 경우
2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
4. 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우
5. 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
6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.

② 개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.

1. 개인정보의 수집·이용 목적
2. 수집하려는 개인정보의 항목
3. 개인정보의 보유 및 이용 기간
4. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

③ 개인정보처리자는 당초 수집 목적과 합리적으로 관련된 범위에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 대통령령으로 정하는 바에 따라 정보주체의 동의 없이 개인정보를 이용할 수 있다. <신설 2020. 2. 4.>

제16조(개인정보의 수집 제한) ① 개인정보처리자는 제15조제1항 각 호의 어느 하나에 해당하여 개인정보를 수집하는 경우에는 그 목적에 필요한 최소한의 개인정보를 수집하여야 한다. 이 경우 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담한다.

② 개인정보처리자는 정보주체의 동의를 받아 개인정보를 수집하는 경우 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 아니할 수 있다는 사실을 구체적으로 알리고 개인정보를 수집하여야 한다. <신설 2013. 8. 6.>

③ 개인정보처리자는 정보주체가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니 된다.

<개정 2013. 8. 6.>

제17조(개인정보의 제공) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당되는 경우에는 정보주체의 개인정보를 제3자에게 제공(공유를 포함한다. 이하 같다)할 수 있다. <개정 2020. 2. 4.>

1. 정보주체의 동의를 받은 경우
2. 제15조제1항제2호·제3호·제5호 및 제39조의3제2항제2호·제3호에 따라 개인정보를 수집한 목적 범위에서 개인정보를 제공하는 경우

② 개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 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

③ 개인정보처리자가 개인정보를 국외의 제3자에게 제공할 때에는 제2항 각 호에 따른 사항을 정보주체에게 알리고 동의를 받아야 하며, 이 법을 위반하는 내용으로 개인정보의 국외 이전에 관한 계약을 체결하여서는 아니 된다.

④ 개인정보처리자는 당초 수집 목적과 합리적으로 관련된 범위에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 대통령령으로 정하는 바에 따라 정보주체의 동의 없이 개인정보를 제공할 수 있다. <신설 2020. 2. 4.>

제18조(개인정보의 목적 외 이용·제공 제한) ① 개인정보처리자는 개인정보를 제15조제1항 및 제39조의3제1항 및 제2항에 따른 범위를 초과하여 이용하거나 제17조제1항 및 제3항에 따른 범위를 초과하여 제3자에게 제공하여서는 아니 된다. <개정 2020. 2. 4.>

② 제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다. 다만, 이용자(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제4호에 해당하는 자를 말한다. 이하 같다)의 개인정보를 처리하는 정보통신서비스 제공자(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제3호에 해당하는 자를 말한다. 이하 같다)의 경우 제1호·제2호의 경우로 한정하고, 제5호부터 제9호까지의 경우는 공공기관의 경우로 한정한다. <개정 2020. 2. 4.>

1. 정보주체로부터 별도의 동의를 받은 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. 삭제 <2020. 2. 4.>
5. 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 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(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우

③ 개인정보처리자는 제2항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.

1. 개인정보를 제공받는 자
2. 개인정보의 이용 목적(제공 시에는 제공받는 자의 이용 목적을 말한다)
3. 이용 또는 제공하는 개인정보의 항목
4. 개인정보의 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용 기간을 말한다)
5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

④ 공공기관은 제2항제2호부터 제6호까지, 제8호 및 제9호에 따라 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우에는 그 이용 또는 제공의 법적 근거, 목적 및 범위 등에 관하여 필요한 사항을 보호위원회가 고시로 정하는 바에 따라 관보 또는 인터넷 홈페이지 등에 게재하여야 한다. <개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>

⑤ 개인정보처리자는 제2항 각 호의 어느 하나의 경우에 해당하여 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 개인정보를 제공받는 자에게 이용 목적, 이용 방법, 그 밖에 필요한 사항에 대하여 제한을 하거나, 개인정보의 안전성 확보를 위하여 필요한 조치를 마련하도록 요청하여야 한다. 이 경우 요청을 받은 자는 개인정보의 안전성 확보를 위하여 필요한 조치를 하여야 한다.

[제목개정 2013. 8. 6.]

제19조(개인정보를 제공받은 자의 이용·제공 제한) 개인정보처리자로부터 개인정보를 제공받은 자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 개인정보를 제공받은 목적 외의 용도로 이용하거나 이를 제3자에게 제공하여서는 아니 된다.

1. 정보주체로부터 별도의 동의를 받은 경우
2. 다른 법률에 특별한 규정이 있는 경우

제20조(정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지) ① 개인정보처리자가 정보주체 이외로부터 수집한 개인정보를 처리하는 때에는 정보주체의 요구가 있으면 즉시 다음 각 호의 모든 사항을 정보주체에게 알려야 한다.

1. 개인정보의 수집 출처
2. 개인정보의 처리 목적
3. 제37조에 따른 개인정보 처리의 정지를 요구할 권리가 있다는 사실

② 제1항에도 불구하고 처리하는 개인정보의 종류·규모, 종업원 수 및 매출액 규모 등을 고려하여 대통령령으로 정하는 기준에 해당하는 개인정보처리자가 제17조제1항제1호에 따라 정보주체 이외로부터 개인정보를 수집하여 처리하는 때에는 제1항 각 호의 모든 사항을 정보주체에게 알려야 한다. 다만, 개인정보처리자가 수집한 정보에 연락처 등 정보주체에게 알릴 수 있는 개인정보가 포함되지 아니한 경우에는 그러하지 아니하다. <신설 2016. 3. 29.>

③ 제2항 본문에 따라 알리는 경우 정보주체에게 알리는 시기·방법 및 절차 등 필요한 사항은 대통령령으로 정한다. <신설 2016. 3. 29.>

④ 제1항과 제2항 본문은 다음 각 호의 어느 하나에 해당하는 경우에는 적용하지 아니한다. 다만, 이 법에 따른 정보주체의 권리보다 명백히 우선하는 경우에 한한다. <개정 2016. 3. 29.>

1. 고지를 요구하는 대상이 되는 개인정보가 제32조제2항 각 호의 어느 하나에 해당하는 개인정보파일에 포함되어 있는 경우
2. 고지로 인하여 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우

제21조(개인정보의 파기) ① 개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.

② 개인정보처리자가 제1항에 따라 개인정보를 파기할 때에는 복구 또는 재생되지 아니하도록 조치하여야 한다.

③ 개인정보처리자가 제1항 단서에 따라 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여서 저장·관리하여야 한다.

④ 개인정보의 파기방법 및 절차 등에 필요한 사항은 대통령령으로 정한다.

제22조(동의를 받는 방법) ① 개인정보처리자는 이 법에 따른 개인정보의 처리에 대하여 정보주체(제6항에 따른 법정대리인을 포함한다. 이하 이 조에서 같다)의 동의를 받을 때에는 각각의 동의 사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 각각 동의를 받아야 한다. <개정 2017. 4. 18.>

② 개인정보처리자는 제1항의 동의를 서면(「전자문서 및 전자거래 기본법」 제2조제1호에 따른 전자문서를 포함한다)으로 받을 때에는 개인정보의 수집·이용 목적, 수집·이용하려는 개인정보의 항목 등 대통령령으로 정하는 중요한 내용을 보호위원회가 고시로 정하는 방법에 따라 명확히 표시하여 알아보기 쉽게 하여야 한다. <신설 2017. 4. 18., 2017. 7. 26., 2020. 2. 4.>

③ 개인정보처리자는 제15조제1항제1호, 제17조제1항제1호, 제23조제1항제1호 및 제24조제1항제1호에 따라 개인정보의 처리에 대하여 정보주체의 동의를 받을 때에는 정보주체와의 계약 체결 등을 위하여 정보주체의 동의 없이 처리할 수 있는 개인정보와 정보주체의 동의가 필요한 개인정보를 구분하여야 한다. 이 경우 동의 없이 처리할 수 있는 개인정보라는 입증책임은 개인정보처리자가 부담한다. <개정 2016. 3. 29., 2017. 4. 18.>

④ 개인정보처리자는 정보주체에게 재화나 서비스를 홍보하거나 판매를 권유하기 위하여 개인정보의 처리에 대한 동의를 받으려는 때에는 정보주체가 이를 명확하게 인지할 수 있도록 알리고 동의를 받아야 한다. <개정 2017. 4. 18.>

⑤ 개인정보처리자는 정보주체가 제3항에 따라 선택적으로 동의할 수 있는 사항을 동의하지 아니하거나 제4항 및 제18조제2항제1호에 따른 동의를 하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니 된다. <개정 2017. 4. 18.>

⑥ 개인정보처리자는 만 14세 미만 아동의 개인정보를 처리하기 위하여 이 법에 따른 동의를 받아야 할 때에는 그 법정대리인의 동의를 받아야 한다. 이 경우 법정대리인의 동의를 받기 위하여 필요한 최소한의 정보는 법정대리인의 동의 없이 해당 아동으로부터 직접 수집할 수 있다. <개정 2017. 4. 18.>

⑦ 제1항부터 제6항까지에서 규정한 사항 외에 정보주체의 동의를 받는 세부적인 방법 및 제6항에 따른 최소한의 정보의 내용에 관하여 필요한 사항은 개인정보의 수집매체 등을 고려하여 대통령령으로 정한다. <개정 2017. 4. 18.>

제2절 개인정보의 처리 제한

제23조(민감정보의 처리 제한) ①개인정보처리자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 “민감정보”라 한다)를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다. <개정 2016. 3. 29.>

1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 민감정보의 처리를 요구하거나 허용하는 경우

② 개인정보처리자가 제1항 각 호에 따라 민감정보를 처리하는 경우에는 그 민감정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 제29조에 따른 안전성 확보에 필요한 조치를 하여야 한다. <신설 2016. 3. 29.>

제24조(고유식별정보의 처리 제한) ① 개인정보처리자는 다음 각 호의 경우를 제외하고는 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 대통령령으로 정하는 정보(이하 “고유식별정보”라 한다)를 처리할 수 없다.

1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 구체적으로 고유식별정보의 처리를 요구하거나 허용하는 경우

② 삭제 <2013. 8. 6.>

③ 개인정보처리자가 제1항 각 호에 따라 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다. <개정 2015. 7. 24.>

④ 보호위원회는 처리하는 개인정보의 종류·규모, 종업원 수 및 매출액 규모 등을 고려하여 대통령령으로 정하는 기준에 해당하는 개인정보처리자가 제3항에 따라 안전성 확보에 필요한 조치를 하였는지에 관하여 대통령령으로 정하는 바에 따라 정기적으로 조사하여야 한다. <신설 2016. 3. 29., 2017. 7. 26., 2020. 2. 4.>

⑤ 보호위원회는 대통령령으로 정하는 전문기관으로 하여금 제4항에 따른 조사를 수행하게 할 수 있다. <신설 2016. 3. 29., 2017. 7. 26., 2020. 2. 4.>

제24조의2(주민등록번호 처리의 제한) ① 제24조제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다. <개정 2014. 11. 19., 2016. 3. 29., 2017. 7. 26., 2020. 2. 4.>

1. 법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
3. 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 보호위원회가 고시로 정하는 경우

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. <신설 2014. 3. 24., 2015. 7. 24.>

③ 개인정보처리자는 제1항 각 호에 따라 주민등록번호를 처리하는 경우에도 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 한다. <개정 2014. 3. 24.>

④ 보호위원회는 개인정보처리자가 제3항에 따른 방법을 제공할 수 있도록 관계 법령의 정비, 계획의 수립, 필요한 시설 및 시스템의 구축 등 제반 조치를 마련·지원할 수 있다. <개정 2014. 3. 24., 2017. 7. 26., 2020. 2. 4.>

[본조신설 2013. 8. 6.]

제25조(영상정보처리기기의 설치·운영 제한) ① 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 영상정보처리기기를 설치·운영하여서는 아니 된다.

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 누구든지 불특정 다수가 이용하는 목욕실, 화장실, 발한실(發汗室), 탈의실 등 개인의 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있도록 영상정보처리기기를 설치·운영하여서는 아니 된다. 다만, 교도소, 정신보건 시설 등 법령에 근거하여 사람을 구금하거나 보호하는 시설로서 대통령령으로 정하는 시설에 대하여는 그러하지 아니하다.

③ 제1항 각 호에 따라 영상정보처리기기를 설치·운영하려는 공공기관의 장과 제2항 단서에 따라 영상정보처리기기를 설치·운영하려는 자는 공청회·설명회의 개최 등 대통령령으로 정하는 절차를 거쳐 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다.

④ 제1항 각 호에 따라 영상정보처리기기를 설치·운영하는 자(이하 "영상정보처리기기운영자"라 한다)는 정보주체가 쉽게 인식할 수 있도록 다음 각 호의 사항이 포함된 안내판을 설치하는 등 필요한 조치를 하여야 한다. 다만, 「군사기지 및 군사시설 보호법」 제2조제2호에 따른 군사시설, 「통합방위법」 제2조제13호에 따른 국가중요시설, 그 밖에 대통령령으로 정하는 시설에 대하여는 그러하지 아니하다. <개정 2016. 3. 29.>

1. 설치 목적 및 장소
2. 촬영 범위 및 시간
3. 관리책임자 성명 및 연락처
4. 그 밖에 대통령령으로 정하는 사항

⑤ 영상정보처리기기운영자는 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비춰서는 아니 되며, 녹음기능은 사용할 수 없다.

⑥ 영상정보처리기기운영자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 제29조에 따라 안전성 확보에 필요한 조치를 하여야 한다. <개정 2015. 7. 24.>

⑦ 영상정보처리기기운영자는 대통령령으로 정하는 바에 따라 영상정보처리기기 운영·관리 방침을 마련하여야 한다. 이 경우 제30조에 따른 개인정보 처리방침을 정하지 아니할 수 있다.

⑧ 영상정보처리기기운영자는 영상정보처리기기의 설치·운영에 관한 사무를 위탁할 수 있다. 다만, 공공기관이 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우에는 대통령령으로 정하는 절차 및 요건에 따라야 한다.

제26조(업무위탁에 따른 개인정보의 처리 제한) ① 개인정보처리자가 제3자에게 개인정보의

처리 업무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서에 의하여야 한다.

1. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
2. 개인정보의 기술적·관리적 보호조치에 관한 사항
3. 그 밖에 개인정보의 안전한 관리를 위하여 대통령령으로 정한 사항

② 제1항에 따라 개인정보의 처리 업무를 위탁하는 개인정보처리자(이하 "위탁자"라 한다)는 위탁하는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자(이하 "수탁자"라 한다)를 정보주체가 언제든지 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.

③ 위탁자가 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 대통령령으로 정하는 방법에 따라 위탁하는 업무의 내용과 수탁자를 정보주체에게 알려야 한다. 위탁하는 업무의 내용이나 수탁자가 변경된 경우에도 또한 같다.

④ 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다. <개정 2015. 7. 24.>

⑤ 수탁자는 개인정보처리자로부터 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하여서는 아니 된다.

⑥ 수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 이 법을 위반하여 발생한 손해배상책임에 대하여는 수탁자를 개인정보처리자의 소속 직원으로 본다.

⑦ 수탁자에 관하여는 제15조부터 제25조까지, 제27조부터 제31조까지, 제33조부터 제38조까지 및 제59조를 준용한다.

제27조(영업양도 등에 따른 개인정보의 이전 제한) ① 개인정보처리자는 영업의 전부 또는 일부의 양도·합병 등으로 개인정보를 다른 사람에게 이전하는 경우에는 미리 다음 각 호의 사항을 대통령령으로 정하는 방법에 따라 해당 정보주체에게 알려야 한다.

1. 개인정보를 이전하려는 사실
2. 개인정보를 이전받는 자(이하 "영업양수자등"이라 한다)의 성명(법인의 경우에는 법인의 명칭을 말한다), 주소, 전화번호 및 그 밖의 연락처
3. 정보주체가 개인정보의 이전을 원하지 아니하는 경우 조치할 수 있는 방법 및 절차

② 영업양수자등은 개인정보를 이전받았을 때에는 지체 없이 그 사실을 대통령령으로 정하는 방법에 따라 정보주체에게 알려야 한다. 다만, 개인정보처리자가 제1항에 따라 그 이전 사실을 이미 알린 경우에는 그러하지 아니하다.

③ 영업양수자등은 영업의 양도·합병 등으로 개인정보를 이전받은 경우에는 이전 당시의 본래 목적으로만 개인정보를 이용하거나 제3자에게 제공할 수 있다. 이 경우 영업양수자등은 개인정보처리자로 본다.

제28조(개인정보취급자에 대한 감독) ① 개인정보처리자는 개인정보를 처리함에 있어서 개인정보가 안전하게 관리될 수 있도록 임직원, 파견근로자, 시간제근로자 등 개인정보처리자

의 지휘·감독을 받아 개인정보를 처리하는 자(이하 “개인정보취급자”라 한다)에 대하여 적절한 관리·감독을 행하여야 한다.

② 개인정보처리자는 개인정보의 적정한 취급을 보장하기 위하여 개인정보취급자에게 정기적으로 필요한 교육을 실시하여야 한다.

제3절 가명정보의 처리에 관한 특례 <신설 2020. 2. 4.>

제28조의2(가명정보의 처리 등) ① 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다.

② 개인정보처리자는 제1항에 따라 가명정보를 제3자에게 제공하는 경우에는 특정 개인을 알아보기 위하여 사용될 수 있는 정보를 포함해서는 아니 된다.

[본조신설 2020. 2. 4.]

제28조의3(가명정보의 결합 제한) ① 제28조의2에도 불구하고 통계작성, 과학적 연구, 공익적 기록보존 등을 위한 서로 다른 개인정보처리자 간의 가명정보의 결합은 보호위원회 또는 관계 중앙행정기관의 장이 지정하는 전문기관이 수행한다.

② 결합을 수행한 기관 외부로 결합된 정보를 반출하려는 개인정보처리자는 가명정보 또는 제58조의2에 해당하는 정보로 처리한 뒤 전문기관의 장의 승인을 받아야 한다.

③ 제1항에 따른 결합 절차와 방법, 전문기관의 지정과 지정 취소 기준·절차, 관리·감독, 제2항에 따른 반출 및 승인 기준·절차 등 필요한 사항은 대통령령으로 정한다.

[본조신설 2020. 2. 4.]

제28조의4(가명정보에 대한 안전조치의무 등) ① 개인정보처리자는 가명정보를 처리하는 경우에는 원래의 상태로 복원하기 위한 추가 정보를 별도로 분리하여 보관·관리하는 등 해당 정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

② 개인정보처리자는 가명정보를 처리하고자 하는 경우에는 가명정보의 처리 목적, 제3자 제공 시 제공받는 자 등 가명정보의 처리 내용을 관리하기 위하여 대통령령으로 정하는 사항에 대한 관련 기록을 작성하여 보관하여야 한다.

[본조신설 2020. 2. 4.]

제28조의5(가명정보 처리 시 금지의무 등) ① 누구든지 특정 개인을 알아보기 위한 목적으로 가명정보를 처리해서는 아니 된다.

② 개인정보처리자는 가명정보를 처리하는 과정에서 특정 개인을 알아볼 수 있는 정보가 생성된 경우에는 즉시 해당 정보의 처리를 중지하고, 지체 없이 회수·파기하여야 한다.

[본조신설 2020. 2. 4.]

제28조의6(가명정보 처리에 대한 과징금 부과 등) ① 보호위원회는 개인정보처리자가 제28조의5제1항을 위반하여 특정 개인을 알아보기 위한 목적으로 정보를 처리한 경우 전체 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다. 다만, 매출액이

없거나 매출액의 산정이 곤란한 경우로서 대통령령으로 정하는 경우에는 4억원 또는 자본금의 100분의 3 중 큰 금액 이하로 과징금을 부과할 수 있다.

② 과징금의 부과·징수 등에 필요한 사항은 제34조의2제3항부터 제5항까지의 규정을 준용한다.

[본조신설 2020. 2. 4.]

제28조의7(적용범위) 가명정보는 제20조, 제21조, 제27조, 제34조제1항, 제35조부터 제37조까지, 제39조의3, 제39조의4, 제39조의6부터 제39조의8까지의 규정을 적용하지 아니한다.

[본조신설 2020. 2. 4.]

제4장 개인정보의 안전한 관리

제29조(안전조치의무) 개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다. <개정 2015. 7. 24.>

제30조(개인정보 처리방침의 수립 및 공개) ① 개인정보처리자는 다음 각 호의 사항이 포함된 개인정보의 처리 방침(이하 "개인정보 처리방침"이라 한다)을 정하여야 한다. 이 경우 공공기관은 제32조에 따라 등록대상이 되는 개인정보파일에 대하여 개인정보 처리방침을 정한다. <개정 2016. 3. 29., 2020. 2. 4.>

1. 개인정보의 처리 목적
2. 개인정보의 처리 및 보유 기간
3. 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다)
3의2. 개인정보의 파기절차 및 파기방법(제21조제1항 단서에 따라 개인정보를 보존하여야 하는 경우에는 그 보존근거와 보존하는 개인정보 항목을 포함한다)
4. 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다)
5. 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항
6. 제31조에 따른 개인정보 보호책임자의 성명 또는 개인정보 보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처
7. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항(해당하는 경우에만 정한다)
8. 그 밖에 개인정보의 처리에 관하여 대통령령으로 정한 사항

② 개인정보처리자가 개인정보 처리방침을 수립하거나 변경하는 경우에는 정보주체가 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.

③ 개인정보 처리방침의 내용과 개인정보처리자와 정보주체 간에 체결한 계약의 내용이 다른 경우에는 정보주체에게 유리한 것을 적용한다.

④ 보호위원회는 개인정보 처리방침의 작성지침을 정하여 개인정보처리자에게 그 준수를

권장할 수 있다. <개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>

제31조(개인정보 보호책임자의 지정) ① 개인정보처리자는 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 지정하여야 한다.

② 개인정보 보호책임자는 다음 각 호의 업무를 수행한다.

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. 그 밖에 개인정보의 적절한 처리를 위하여 대통령령으로 정한 업무

③ 개인정보 보호책임자는 제2항 각 호의 업무를 수행함에 있어서 필요한 경우 개인정보의 처리 현황, 처리 체계 등에 대하여 수시로 조사하거나 관계 당사자로부터 보고를 받을 수 있다.

④ 개인정보 보호책임자는 개인정보 보호와 관련하여 이 법 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 하며, 필요하면 소속 기관 또는 단체의 장에게 개선조치를 보고하여야 한다.

⑤ 개인정보처리자는 개인정보 보호책임자가 제2항 각 호의 업무를 수행함에 있어서 정당한 이유 없이 불이익을 주거나 받게 하여서는 아니 된다.

⑥ 개인정보 보호책임자의 지정요건, 업무, 자격요건, 그 밖에 필요한 사항은 대통령령으로 정한다.

제32조(개인정보파일의 등록 및 공개) ① 공공기관의 장이 개인정보파일을 운용하는 경우에는 다음 각 호의 사항을 보호위원회에 등록하여야 한다. 등록한 사항이 변경된 경우에도 또한 같다. <개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>

1. 개인정보파일의 명칭
2. 개인정보파일의 운영 근거 및 목적
3. 개인정보파일에 기록되는 개인정보의 항목
4. 개인정보의 처리방법
5. 개인정보의 보유기간
6. 개인정보를 통상적 또는 반복적으로 제공하는 경우에는 그 제공받는 자
7. 그 밖에 대통령령으로 정하는 사항

② 다음 각 호의 어느 하나에 해당하는 개인정보파일에 대하여는 제1항을 적용하지 아니한다.

1. 국가 안전, 외교상 비밀, 그 밖에 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일
2. 범죄의 수사, 공소의 제기 및 유지, 형 및 감호의 집행, 교정처분, 보호처분, 보안관찰

처분과 출입국관리에 관한 사항을 기록한 개인정보파일
3. 「조세범처벌법」에 따른 범칙행위 조사 및 「관세법」에 따른 범칙행위 조사에 관한 사항을 기록한 개인정보파일
4. 공공기관의 내부적 업무처리만을 위하여 사용되는 개인정보파일
5. 다른 법령에 따라 비밀로 분류된 개인정보파일

③ 보호위원회는 필요하면 제1항에 따른 개인정보파일의 등록사항과 그 내용을 검토하여 해당 공공기관의 장에게 개선을 권고할 수 있다. <개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>

④ 보호위원회는 제1항에 따른 개인정보파일의 등록 현황을 누구든지 쉽게 열람할 수 있도록 공개하여야 한다. <개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>

⑤ 제1항에 따른 등록과 제4항에 따른 공개의 방법, 범위 및 절차에 관하여 필요한 사항은 대통령령으로 정한다.

⑥ 국회, 법원, 헌법재판소, 중앙선거관리위원회(그 소속 기관을 포함한다)의 개인정보파일 등록 및 공개에 관하여는 국회규칙, 대법원규칙, 헌법재판소규칙 및 중앙선거관리위원회규칙으로 정한다.

제32조의2(개인정보 보호 인증) ① 보호위원회는 개인정보처리자의 개인정보 처리 및 보호와 관련한 일련의 조치가 이 법에 부합하는지 등에 관하여 인증할 수 있다. <개정 2017. 7. 26., 2020. 2. 4.>

② 제1항에 따른 인증의 유효기간은 3년으로 한다.

③ 보호위원회는 다음 각 호의 어느 하나에 해당하는 경우에는 대통령령으로 정하는 바에 따라 제1항에 따른 인증을 취소할 수 있다. 다만, 제1호에 해당하는 경우에는 취소하여야 한다. <개정 2017. 7. 26., 2020. 2. 4.>

1. 거짓이나 그 밖의 부정한 방법으로 개인정보 보호 인증을 받은 경우
2. 제4항에 따른 사후관리를 거부 또는 방해한 경우
3. 제8항에 따른 인증기준에 미달하게 된 경우
4. 개인정보 보호 관련 법령을 위반하고 그 위반사유가 중대한 경우

④ 보호위원회는 개인정보 보호 인증의 실효성 유지를 위하여 연 1회 이상 사후관리를 실시하여야 한다. <개정 2017. 7. 26., 2020. 2. 4.>

⑤ 보호위원회는 대통령령으로 정하는 전문기관으로 하여금 제1항에 따른 인증, 제3항에 따른 인증 취소, 제4항에 따른 사후관리 및 제7항에 따른 인증 심사원 관리 업무를 수행하게 할 수 있다. <개정 2017. 7. 26., 2020. 2. 4.>

⑥ 제1항에 따른 인증을 받은 자는 대통령령으로 정하는 바에 따라 인증의 내용을 표시하거나 홍보할 수 있다.

⑦ 제1항에 따른 인증을 위하여 필요한 심사를 수행할 심사원의 자격 및 자격 취소 요건 등에 관하여는 전문성과 경력 및 그 밖에 필요한 사항을 고려하여 대통령령으로 정한다.

⑧ 그 밖에 개인정보 관리체계, 정보주체 권리보장, 안전성 확보조치가 이 법에 부합하는

지 여부 등 제1항에 따른 인증의 기준·방법·절차 등 필요한 사항은 대통령령으로 정한다.

[본조신설 2015. 7. 24.]

제33조(개인정보 영향평가) ① 공공기관의 장은 대통령령으로 정하는 기준에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 그 위험요인의 분석과 개선 사항 도출을 위한 평가(이하 "영향평가"라 한다)를 하고 그 결과를 보호위원회에 제출하여야 한다. 이 경우 공공기관의 장은 영향평가를 보호위원회가 지정하는 기관(이하 "평가기관"이라 한다) 중에서 의뢰하여야 한다. <개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>

② 영향평가를 하는 경우에는 다음 각 호의 사항을 고려하여야 한다.

1. 처리하는 개인정보의 수
2. 개인정보의 제3자 제공 여부
3. 정보주체의 권리를 해할 가능성 및 그 위험 정도
4. 그 밖에 대통령령으로 정한 사항

③ 보호위원회는 제1항에 따라 제출받은 영향평가 결과에 대하여 의견을 제시할 수 있다. <개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>

④ 공공기관의 장은 제1항에 따라 영향평가를 한 개인정보파일을 제32조제1항에 따라 등록할 때에는 영향평가 결과를 함께 첨부하여야 한다.

⑤ 보호위원회는 영향평가의 활성화를 위하여 관계 전문가의 육성, 영향평가 기준의 개발·보급 등 필요한 조치를 마련하여야 한다. <개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>

⑥ 제1항에 따른 평가기관의 지정기준 및 지정취소, 평가기준, 영향평가의 방법·절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

⑦ 국회, 법원, 헌법재판소, 중앙선거관리위원회(그 소속 기관을 포함한다)의 영향평가에 관한 사항은 국회규칙, 대법원규칙, 헌법재판소규칙 및 중앙선거관리위원회규칙으로 정하는 바에 따른다.

⑧ 공공기관 외의 개인정보처리자는 개인정보파일 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 영향평가를 하기 위하여 적극 노력하여야 한다.

제34조(개인정보 유출 통지 등) ① 개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사실을 알려야 한다.

1. 유출된 개인정보의 항목
2. 유출된 시점과 그 경위
3. 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
4. 개인정보처리자의 대응조치 및 피해 구제절차
5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

② 개인정보처리자는 개인정보가 유출된 경우 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다.

③ 개인정보처리자는 대통령령으로 정한 규모 이상의 개인정보가 유출된 경우에는 제1항에 따른 통지 및 제2항에 따른 조치 결과를 지체 없이 보호위원회 또는 대통령령으로 정하는 전문기관에 신고하여야 한다. 이 경우 보호위원회 또는 대통령령으로 정하는 전문기관은 피해 확산방지, 피해 복구 등을 위한 기술을 지원할 수 있다. <개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>

④ 제1항에 따른 통지의 시기, 방법 및 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

제34조의2(과징금의 부과 등) ① 보호위원회는 개인정보처리자가 처리하는 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손된 경우에는 5억원 이하의 과징금을 부과·징수할 수 있다. 다만, 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 개인정보처리자가 제24조제3항에 따른 안전성 확보에 필요한 조치를 다한 경우에는 그러하지 아니하다. <개정 2014. 11. 19., 2015. 7. 24., 2017. 7. 26., 2020. 2. 4.>

② 보호위원회는 제1항에 따른 과징금을 부과하는 경우에는 다음 각 호의 사항을 고려하여야 한다. <개정 2014. 11. 19., 2015. 7. 24., 2017. 7. 26., 2020. 2. 4.>

1. 제24조제3항에 따른 안전성 확보에 필요한 조치 이행 노력 정도
2. 분실·도난·유출·위조·변조 또는 훼손된 주민등록번호의 정도
3. 피해확산 방지를 위한 후속조치 이행 여부

③ 보호위원회는 제1항에 따른 과징금을 내야 할 자가 납부기한까지 내지 아니하면 납부기한의 다음 날부터 과징금을 낸 날의 전날까지의 기간에 대하여 내지 아니한 과징금의 연 100분의 6의 범위에서 대통령령으로 정하는 가산금을 징수한다. 이 경우 가산금을 징수하는 기간은 60개월을 초과하지 못한다. <개정 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>

④ 보호위원회는 제1항에 따른 과징금을 내야 할 자가 납부기한까지 내지 아니하면 기간을 정하여 독촉을 하고, 그 지정한 기간 내에 과징금 및 제2항에 따른 가산금을 내지 아니하면 국세 체납처분의 예에 따라 징수한다. <개정 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>

⑤ 과징금의 부과·징수에 관하여 그 밖에 필요한 사항은 대통령령으로 정한다.

[본조신설 2013. 8. 6.]

제5장 정보주체의 권리 보장

제35조(개인정보의 열람) ① 정보주체는 개인정보처리자가 처리하는 자신의 개인정보에 대한 열람을 해당 개인정보처리자에게 요구할 수 있다.

② 제1항에도 불구하고 정보주체가 자신의 개인정보에 대한 열람을 공공기관에 요구하고자 할 때에는 공공기관에 직접 열람을 요구하거나 대통령령으로 정하는 바에 따라 보호위

원회를 통하여 열람을 요구할 수 있다. <개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>

③ 개인정보처리자는 제1항 및 제2항에 따른 열람을 요구받았을 때에는 대통령령으로 정하는 기간 내에 정보주체가 해당 개인정보를 열람할 수 있도록 하여야 한다. 이 경우 해당 기간 내에 열람할 수 없는 정당한 사유가 있을 때에는 정보주체에게 그 사유를 알리고 열람을 연기할 수 있으며, 그 사유가 소멸하면 지체 없이 열람하게 하여야 한다.

④ 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체에게 그 사유를 알리고 열람을 제한하거나 거절할 수 있다.

1. 법률에 따라 열람이 금지되거나 제한되는 경우
2. 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우
3. 공공기관이 다음 각 목의 어느 하나에 해당하는 업무를 수행할 때 중대한 지장을 초래하는 경우
   가. 조세의 부과·징수 또는 환급에 관한 업무
   나. 「초·중등교육법」 및 「고등교육법」에 따른 각급 학교, 「평생교육법」에 따른 평생교육시설, 그 밖의 다른 법률에 따라 설치된 고등교육기관에서의 성적 평가 또는 입학자 선발에 관한 업무
   다. 학력·기능 및 채용에 관한 시험, 자격 심사에 관한 업무
   라. 보상금·급부금 산정 등에 대하여 진행 중인 평가 또는 판단에 관한 업무
   마. 다른 법률에 따라 진행 중인 감사 및 조사에 관한 업무

⑤ 제1항부터 제4항까지의 규정에 따른 열람 요구, 열람 제한, 통지 등의 방법 및 절차에 관하여 필요한 사항은 대통령령으로 정한다.

제36조(개인정보의 정정·삭제) ① 제35조에 따라 자신의 개인정보를 열람한 정보주체는 개인정보처리자에게 그 개인정보의 정정 또는 삭제를 요구할 수 있다. 다만, 다른 법령에서 그 개인정보가 수집 대상으로 명시되어 있는 경우에는 그 삭제를 요구할 수 없다.

② 개인정보처리자는 제1항에 따른 정보주체의 요구를 받았을 때에는 개인정보의 정정 또는 삭제에 관하여 다른 법령에 특별한 절차가 규정되어 있는 경우를 제외하고는 지체 없이 그 개인정보를 조사하여 정보주체의 요구에 따라 정정·삭제 등 필요한 조치를 한 후 그 결과를 정보주체에게 알려야 한다.

③ 개인정보처리자가 제2항에 따라 개인정보를 삭제할 때에는 복구 또는 재생되지 아니하도록 조치하여야 한다.

④ 개인정보처리자는 정보주체의 요구가 제1항 단서에 해당될 때에는 지체 없이 그 내용을 정보주체에게 알려야 한다.

⑤ 개인정보처리자는 제2항에 따른 조사를 할 때 필요하면 해당 정보주체에게 정정·삭제 요구사항의 확인에 필요한 증거자료를 제출하게 할 수 있다.

⑥ 제1항·제2항 및 제4항에 따른 정정 또는 삭제 요구, 통지 방법 및 절차 등에 필요한

사항은 대통령령으로 정한다.

제37조(개인정보의 처리정지 등) ① 정보주체는 개인정보처리자에 대하여 자신의 개인정보 처리의 정지를 요구할 수 있다. 이 경우 공공기관에 대하여는 제32조에 따라 등록 대상이 되는 개인정보파일 중 자신의 개인정보에 대한 처리의 정지를 요구할 수 있다.

② 개인정보처리자는 제1항에 따른 요구를 받았을 때에는 지체 없이 정보주체의 요구에 따라 개인정보 처리의 전부를 정지하거나 일부를 정지하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체의 처리정지 요구를 거절할 수 있다.

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

③ 개인정보처리자는 제2항 단서에 따라 처리정지 요구를 거절하였을 때에는 정보주체에게 지체 없이 그 사유를 알려야 한다.

④ 개인정보처리자는 정보주체의 요구에 따라 처리가 정지된 개인정보에 대하여 지체 없이 해당 개인정보의 파기 등 필요한 조치를 하여야 한다.

⑤ 제1항부터 제3항까지의 규정에 따른 처리정지의 요구, 처리정지의 거절, 통지 등의 방법 및 절차에 필요한 사항은 대통령령으로 정한다.

제38조(권리행사의 방법 및 절차) ① 정보주체는 제35조에 따른 열람, 제36조에 따른 정정·삭제, 제37조에 따른 처리정지, 제39조의7에 따른 동의 철회 등의 요구(이하 “열람등요구”라 한다)를 문서 등 대통령령으로 정하는 방법·절차에 따라 대리인에게 하게 할 수 있다. <개정 2020. 2. 4.>

② 만 14세 미만 아동의 법정대리인은 개인정보처리자에게 그 아동의 개인정보 열람등요구를 할 수 있다.

③ 개인정보처리자는 열람등요구를 하는 자에게 대통령령으로 정하는 바에 따라 수수료와 우송료(사본의 우송을 청구하는 경우에 한한다)를 청구할 수 있다.

④ 개인정보처리자는 정보주체가 열람등요구를 할 수 있는 구체적인 방법과 절차를 마련하고, 이를 정보주체가 알 수 있도록 공개하여야 한다.

⑤ 개인정보처리자는 정보주체가 열람등요구에 대한 거절 등 조치에 대하여 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하고 안내하여야 한다.

제39조(손해배상책임) ① 정보주체는 개인정보처리자가 이 법을 위반한 행위로 손해를 입으면 개인정보처리자에게 손해배상을 청구할 수 있다. 이 경우 그 개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.

② 삭제 <2015. 7. 24.>

③ 개인정보처리자의 고의 또는 중대한 과실로 인하여 개인정보가 분실・도난・유출・위조・변조 또는 훼손된 경우로서 정보주체에게 손해가 발생한 때에는 법원은 그 손해액의 3배를 넘지 아니하는 범위에서 손해배상액을 정할 수 있다. 다만, 개인정보처리자가 고의 또는 중대한 과실이 없음을 증명한 경우에는 그러하지 아니하다. <신설 2015. 7. 24.>

④ 법원은 제3항의 배상액을 정할 때에는 다음 각 호의 사항을 고려하여야 한다. <신설 2015. 7. 24.>

1. 고의 또는 손해 발생의 우려를 인식한 정도
2. 위반행위로 인하여 입은 피해 규모
3. 위법행위로 인하여 개인정보처리자가 취득한 경제적 이익
4. 위반행위에 따른 벌금 및 과징금
5. 위반행위의 기간・횟수 등
6. 개인정보처리자의 재산상태
7. 개인정보처리자가 정보주체의 개인정보 분실・도난・유출 후 해당 개인정보를 회수하기 위하여 노력한 정도
8. 개인정보처리자가 정보주체의 피해구제를 위하여 노력한 정도

제39조의2(법정손해배상의 청구) ① 제39조제1항에도 불구하고 정보주체는 개인정보처리자의 고의 또는 과실로 인하여 개인정보가 분실・도난・유출・위조・변조 또는 훼손된 경우에는 300만원 이하의 범위에서 상당한 금액을 손해액으로 하여 배상을 청구할 수 있다. 이 경우 해당 개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.

② 법원은 제1항에 따른 청구가 있는 경우에 변론 전체의 취지와 증거조사의 결과를 고려하여 제1항의 범위에서 상당한 손해액을 인정할 수 있다.

③ 제39조에 따라 손해배상을 청구한 정보주체는 사실심(事實審)의 변론이 종결되기 전까지 그 청구를 제1항에 따른 청구로 변경할 수 있다.

[본조신설 2015. 7. 24.]

제6장 정보통신서비스 제공자 등의 개인정보 처리 등 특례 <신설 2020. 2. 4.>

제39조의3(개인정보의 수집・이용 동의 등에 대한 특례) ① 정보통신서비스 제공자는 제15조제1항에도 불구하고 이용자의 개인정보를 이용하려고 수집하는 경우에는 다음 각 호의 모든 사항을 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항을 변경하려는 경우에도 또한 같다.

1. 개인정보의 수집・이용 목적
2. 수집하는 개인정보의 항목
3. 개인정보의 보유・이용 기간

② 정보통신서비스 제공자는 다음 각 호의 어느 하나에 해당하는 경우에는 제1항에 따른

동의 없이 이용자의 개인정보를 수집·이용할 수 있다.

1. 정보통신서비스(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제2호에 따른 정보통신서비스를 말한다. 이하 같다)의 제공에 관한 계약을 이행하기 위하여 필요한 개인정보로서 경제적·기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우
2. 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우
3. 다른 법률에 특별한 규정이 있는 경우

③ 정보통신서비스 제공자는 이용자가 필요한 최소한의 개인정보 이외의 개인정보를 제공하지 아니한다는 이유로 그 서비스의 제공을 거부해서는 아니 된다. 이 경우 필요한 최소한의 개인정보는 해당 서비스의 본질적 기능을 수행하기 위하여 반드시 필요한 정보를 말한다.

④ 정보통신서비스 제공자는 만 14세 미만의 아동으로부터 개인정보 수집·이용·제공 등의 동의를 받으려면 그 법정대리인의 동의를 받아야 하고, 대통령령으로 정하는 바에 따라 법정대리인이 동의하였는지를 확인하여야 한다.

⑤ 정보통신서비스 제공자는 만 14세 미만의 아동에게 개인정보 처리와 관련한 사항의 고지 등을 하는 때에는 이해하기 쉬운 양식과 명확하고 알기 쉬운 언어를 사용하여야 한다.

⑥ 보호위원회는 개인정보 처리에 따른 위험성 및 결과, 이용자의 권리 등을 명확하게 인지하지 못할 수 있는 만 14세 미만의 아동의 개인정보 보호 시책을 마련하여야 한다. [본조신설 2020. 2. 4.]

제39조의4(개인정보 유출등의 통지·신고에 대한 특례) ① 제34조제1항 및 제3항에도 불구하고 정보통신서비스 제공자와 그로부터 제17조제1항에 따라 이용자의 개인정보를 제공받은 자(이하 “정보통신서비스 제공자등”이라 한다)는 개인정보의 분실·도난·유출(이하 “유출등”이라 한다) 사실을 안 때에는 지체 없이 다음 각 호의 사항을 해당 이용자에게 알리고 보호위원회 또는 대통령령으로 정하는 전문기관에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다. 다만, 이용자의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다.

1. 유출등이 된 개인정보 항목
2. 유출등이 발생한 시점
3. 이용자가 취할 수 있는 조치
4. 정보통신서비스 제공자등의 대응 조치
5. 이용자가 상담 등을 접수할 수 있는 부서 및 연락처

② 제1항의 신고를 받은 대통령령으로 정하는 전문기관은 지체 없이 그 사실을 보호위원회에 알려야 한다.

③ 정보통신서비스 제공자등은 제1항에 따른 정당한 사유를 보호위원회에 소명하여야 한

다.

④ 제1항에 따른 통지 및 신고의 방법·절차 등에 필요한 사항은 대통령령으로 정한다.

[본조신설 2020. 2. 4.]

제39조의5(개인정보의 보호조치에 대한 특례) 정보통신서비스 제공자등은 이용자의 개인정보를 처리하는 자를 최소한으로 제한하여야 한다.

[본조신설 2020. 2. 4.]

제39조의6(개인정보의 파기에 대한 특례) ① 정보통신서비스 제공자등은 정보통신서비스를 1년의 기간 동안 이용하지 아니하는 이용자의 개인정보를 보호하기 위하여 대통령령으로 정하는 바에 따라 개인정보의 파기 등 필요한 조치를 취하여야 한다. 다만, 그 기간에 대하여 다른 법령 또는 이용자의 요청에 따라 달리 정한 경우에는 그에 따른다.

② 정보통신서비스 제공자등은 제1항의 기간 만료 30일 전까지 개인정보가 파기되는 사실, 기간 만료일 및 파기되는 개인정보의 항목 등 대통령령으로 정하는 사항을 전자우편 등 대통령령으로 정하는 방법으로 이용자에게 알려야 한다.

[본조신설 2020. 2. 4.]

제39조의7(이용자의 권리 등에 대한 특례) ① 이용자는 정보통신서비스 제공자등에 대하여 언제든지 개인정보 수집·이용·제공 등의 동의를 철회할 수 있다.

② 정보통신서비스 제공자등은 제1항에 따른 동의의 철회, 제35조에 따른 개인정보의 열람, 제36조에 따른 정정을 요구하는 방법을 개인정보의 수집방법보다 쉽게 하여야 한다.

③ 정보통신서비스 제공자등은 제1항에 따라 동의를 철회하면 지체 없이 수집된 개인정보를 복구·재생할 수 없도록 파기하는 등 필요한 조치를 하여야 한다.

[본조신설 2020. 2. 4.]

제39조의8(개인정보 이용내역의 통지) ① 정보통신서비스 제공자 등으로서 대통령령으로 정하는 기준에 해당하는 자는 제23조, 제39조의3에 따라 수집한 이용자의 개인정보의 이용내역(제17조에 따른 제공을 포함한다)을 주기적으로 이용자에게 통지하여야 한다. 다만, 연락처 등 이용자에게 통지할 수 있는 개인정보를 수집하지 아니한 경우에는 그러하지 아니한다.

② 제1항에 따라 이용자에게 통지하여야 하는 정보의 종류, 통지주기 및 방법, 그 밖에 이용내역 통지에 필요한 사항은 대통령령으로 정한다.

[본조신설 2020. 2. 4.]

제39조의9(손해배상의 보장) ① 정보통신서비스 제공자등은 제39조 및 제39조의2에 따른 손해배상책임의 이행을 위하여 보험 또는 공제에 가입하거나 준비금을 적립하는 등 필요한 조치를 하여야 한다.

② 제1항에 따른 가입 대상 개인정보처리자의 범위, 기준 등에 필요한 사항은 대통령령으로 정한다.

[본조신설 2020. 2. 4.]

제39조의10(노출된 개인정보의 삭제·차단) ① 정보통신서비스 제공자등은 주민등록번호, 계좌정보, 신용카드정보 등 이용자의 개인정보가 정보통신망을 통하여 공중에 노출되지 아니하도록 하여야 한다.

② 제1항에도 불구하고 공중에 노출된 개인정보에 대하여 보호위원회 또는 대통령령으로 지정한 전문기관의 요청이 있는 경우 정보통신서비스 제공자등은 삭제·차단 등 필요한 조치를 취하여야 한다.

[본조신설 2020. 2. 4.]

제39조의11(국내대리인의 지정) ① 국내에 주소 또는 영업소가 없는 정보통신서비스 제공자등으로서 이용자 수, 매출액 등을 고려하여 대통령령으로 정하는 기준에 해당하는 자는 다음 각 호의 사항을 대리하는 자(이하 "국내대리인"이라 한다)를 서면으로 지정하여야 한다.

1. 제31조에 따른 개인정보 보호책임자의 업무
2. 제39조의4에 따른 통지·신고
3. 제63조제1항에 따른 관계 물품·서류 등의 제출

② 국내대리인은 국내에 주소 또는 영업소가 있는 자로 한다.

③ 제1항에 따라 국내대리인을 지정한 때에는 다음 각 호의 사항 모두를 제30조에 따른 개인정보 처리방침에 포함하여야 한다.

1. 국내대리인의 성명(법인의 경우에는 그 명칭 및 대표자의 성명을 말한다)
2. 국내대리인의 주소(법인의 경우에는 영업소 소재지를 말한다), 전화번호 및 전자우편 주소

④ 국내대리인이 제1항 각 호와 관련하여 이 법을 위반한 경우에는 정보통신서비스 제공자등이 그 행위를 한 것으로 본다.

[본조신설 2020. 2. 4.]

제39조의12(국외 이전 개인정보의 보호) ① 정보통신서비스 제공자등은 이용자의 개인정보에 관하여 이 법을 위반하는 사항을 내용으로 하는 국제계약을 체결해서는 아니 된다.

② 제17조제3항에도 불구하고 정보통신서비스 제공자등은 이용자의 개인정보를 국외에 제공(조회되는 경우를 포함한다)·처리위탁·보관(이하 이 조에서 "이전"이라 한다)하려면 이용자의 동의를 받아야 한다. 다만, 제3항 각 호의 사항 모두를 제30조제2항에 따라 공개하거나 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알린 경우에는 개인정보 처리위탁·보관에 따른 동의절차를 거치지 아니할 수 있다.

③ 정보통신서비스 제공자등은 제2항 본문에 따른 동의를 받으려면 미리 다음 각 호의 사항 모두를 이용자에게 고지하여야 한다.

1. 이전되는 개인정보 항목
2. 개인정보가 이전되는 국가, 이전일시 및 이전방법
3. 개인정보를 이전받는 자의 성명(법인인 경우에는 그 명칭 및 정보관리책임자의 연락처를 말한다)

4. 개인정보를 이전받는 자의 개인정보 이용목적 및 보유·이용 기간

④ 정보통신서비스 제공자등은 제2항 본문에 따른 동의를 받아 개인정보를 국외로 이전하는 경우 대통령령으로 정하는 바에 따라 보호조치를 하여야 한다.

⑤ 이용자의 개인정보를 이전받는 자가 해당 개인정보를 제3국으로 이전하는 경우에 관하여는 제1항부터 제4항까지의 규정을 준용한다. 이 경우 “정보통신서비스 제공자등”은 “개인정보를 이전받는 자”로, “개인정보를 이전받는 자”는 “제3국에서 개인정보를 이전받는 자”로 본다.

[본조신설 2020. 2. 4.]

제39조의13(상호주의) 제39조의12에도 불구하고 개인정보의 국외 이전을 제한하는 국가의 정보통신서비스 제공자등에 대하여는 해당 국가의 수준에 상응하는 제한을 할 수 있다. 다만, 조약 또는 그 밖의 국제협정의 이행에 필요한 경우에는 그러하지 아니하다.

[본조신설 2020. 2. 4.]

제39조의14(방송사업자등에 대한 특례) 「방송법」 제2조제3호가목부터 마목까지와 같은 조 제6호·제9호·제12호 및 제14호에 해당하는 자(이하 이 조에서 “방송사업자등”이라 한다)가 시청자의 개인정보를 처리하는 경우에는 정보통신서비스 제공자에게 적용되는 규정을 준용한다. 이 경우 “방송사업자등”은 “정보통신서비스 제공자” 또는 “정보통신서비스 제공자등”으로, “시청자”는 “이용자”로 본다.

[본조신설 2020. 2. 4.]

제39조의15(과징금의 부과 등에 대한 특례) ① 보호위원회는 정보통신서비스 제공자등에게 다음 각 호의 어느 하나에 해당하는 행위가 있는 경우에는 해당 정보통신서비스 제공자등에게 위반행위와 관련한 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다.

1. 제17조제1항·제2항, 제18조제1항·제2항 및 제19조(제39조의14에 따라 준용되는 경우를 포함한다)를 위반하여 개인정보를 이용·제공한 경우
2. 제22조제6항(제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 법정대리인의 동의를 받지 아니하고 만 14세 미만인 아동의 개인정보를 수집한 경우
3. 제23조제1항제1호(제39조의14에 따라 준용되는 경우를 포함한다)를 위반하여 이용자의 동의를 받지 아니하고 민감정보를 수집한 경우
4. 제26조제4항(제39조의14에 따라 준용되는 경우를 포함한다)에 따른 관리·감독 또는 교육을 소홀히 하여 특례 수탁자가 이 법의 규정을 위반한 경우
5. 이용자의 개인정보를 분실·도난·유출·위조·변조 또는 훼손한 경우로서 제29조의 조치(내부 관리계획 수립에 관한 사항은 제외한다)를 하지 아니한 경우(제39조의14에 따라 준용되는 경우를 포함한다)
6. 제39조의3제1항(제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 이용자의 동의를 받지 아니하고 개인정보를 수집한 경우
7. 제39조의12제2항 본문(같은 조 제5항에 따라 준용되는 경우를 포함한다)을 위반하여

이용자의 동의를 받지 아니하고 이용자의 개인정보를 국외에 제공한 경우

② 제1항에 따른 과징금을 부과하는 경우 정보통신서비스 제공자등이 매출액 산정자료의 제출을 거부하거나 거짓의 자료를 제출한 경우에는 해당 정보통신서비스 제공자등과 비슷한 규모의 정보통신서비스 제공자등의 재무제표 등 회계자료와 가입자 수 및 이용요금 등 영업현황 자료에 근거하여 매출액을 추정할 수 있다. 다만, 매출액이 없거나 매출액의 산정이 곤란한 경우로서 대통령령으로 정하는 경우에는 4억원 이하의 과징금을 부과할 수 있다.

③ 보호위원회는 제1항에 따른 과징금을 부과하려면 다음 각 호의 사항을 고려하여야 한다.

1. 위반행위의 내용 및 정도
2. 위반행위의 기간 및 횟수
3. 위반행위로 인하여 취득한 이익의 규모

④ 제1항에 따른 과징금은 제3항을 고려하여 산정하되, 구체적인 산정기준과 산정절차는 대통령령으로 정한다.

⑤ 보호위원회는 제1항에 따른 과징금을 내야 할 자가 납부기한까지 이를 내지 아니하면 납부기한의 다음 날부터 내지 아니한 과징금의 연 100분의 6에 해당하는 가산금을 징수한다.

⑥ 보호위원회는 제1항에 따른 과징금을 내야 할 자가 납부기한까지 이를 내지 아니한 경우에는 기간을 정하여 독촉을 하고, 그 지정된 기간에 과징금과 제5항에 따른 가산금을 내지 아니하면 국세 체납처분의 예에 따라 징수한다.

⑦ 법원의 판결 등의 사유로 제1항에 따라 부과된 과징금을 환급하는 경우에는 과징금을 낸 날부터 환급하는 날까지의 기간에 대하여 금융회사 등의 예금이자율 등을 고려하여 대통령령으로 정하는 이자율에 따라 계산한 환급가산금을 지급하여야 한다.

⑧ 제7항에도 불구하고 법원의 판결에 의하여 과징금 부과처분이 취소되어 그 판결이유에 따라 새로운 과징금을 부과하는 경우에는 당초 납부한 과징금에서 새로 부과하기로 결정한 과징금을 공제한 나머지 금액에 대해서만 환급가산금을 계산하여 지급한다.

[본조신설 2020. 2. 4.]

제7장 개인정보 분쟁조정위원회 <개정 2020. 2. 4.>

제40조(설치 및 구성) ① 개인정보에 관한 분쟁의 조정(調停)을 위하여 개인정보 분쟁조정위원회(이하 “분쟁조정위원회”라 한다)를 둔다.

② 분쟁조정위원회는 위원장 1명을 포함한 20명 이내의 위원으로 구성하며, 위원은 당연직위원과 위촉위원으로 구성한다. <개정 2015. 7. 24.>

③ 위촉위원은 다음 각 호의 어느 하나에 해당하는 사람 중에서 보호위원회 위원장이 위촉하고, 대통령령으로 정하는 국가기관 소속 공무원은 당연직위원이 된다. <개정 2013. 3. 23., 2014. 11. 19., 2015. 7. 24.>

1. 개인정보 보호업무를 관장하는 중앙행정기관의 고위공무원단에 속하는 공무원으로 재직하였던 사람 또는 이에 상당하는 공공부문 및 관련 단체의 직에 재직하고 있거나 재직하였던 사람으로서 개인정보 보호업무의 경험이 있는 사람
2. 대학이나 공인된 연구기관에서 부교수 이상 또는 이에 상당하는 직에 재직하고 있거나 재직하였던 사람
3. 판사·검사 또는 변호사로 재직하고 있거나 재직하였던 사람
4. 개인정보 보호와 관련된 시민사회단체 또는 소비자단체로부터 추천을 받은 사람
5. 개인정보처리자로 구성된 사업자단체의 임원으로 재직하고 있거나 재직하였던 사람

④ 위원장은 위원 중에서 공무원이 아닌 사람으로 보호위원회 위원장이 위촉한다. <개정 2013. 3. 23., 2014. 11. 19., 2015. 7. 24.>

⑤ 위원장과 위촉위원의 임기는 2년으로 하되, 1차에 한하여 연임할 수 있다. <개정 2015. 7. 24.>

⑥ 분쟁조정위원회는 분쟁조정 업무를 효율적으로 수행하기 위하여 필요하면 대통령령으로 정하는 바에 따라 조정사건의 분야별로 5명 이내의 위원으로 구성되는 조정부를 둘 수 있다. 이 경우 조정부가 분쟁조정위원회에서 위임받아 의결한 사항은 분쟁조정위원회에서 의결한 것으로 본다.

⑦ 분쟁조정위원회 또는 조정부는 재적위원 과반수의 출석으로 개의하며 출석위원 과반수의 찬성으로 의결한다.

⑧ 보호위원회는 분쟁조정 접수, 사실 확인 등 분쟁조정에 필요한 사무를 처리할 수 있다. <개정 2015. 7. 24.>

⑨ 이 법에서 정한 사항 외에 분쟁조정위원회 운영에 필요한 사항은 대통령령으로 정한다.

제41조(위원의 신분보장) 위원은 자격정지 이상의 형을 선고받거나 심신상의 장애로 직무를 수행할 수 없는 경우를 제외하고는 그의 의사에 반하여 면직되거나 해촉되지 아니한다.

제42조(위원의 제척·기피·회피) ① 분쟁조정위원회의 위원은 다음 각 호의 어느 하나에 해당하는 경우에는 제43조제1항에 따라 분쟁조정위원회에 신청된 분쟁조정사건(이하 이 조에서 “사건”이라 한다)의 심의·의결에서 제척(除斥)된다.

1. 위원 또는 그 배우자나 배우자였던 자가 그 사건의 당사자가 되거나 그 사건에 관하여 공동의 권리자 또는 의무자의 관계에 있는 경우
2. 위원이 그 사건의 당사자와 친족이거나 친족이었던 경우
3. 위원이 그 사건에 관하여 증언, 감정, 법률자문을 한 경우
4. 위원이 그 사건에 관하여 당사자의 대리인으로서 관여하거나 관여하였던 경우

② 당사자는 위원에게 공정한 심의·의결을 기대하기 어려운 사정이 있으면 위원장에게 기피신청을 할 수 있다. 이 경우 위원장은 기피신청에 대하여 분쟁조정위원회의 의결을 거치지 아니하고 결정한다.

③ 위원이 제1항 또는 제2항의 사유에 해당하는 경우에는 스스로 그 사건의 심의·의결

에서 회피할 수 있다.

제43조(조정의 신청 등) ① 개인정보와 관련한 분쟁의 조정을 원하는 자는 분쟁조정위원회에 분쟁조정을 신청할 수 있다.

② 분쟁조정위원회는 당사자 일방으로부터 분쟁조정 신청을 받았을 때에는 그 신청내용을 상대방에게 알려야 한다.

③ 공공기관이 제2항에 따른 분쟁조정의 통지를 받은 경우에는 특별한 사유가 없으면 분쟁조정에 응하여야 한다.

제44조(처리기간) ① 분쟁조정위원회는 제43조제1항에 따른 분쟁조정 신청을 받은 날부터 60일 이내에 이를 심사하여 조정안을 작성하여야 한다. 다만, 부득이한 사정이 있는 경우에는 분쟁조정위원회의 의결로 처리기간을 연장할 수 있다.

② 분쟁조정위원회는 제1항 단서에 따라 처리기간을 연장한 경우에는 기간연장의 사유와 그 밖의 기간연장에 관한 사항을 신청인에게 알려야 한다.

제45조(자료의 요청 등) ① 분쟁조정위원회는 제43조제1항에 따라 분쟁조정 신청을 받았을 때에는 해당 분쟁의 조정을 위하여 필요한 자료를 분쟁당사자에게 요청할 수 있다. 이 경우 분쟁당사자는 정당한 사유가 없으면 요청에 따라야 한다.

② 분쟁조정위원회는 필요하다고 인정하면 분쟁당사자나 참고인을 위원회에 출석하도록 하여 그 의견을 들을 수 있다.

제46조(조정 전 합의 권고) 분쟁조정위원회는 제43조제1항에 따라 분쟁조정 신청을 받았을 때에는 당사자에게 그 내용을 제시하고 조정 전 합의를 권고할 수 있다.

제47조(분쟁의 조정) ① 분쟁조정위원회는 다음 각 호의 어느 하나의 사항을 포함하여 조정안을 작성할 수 있다.

1. 조사 대상 침해행위의 중지
2. 원상회복, 손해배상, 그 밖에 필요한 구제조치
3. 같거나 비슷한 침해의 재발을 방지하기 위하여 필요한 조치

② 분쟁조정위원회는 제1항에 따라 조정안을 작성하면 지체 없이 각 당사자에게 제시하여야 한다.

③ 제1항에 따라 조정안을 제시받은 당사자가 제시받은 날부터 15일 이내에 수락 여부를 알리지 아니하면 조정을 거부한 것으로 본다.

④ 당사자가 조정내용을 수락한 경우 분쟁조정위원회는 조정서를 작성하고, 분쟁조정위원회의 위원장과 각 당사자가 기명날인하여야 한다.

⑤ 제4항에 따른 조정의 내용은 재판상 화해와 동일한 효력을 갖는다.

제48조(조정의 거부 및 중지) ① 분쟁조정위원회는 분쟁의 성질상 분쟁조정위원회에서 조정하는 것이 적합하지 아니하다고 인정하거나 부정한 목적으로 조정이 신청되었다고 인정하는 경우에는 그 조정을 거부할 수 있다. 이 경우 조정거부의 사유 등을 신청인에게 알려야 한다.

② 분쟁조정위원회는 신청된 조정사건에 대한 처리절차를 진행하던 중에 한 쪽 당사자가 소를 제기하면 그 조정의 처리를 중지하고 이를 당사자에게 알려야 한다.

제49조(집단분쟁조정) ① 국가 및 지방자치단체, 개인정보 보호단체 및 기관, 정보주체, 개인정보처리자는 정보주체의 피해 또는 권리침해가 다수의 정보주체에게 같거나 비슷한 유형으로 발생하는 경우로서 대통령령으로 정하는 사건에 대하여는 분쟁조정위원회에 일괄적인 분쟁조정(이하 “집단분쟁조정”이라 한다)을 의뢰 또는 신청할 수 있다.

② 제1항에 따라 집단분쟁조정을 의뢰받거나 신청받은 분쟁조정위원회는 그 의결로써 제3항부터 제7항까지의 규정에 따른 집단분쟁조정의 절차를 개시할 수 있다. 이 경우 분쟁조정위원회는 대통령령으로 정하는 기간 동안 그 절차의 개시를 공고하여야 한다.

③ 분쟁조정위원회는 집단분쟁조정의 당사자가 아닌 정보주체 또는 개인정보처리자로부터 그 분쟁조정의 당사자에 추가로 포함될 수 있도록 하는 신청을 받을 수 있다.

④ 분쟁조정위원회는 그 의결로써 제1항 및 제3항에 따른 집단분쟁조정의 당사자 중에서 공동의 이익을 대표하기에 가장 적합한 1인 또는 수인을 대표당사자로 선임할 수 있다.

⑤ 분쟁조정위원회는 개인정보처리자가 분쟁조정위원회의 집단분쟁조정의 내용을 수락한 경우에는 집단분쟁조정의 당사자가 아닌 자로서 피해를 입은 정보주체에 대한 보상계획서를 작성하여 분쟁조정위원회에 제출하도록 권고할 수 있다.

⑥ 제48조제2항에도 불구하고 분쟁조정위원회는 집단분쟁조정의 당사자인 다수의 정보주체 중 일부의 정보주체가 법원에 소를 제기한 경우에는 그 절차를 중지하지 아니하고, 소를 제기한 일부의 정보주체를 그 절차에서 제외한다.

⑦ 집단분쟁조정의 기간은 제2항에 따른 공고가 종료된 날의 다음 날부터 60일 이내로 한다. 다만, 부득이한 사정이 있는 경우에는 분쟁조정위원회의 의결로 처리기간을 연장할 수 있다.

⑧ 집단분쟁조정의 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

제50조(조정절차 등) ① 제43조부터 제49조까지의 규정에서 정한 것 외에 분쟁의 조정방법, 조정절차 및 조정업무의 처리 등에 필요한 사항은 대통령령으로 정한다.

② 분쟁조정위원회의 운영 및 분쟁조정 절차에 관하여 이 법에서 규정하지 아니한 사항에 대하여는 「민사조정법」을 준용한다.

제8장 개인정보 단체소송 <개정 2020. 2. 4.>

제51조(단체소송의 대상 등) 다음 각 호의 어느 하나에 해당하는 단체는 개인정보처리자가 제49조에 따른 집단분쟁조정을 거부하거나 집단분쟁조정의 결과를 수락하지 아니한 경우에는 법원에 권리침해 행위의 금지·중지를 구하는 소송(이하 “단체소송”이라 한다)을 제기할 수 있다.

1. 「소비자기본법」 제29조에 따라 공정거래위원회에 등록한 소비자단체로서 다음 각 목의 요건을 모두 갖춘 단체

가. 정관에 따라 상시적으로 정보주체의 권익증진을 주된 목적으로 하는 단체일 것

나. 단체의 정회원수가 1천명 이상일 것
다. 「소비자기본법」 제29조에 따른 등록 후 3년이 경과하였을 것
2. 「비영리민간단체 지원법」 제2조에 따른 비영리민간단체로서 다음 각 목의 요건을 모두 갖춘 단체
가. 법률상 또는 사실상 동일한 침해를 입은 100명 이상의 정보주체로부터 단체소송의 제기를 요청받을 것
나. 정관에 개인정보 보호를 단체의 목적으로 명시한 후 최근 3년 이상 이를 위한 활동실적이 있을 것
다. 단체의 상시 구성원수가 5천명 이상일 것
라. 중앙행정기관에 등록되어 있을 것

제52조(전속관할) ① 단체소송의 소는 피고의 주된 사무소 또는 영업소가 있는 곳, 주된 사무소나 영업소가 없는 경우에는 주된 업무담당자의 주소가 있는 곳의 지방법원 본원 합의부의 관할에 전속한다.
② 제1항을 외국사업자에 적용하는 경우 대한민국에 있는 이들의 주된 사무소·영업소 또는 업무담당자의 주소에 따라 정한다.

제53조(소송대리인의 선임) 단체소송의 원고는 변호사를 소송대리인으로 선임하여야 한다.

제54조(소송허가신청) ① 단체소송을 제기하는 단체는 소장과 함께 다음 각 호의 사항을 기재한 소송허가신청서를 법원에 제출하여야 한다.
1. 원고 및 그 소송대리인
2. 피고
3. 정보주체의 침해된 권리의 내용
② 제1항에 따른 소송허가신청서에는 다음 각 호의 자료를 첨부하여야 한다.
1. 소제기단체가 제51조 각 호의 어느 하나에 해당하는 요건을 갖추고 있음을 소명하는 자료
2. 개인정보처리자가 조정을 거부하였거나 조정결과를 수락하지 아니하였음을 증명하는 서류

제55조(소송허가요건 등) ① 법원은 다음 각 호의 요건을 모두 갖춘 경우에 한하여 결정으로 단체소송을 허가한다.
1. 개인정보처리자가 분쟁조정위원회의 조정을 거부하거나 조정결과를 수락하지 아니하였을 것
2. 제54조에 따른 소송허가신청서의 기재사항에 흠결이 없을 것
② 단체소송을 허가하거나 불허가하는 결정에 대하여는 즉시항고할 수 있다.

제56조(확정판결의 효력) 원고의 청구를 기각하는 판결이 확정된 경우 이와 동일한 사안에 관하여는 제51조에 따른 다른 단체는 단체소송을 제기할 수 없다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.

1. 판결이 확정된 후 그 사안과 관련하여 국가·지방자치단체 또는 국가·지방자치단체가 설립한 기관에 의하여 새로운 증거가 나타난 경우
2. 기각판결이 원고의 고의로 인한 것임이 밝혀진 경우

제57조(「민사소송법」의 적용 등) ① 단체소송에 관하여 이 법에 특별한 규정이 없는 경우에는 「민사소송법」을 적용한다.
② 제55조에 따른 단체소송의 허가결정이 있는 경우에는 「민사집행법」 제4편에 따른 보전처분을 할 수 있다.
③ 단체소송의 절차에 관하여 필요한 사항은 대법원규칙으로 정한다.

제9장 보칙 <개정 2020. 2. 4.>

제58조(적용의 일부 제외) ① 다음 각 호의 어느 하나에 해당하는 개인정보에 관하여는 제3장부터 제7장까지를 적용하지 아니한다.
1. 공공기관이 처리하는 개인정보 중 「통계법」에 따라 수집되는 개인정보
2. 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보
3. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보
4. 언론, 종교단체, 정당이 각각 취재·보도, 선교, 선거 입후보자 추천 등 고유 목적을 달성하기 위하여 수집·이용하는 개인정보
② 제25조제1항 각 호에 따라 공개된 장소에 영상정보처리기기를 설치·운영하여 처리되는 개인정보에 대하여는 제15조, 제22조, 제27조제1항·제2항, 제34조 및 제37조를 적용하지 아니한다.
③ 개인정보처리자가 동창회, 동호회 등 친목 도모를 위한 단체를 운영하기 위하여 개인정보를 처리하는 경우에는 제15조, 제30조 및 제31조를 적용하지 아니한다.
④ 개인정보처리자는 제1항 각 호에 따라 개인정보를 처리하는 경우에도 그 목적을 위하여 필요한 범위에서 최소한의 기간에 최소한의 개인정보만을 처리하여야 하며, 개인정보의 안전한 관리를 위하여 필요한 기술적·관리적 및 물리적 보호조치, 개인정보의 처리에 관한 고충처리, 그 밖에 개인정보의 적절한 처리를 위하여 필요한 조치를 마련하여야 한다.

제58조의2(적용제외) 이 법은 시간·비용·기술 등을 합리적으로 고려할 때 다른 정보를 사용하여도 더 이상 개인을 알아볼 수 없는 정보에는 적용하지 아니한다.
[본조신설 2020. 2. 4.]

제59조(금지행위) 개인정보를 처리하거나 처리하였던 자는 다음 각 호의 어느 하나에 해당하는 행위를 하여서는 아니 된다.
1. 거짓이나 그 밖의 부정한 수단이나 방법으로 개인정보를 취득하거나 처리에 관한 동의를 받는 행위

2. 업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공하는 행위
3. 정당한 권한 없이 또는 허용된 권한을 초과하여 다른 사람의 개인정보를 훼손, 멸실, 변경, 위조 또는 유출하는 행위

제60조(비밀유지 등) 다음 각 호의 업무에 종사하거나 종사하였던 자는 직무상 알게 된 비밀을 다른 사람에게 누설하거나 직무상 목적 외의 용도로 이용하여서는 아니 된다. 다만, 다른 법률에 특별한 규정이 있는 경우에는 그러하지 아니하다. <개정 2020. 2. 4.>
1. 제7조의8 및 제7조의9에 따른 보호위원회의 업무
1의2. 제32조의2에 따른 개인정보 보호 인증 업무
2. 제33조에 따른 영향평가 업무
3. 제40조에 따른 분쟁조정위원회의 분쟁조정 업무

제61조(의견제시 및 개선권고) ① 보호위원회는 개인정보 보호에 영향을 미치는 내용이 포함된 법령이나 조례에 대하여 필요하다고 인정하면 심의·의결을 거쳐 관계 기관에 의견을 제시할 수 있다. <개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>
② 보호위원회는 개인정보 보호를 위하여 필요하다고 인정하면 개인정보처리자에게 개인정보 처리 실태의 개선을 권고할 수 있다. 이 경우 권고를 받은 개인정보처리자는 이를 이행하기 위하여 성실하게 노력하여야 하며, 그 조치 결과를 보호위원회에 알려야 한다. <개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>
③ 관계 중앙행정기관의 장은 개인정보 보호를 위하여 필요하다고 인정하면 소관 법률에 따라 개인정보처리자에게 개인정보 처리 실태의 개선을 권고할 수 있다. 이 경우 권고를 받은 개인정보처리자는 이를 이행하기 위하여 성실하게 노력하여야 하며, 그 조치 결과를 관계 중앙행정기관의 장에게 알려야 한다.
④ 중앙행정기관, 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회는 그 소속 기관 및 소관 공공기관에 대하여 개인정보 보호에 관한 의견을 제시하거나 지도·점검을 할 수 있다.

제62조(침해 사실의 신고 등) ① 개인정보처리자가 개인정보를 처리할 때 개인정보에 관한 권리 또는 이익을 침해받은 사람은 보호위원회에 그 침해 사실을 신고할 수 있다. <개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>
② 보호위원회는 제1항에 따른 신고의 접수·처리 등에 관한 업무를 효율적으로 수행하기 위하여 대통령령으로 정하는 바에 따라 전문기관을 지정할 수 있다. 이 경우 전문기관은 개인정보침해 신고센터(이하 “신고센터”라 한다)를 설치·운영하여야 한다. <개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>
③ 신고센터는 다음 각 호의 업무를 수행한다.
1. 개인정보 처리와 관련한 신고의 접수·상담
2. 사실의 조사·확인 및 관계자의 의견 청취
3. 제1호 및 제2호에 따른 업무에 딸린 업무

④ 보호위원회는 제3항제2호의 사실 조사·확인 등의 업무를 효율적으로 하기 위하여 필요하면 「국가공무원법」 제32조의4에 따라 소속 공무원을 제2항에 따른 전문기관에 파견할 수 있다. <개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>

제63조(자료제출 요구 및 검사) ① 보호위원회는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보처리자에게 관계 물품·서류 등 자료를 제출하게 할 수 있다. <개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>

1. 이 법을 위반하는 사항을 발견하거나 혐의가 있음을 알게 된 경우
2. 이 법 위반에 대한 신고를 받거나 민원이 접수된 경우
3. 그 밖에 정보주체의 개인정보 보호를 위하여 필요한 경우로서 대통령령으로 정하는 경우

② 보호위원회는 개인정보처리자가 제1항에 따른 자료를 제출하지 아니하거나 이 법을 위반한 사실이 있다고 인정되면 소속 공무원으로 하여금 개인정보처리자 및 해당 법 위반 사실과 관련한 관계인의 사무소나 사업장에 출입하여 업무 상황, 장부 또는 서류 등을 검사하게 할 수 있다. 이 경우 검사를 하는 공무원은 그 권한을 나타내는 증표를 지니고 이를 관계인에게 내보여야 한다. <개정 2013. 3. 23., 2014. 11. 19., 2015. 7. 24., 2017. 7. 26., 2020. 2. 4.>

③ 관계 중앙행정기관의 장은 소관 법률에 따라 개인정보처리자에게 제1항에 따른 자료 제출을 요구하거나 개인정보처리자 및 해당 법 위반사실과 관련한 관계인에 대하여 제2항에 따른 검사를 할 수 있다. <개정 2015. 7. 24.>

④ 보호위원회는 이 법을 위반하는 사항을 발견하거나 혐의가 있음을 알게 된 경우에는 관계 중앙행정기관의 장(해당 중앙행정기관의 장의 지휘·감독을 받아 검사권한을 수행하는 법인이 있는 경우 그 법인을 말한다)에게 구체적인 범위를 정하여 개인정보처리자에 대한 검사를 요구할 수 있으며, 필요 시 보호위원회의 소속 공무원이 해당 검사에 공동으로 참여하도록 요청할 수 있다. 이 경우 그 요구를 받은 관계 중앙행정기관의 장은 특별한 사정이 없으면 이에 따라야 한다. <개정 2020. 2. 4.>

⑤ 보호위원회는 관계 중앙행정기관의 장(해당 중앙행정기관의 장의 지휘·감독을 받아 검사권한을 수행하는 법인이 있는 경우 그 법인을 말한다)에게 제4항에 따른 검사 결과와 관련하여 개인정보처리자에 대한 시정조치를 요청하거나, 처분 등에 대한 의견을 제시할 수 있다. <개정 2020. 2. 4.>

⑥ 제4항 및 제5항에 대한 방법과 절차 등에 관한 사항은 대통령령으로 정한다. <개정 2020. 2. 4.>

⑦ 보호위원회는 개인정보 침해사고의 예방과 효과적인 대응을 위하여 관계 중앙행정기관의 장과 합동으로 개인정보 보호실태를 점검할 수 있다. <신설 2015. 7. 24., 2017. 7. 26., 2020. 2. 4.>

⑧ 보호위원회와 관계 중앙행정기관의 장은 제1항 및 제2항에 따라 제출받거나 수집한 서류·자료 등을 이 법에 따른 경우를 제외하고는 제3자에게 제공하거나 일반에 공개해서

는 아니 된다. <신설 2020. 2. 4.>

⑨ 보호위원회와 관계 중앙행정기관의 장은 정보통신망을 통하여 자료의 제출 등을 받은 경우나 수집한 자료 등을 전자화한 경우에는 개인정보·영업비밀 등이 유출되지 아니하도록 제도적·기술적 보완조치를 하여야 한다. <신설 2020. 2. 4.>

제64조(시정조치 등) ① 보호위원회는 개인정보가 침해되었다고 판단할 상당한 근거가 있고 이를 방치할 경우 회복하기 어려운 피해가 발생할 우려가 있다고 인정되면 이 법을 위반한 자(중앙행정기관, 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회는 제외한다)에 대하여 다음 각 호에 해당하는 조치를 명할 수 있다. <개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>

1. 개인정보 침해행위의 중지
2. 개인정보 처리의 일시적인 정지
3. 그 밖에 개인정보의 보호 및 침해 방지를 위하여 필요한 조치

② 관계 중앙행정기관의 장은 개인정보가 침해되었다고 판단할 상당한 근거가 있고 이를 방치할 경우 회복하기 어려운 피해가 발생할 우려가 있다고 인정되면 소관 법률에 따라 개인정보처리자에 대하여 제1항 각 호에 해당하는 조치를 명할 수 있다.

③ 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회는 그 소속 기관 및 소관 공공기관이 이 법을 위반하였을 때에는 제1항 각 호에 해당하는 조치를 명할 수 있다.

④ 보호위원회는 중앙행정기관, 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회가 이 법을 위반하였을 때에는 해당 기관의 장에게 제1항 각 호에 해당하는 조치를 하도록 권고할 수 있다. 이 경우 권고를 받은 기관은 특별한 사유가 없으면 이를 존중하여야 한다.

제65조(고발 및 징계권고) ① 보호위원회는 개인정보처리자에게 이 법 등 개인정보 보호와 관련된 법규의 위반에 따른 범죄혐의가 있다고 인정될 만한 상당한 이유가 있을 때에는 관할 수사기관에 그 내용을 고발할 수 있다. <개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>

② 보호위원회는 이 법 등 개인정보 보호와 관련된 법규의 위반행위가 있다고 인정될 만한 상당한 이유가 있을 때에는 책임이 있는 자(대표자 및 책임있는 임원을 포함한다)를 징계할 것을 해당 개인정보처리자에게 권고할 수 있다. 이 경우 권고를 받은 사람은 이를 존중하여야 하며 그 결과를 보호위원회에 통보하여야 한다. <개정 2013. 3. 23., 2013. 8. 6., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>

③ 관계 중앙행정기관의 장은 소관 법률에 따라 개인정보처리자에 대하여 제1항에 따른 고발을 하거나 소속 기관·단체 등의 장에게 제2항에 따른 징계권고를 할 수 있다. 이 경우 제2항에 따른 권고를 받은 사람은 이를 존중하여야 하며 그 결과를 관계 중앙행정기관의 장에게 통보하여야 한다.

제66조(결과의 공표) ① 보호위원회는 제61조에 따른 개선권고, 제64조에 따른 시정조치 명령, 제65조에 따른 고발 또는 징계권고 및 제75조에 따른 과태료 부과의 내용 및 결과에

대하여 공표할 수 있다. <개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>
② 관계 중앙행정기관의 장은 소관 법률에 따라 제1항에 따른 공표를 할 수 있다.
③ 제1항 및 제2항에 따른 공표의 방법, 기준 및 절차 등은 대통령령으로 정한다.

제67조(연차보고) ① 보호위원회는 관계 기관 등으로부터 필요한 자료를 제출받아 매년 개인정보 보호시책의 수립 및 시행에 관한 보고서를 작성하여 정기국회 개회 전까지 국회에 제출(정보통신망에 의한 제출을 포함한다)하여야 한다.
② 제1항에 따른 보고서에는 다음 각 호의 내용이 포함되어야 한다. <개정 2016. 3. 29.>
1. 정보주체의 권리침해 및 그 구제현황
2. 개인정보 처리에 관한 실태조사 등의 결과
3. 개인정보 보호시책의 추진현황 및 실적
4. 개인정보 관련 해외의 입법 및 정책 동향
5. 주민등록번호 처리와 관련된 법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 감사원규칙의 제정·개정 현황
6. 그 밖에 개인정보 보호시책에 관하여 공개 또는 보고하여야 할 사항

제68조(권한의 위임·위탁) ① 이 법에 따른 보호위원회 또는 관계 중앙행정기관의 장의 권한은 그 일부를 대통령령으로 정하는 바에 따라 특별시장, 광역시장, 도지사, 특별자치도지사 또는 대통령령으로 정하는 전문기관에 위임하거나 위탁할 수 있다. <개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>
② 제1항에 따라 보호위원회 또는 관계 중앙행정기관의 장의 권한을 위임 또는 위탁받은 기관은 위임 또는 위탁받은 업무의 처리 결과를 보호위원회 또는 관계 중앙행정기관의 장에게 통보하여야 한다. <개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>
③ 보호위원회는 제1항에 따른 전문기관에 권한의 일부를 위임하거나 위탁하는 경우 해당 전문기관의 업무 수행을 위하여 필요한 경비를 출연할 수 있다. <개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>

제69조(벌칙 적용 시의 공무원 의제) ① 보호위원회의 위원 중 공무원이 아닌 위원 및 공무원이 아닌 직원은 「형법」이나 그 밖의 법률에 따른 벌칙을 적용할 때에는 공무원으로 본다. <신설 2020. 2. 4.>
② 보호위원회 또는 관계 중앙행정기관의 장의 권한을 위탁한 업무에 종사하는 관계 기관의 임직원은 「형법」 제129조부터 제132조까지의 규정을 적용할 때에는 공무원으로 본다. <신설 2020. 2. 4.>

제10장 벌칙 <개정 2020. 2. 4.>

제70조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처한다. <개정 2015. 7. 24.>

1. 공공기관의 개인정보 처리업무를 방해할 목적으로 공공기관에서 처리하고 있는 개인정보를 변경하거나 말소하여 공공기관의 업무 수행의 중단·마비 등 심각한 지장을 초래한 자
2. 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

제71조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다. <개정 2016. 3. 29., 2020. 2. 4.>

1. 제17조제1항제2호에 해당하지 아니함에도 같은 항 제1호를 위반하여 정보주체의 동의를 받지 아니하고 개인정보를 제3자에게 제공한 자 및 그 사정을 알고 개인정보를 제공받은 자
2. 제18조제1항·제2항(제39조의14에 따라 준용되는 경우를 포함한다), 제19조, 제26조제5항, 제27조제3항 또는 제28조의2를 위반하여 개인정보를 이용하거나 제3자에게 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자
3. 제23조제1항을 위반하여 민감정보를 처리한 자
4. 제24조제1항을 위반하여 고유식별정보를 처리한 자

4의2. 제28조의3을 위반하여 가명정보를 처리하거나 제3자에게 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 가명정보를 제공받은 자

4의3. 제28조의5제1항을 위반하여 특정 개인을 알아보기 위한 목적으로 가명정보를 처리한 자

4의4. 제36조제2항(제27조에 따라 정보통신서비스 제공자등으로부터 개인정보를 이전받은 자와 제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 정정·삭제 등 필요한 조치(제38조제2항에 따른 열람등요구에 따른 필요한 조치를 포함한다)를 하지 아니하고 개인정보를 이용하거나 이를 제3자에게 제공한 정보통신서비스 제공자등

4의5. 제39조의3제1항(제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 이용자의 동의를 받지 아니하고 개인정보를 수집한 자

4의6. 제39조의3제4항(제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 법정대리인의 동의를 받지 아니하거나 법정대리인이 동의하였는지를 확인하지 아니하고 만 14세 미만인 아동의 개인정보를 수집한 자

5. 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
6. 제59조제3호를 위반하여 다른 사람의 개인정보를 훼손, 멸실, 변경, 위조 또는 유출한 자

제72조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.

1. 제25조제5항을 위반하여 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비추는 자 또는 녹음기능을 사용한 자
2. 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
3. 제60조를 위반하여 직무상 알게 된 비밀을 누설하거나 직무상 목적 외에 이용한 자

제73조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 2년 이하의 징역 또는 2천만원 이하의 벌금에 처한다. <개정 2015. 7. 24., 2016. 3. 29., 2020. 2. 4.>

1. 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4제1항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 아니하여 개인정보를 분실·도난·유출·위조·변조 또는 훼손당한 자
1의2. 제21조제1항(제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보를 파기하지 아니한 정보통신서비스 제공자등
2. 제36조제2항을 위반하여 정정·삭제 등 필요한 조치를 하지 아니하고 개인정보를 계속 이용하거나 이를 제3자에게 제공한 자
3. 제37조제2항을 위반하여 개인정보의 처리를 정지하지 아니하고 계속 이용하거나 제3자에게 제공한 자

제74조(양벌규정) ① 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. 다만, 법인 또는 개인이 그 위반행위를 방지하기 위하여 해당 업무에 관하여 상당한 주의와 감독을 게을리하지 아니한 경우에는 그러하지 아니하다.

② 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. 다만, 법인 또는 개인이 그 위반행위를 방지하기 위하여 해당 업무에 관하여 상당한 주의와 감독을 게을리하지 아니한 경우에는 그러하지 아니하다.

제74조의2(몰수·추징 등) 제70조부터 제73조까지의 어느 하나에 해당하는 죄를 지은 자가 해당 위반행위와 관련하여 취득한 금품이나 그 밖의 이익은 몰수할 수 있으며, 이를 몰수할 수 없을 때에는 그 가액을 추징할 수 있다. 이 경우 몰수 또는 추징은 다른 벌칙에 부가하여 과할 수 있다.

[본조신설 2015. 7. 24.]

제75조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자에게는 5천만원 이하의 과태료를 부과한다. <개정 2017. 4. 18.>

1. 제15조제1항을 위반하여 개인정보를 수집한 자
2. 제22조제6항을 위반하여 법정대리인의 동의를 받지 아니한 자

3. 제25조제2항을 위반하여 영상정보처리기기를 설치·운영한 자

② 다음 각 호의 어느 하나에 해당하는 자에게는 3천만원 이하의 과태료를 부과한다. <개정 2013. 8. 6., 2014. 3. 24., 2015. 7. 24., 2016. 3. 29., 2017. 4. 18., 2020. 2. 4.>

1. 제15조제2항, 제17조제2항, 제18조제3항 또는 제26조제3항을 위반하여 정보주체에게 알려야 할 사항을 알리지 아니한 자
2. 제16조제3항 또는 제22조제5항을 위반하여 재화 또는 서비스의 제공을 거부한 자
3. 제20조제1항 또는 제2항을 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 아니한 자
4. 제21조제1항·제39조의6(제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보의 파기 등 필요한 조치를 하지 아니한 자

4의2. 제24조의2제1항을 위반하여 주민등록번호를 처리한 자

4의3. 제24조의2제2항을 위반하여 암호화 조치를 하지 아니한 자

5. 제24조의2제3항을 위반하여 정보주체가 주민등록번호를 사용하지 아니할 수 있는 방법을 제공하지 아니한 자
6. 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4제1항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 아니한 자
7. 제25조제1항을 위반하여 영상정보처리기기를 설치·운영한 자

7의2. 제28조의5제2항을 위반하여 개인을 알아볼 수 있는 정보가 생성되었음에도 이용을 중지하지 아니하거나 이를 회수·파기하지 아니한 자

7의3. 제32조의2제6항을 위반하여 인증을 받지 아니하였음에도 거짓으로 인증의 내용을 표시하거나 홍보한 자

8. 제34조제1항을 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 아니한 자
9. 제34조제3항을 위반하여 조치 결과를 신고하지 아니한 자
10. 제35조제3항을 위반하여 열람을 제한하거나 거절한 자
11. 제36조제2항을 위반하여 정정·삭제 등 필요한 조치를 하지 아니한 자
12. 제37조제4항을 위반하여 처리가 정지된 개인정보에 대하여 파기 등 필요한 조치를 하지 아니한 자

12의2. 제39조의3제3항(제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 서비스의 제공을 거부한 자

12의3. 제39조의4제1항(제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 이용자·보호위원회 및 전문기관에 통지 또는 신고하지 아니하거나 정당한 사유 없이 24시간을 경과하여 통지 또는 신고한 자

12의4. 제39조의4제3항을 위반하여 소명을 하지 아니하거나 거짓으로 한 자

12의5. 제39조의7제2항(제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보의 동의 철회·열람·정정 방법을 제공하지 아니한 자

12의6. 제39조의7제3항(제39조의14에 따라 준용되는 경우와 제27조에 따라 정보통신서비스 제공자등으로부터 개인정보를 이전받은 자를 포함한다)을 위반하여 필요한 조치를

하지 아니한 정보통신서비스 제공자등

12의7. 제39조의8제1항 본문(제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보의 이용내역을 통지하지 아니한 자

12의8. 제39조의12제4항(같은 조 제5항에 따라 준용되는 경우를 포함한다)을 위반하여 보호조치를 하지 아니한 자

13. 제64조제1항에 따른 시정명령에 따르지 아니한 자

③ 다음 각 호의 어느 하나에 해당하는 자에게는 2천만원 이하의 과태료를 부과한다. <신설 2020. 2. 4.>

1. 제39조의9제1항을 위반하여 보험 또는 공제 가입, 준비금 적립 등 필요한 조치를 하지 아니한 자

2. 제39조의11제1항을 위반하여 국내대리인을 지정하지 아니한 자

3. 제39조의12제2항 단서를 위반하여 제39조의12제3항 각 호의 사항 모두를 공개하거나 이용자에게 알리지 아니하고 이용자의 개인정보를 국외에 처리위탁·보관한 자

④ 다음 각 호의 어느 하나에 해당하는 자에게는 1천만원 이하의 과태료를 부과한다. <개정 2017. 4. 18., 2020. 2. 4.>

1. 제21조제3항을 위반하여 개인정보를 분리하여 저장·관리하지 아니한 자

2. 제22조제1항부터 제4항까지의 규정을 위반하여 동의를 받은 자

3. 제25조제4항을 위반하여 안내판 설치 등 필요한 조치를 하지 아니한 자

4. 제26조제1항을 위반하여 업무 위탁 시 같은 항 각 호의 내용이 포함된 문서에 의하지 아니한 자

5. 제26조제2항을 위반하여 위탁하는 업무의 내용과 수탁자를 공개하지 아니한 자

6. 제27조제1항 또는 제2항을 위반하여 정보주체에게 개인정보의 이전 사실을 알리지 아니한 자

6의2. 제28조의4제2항을 위반하여 관련 기록을 작성하여 보관하지 아니한 자

7. 제30조제1항 또는 제2항을 위반하여 개인정보 처리방침을 정하지 아니하거나 이를 공개하지 아니한 자

8. 제31조제1항을 위반하여 개인정보 보호책임자를 지정하지 아니한 자

9. 제35조제3항·제4항, 제36조제2항·제4항 또는 제37조제3항을 위반하여 정보주체에게 알려야 할 사항을 알리지 아니한 자

10. 제63조제1항에 따른 관계 물품·서류 등 자료를 제출하지 아니하거나 거짓으로 제출한 자

11. 제63조제2항에 따른 출입·검사를 거부·방해 또는 기피한 자

⑤ 제1항부터 제4항까지의 규정에 따른 과태료는 대통령령으로 정하는 바에 따라 보호위원회와 관계 중앙행정기관의 장이 부과·징수한다. 이 경우 관계 중앙행정기관의 장은 소관 분야의 개인정보처리자에게 과태료를 부과·징수한다. <개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26., 2020. 2. 4.>

제76조(과태료에 관한 규정 적용의 특례) 제75조의 과태료에 관한 규정을 적용할 때 제34조의2에 따라 과징금을 부과한 행위에 대하여는 과태료를 부과할 수 없다.
[본조신설 2013. 8. 6.]

부칙 <제16930호, 2020. 2. 4.>

제1조(시행일) 이 법은 공포 후 6개월이 경과한 날부터 시행한다.

제2조(위원 임기에 관한 경과조치) 이 법 시행 당시 종전의 규정에 따라 임명된 보호위원회의 위원의 임기는 이 법 시행 전날 만료된 것으로 본다.

제3조(기능조정에 따른 소관 사무 등에 관한 경과조치) ① 이 법 시행 당시 「방송통신위원회의 설치 및 운영에 관한 법률」 제11조제1항의 방송통신위원회의 소관사무 중 개인정보 보호에 해당하는 사무는 보호위원회가 승계한다.

② 이 법 시행 당시 행정안전부장관의 소관 사무 중 제7조의8의 개정규정에 따른 사무는 보호위원회가 승계한다.

③ 이 법 시행 전에 행정안전부장관이 행한 고시·행정처분, 그 밖에 행정안전부장관의 행위와 행정안전부장관에 대한 신청·신고, 그 밖의 행위 중 그 소관이 행정안전부장관으로부터 보호위원회로 이관되는 사항에 관한 행위는 보호위원회의 행위 또는 보호위원회에 대한 행위로 본다.

④ 이 법 시행 전에 방송통신위원회가 행한 고시·행정처분, 그 밖의 행위와 신고 등 방송통신위원회에 대한 행위 중 그 소관이 방송통신위원회에서 보호위원회로 이관되는 사항에 관한 행위는 이 법에 따른 보호위원회의 행위 또는 보호위원회에 대한 행위로 본다.

⑤ 이 법 시행 당시 행정안전부·방송통신위원회 소속 공무원 중 대통령령으로 정하는 공무원은 이 법에 따른 보호위원회 소속 공무원으로 본다.

제4조(보호위원회에 관한 경과조치) ① 이 법 시행 당시 종전의 규정에 따른 보호위원회의 행위나 보호위원회에 대한 행위는 이 법에 따른 보호위원회의 행위나 보호위원회에 대한 행위로 본다.

제5조(개인정보보호 관리체계 인증기관 등에 관한 경과조치) ① 이 법 시행 당시 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 "「정보통신망법」"이라 한다) 제47조의3에 따라 인증기관 또는 심사기관으로 지정받은 자는 이 법 제32조의2에 따라 전문기관으로 지정받은 것으로 본다.

② 이 법 시행 당시 「정보통신망법」 제47조의3에 따라 개인정보보호 관리체계 인증을 받거나 인증심사원 자격을 부여받은 자는 이 법 제32조의2에 따라 개인정보보호 관리체계 인증을 받거나 인증심사원 자격을 부여받은 것으로 본다.

제6조(권한의 위임·위탁에 관한 경과조치) 이 법 시행 당시 종전의 규정에 따라 행정안전부장관의 권한 일부를 위임 또는 위탁받은 특별시장, 광역시장, 도지사, 특별자치도지사, 특별자치시장 또는 전문기관은 이 법에 따라 보호위원회의 권한 일부를 위임 또는 위탁받은 것으로 본다.

제7조(벌칙 및 과태료에 관한 경과조치) 이 법 시행 전의 행위에 대한 벌칙 및 과태료의 적용은 종전의 규정에 따른다.

제8조(과징금 부과에 관한 경과조치) 이 법 시행 전에 종료된 행위에 대한 과징금의 부과는 종전의 규정에 따른다.

제9조(다른 법률의 개정) ① 방송통신위원회의 설치 및 운영에 관한 법률 일부를 다음과 같이 개정한다.

제11조제1항제2호 중 “개인정보보호윤리”를 “인터넷 윤리, 건전한 인터넷 이용환경 조성”으로 한다.

② 신용정보의 이용 및 보호에 관한 법률 일부를 다음과 같이 개정한다.

제39조의2제4항 중 “행정안전부장관에게”를 “개인정보 보호위원회에”로 한다.

③ 정부조직법 일부를 다음과 같이 개정한다.

제34조제1항 중 “전자정부, 개인정보보호”를 “전자정부”로 한다.

④ 주민등록법 일부를 다음과 같이 개정한다.

제7조의5제6항제1호 중 “관계 행정기관(「개인정보 보호법」 제7조에 따른 개인정보 보호위원회를 포함한다)”을 “관계 행정기관”으로 한다.

제10조(다른 법령과의 관계) ① 이 법 시행 당시 다른 법령(이 법 시행 전에 공포되었으나 시행일이 도래하지 아니한 법령을 포함한다)에서 이 법에 따라 보호위원회가 승계하는 방송통신위원회 및 행정안전부의 사무와 관련하여 “방송통신위원회” 또는 “방송통신위원회 위원장”을 인용한 경우에는 그 법령에서 규정한 내용에 따라 “보호위원회” 또는 “보호위원회 위원장”을 인용한 것으로, “방송통신위원회 소속 공무원”을 인용한 경우에는 “보호위원회 소속 공무원”을 인용한 것으로 보며, “행정안전부” 또는 “행정안전부장관”을 인용한 경우에는 그 법령에서 규정한 내용에 따라 “보호위원회” 또는 “보호위원회 위원장”을 인용한 것으로, “행정안전부 소속 공무원”을 인용한 경우에는 “보호위원회 소속 공무원”을 인용한 것으로 본다.

② 이 법 시행 당시 다른 법령에서 종전의 「정보통신망법」 또는 그 규정을 인용하고 있는 경우 이 법에 그에 해당하는 규정이 있는 때에는 이 법 또는 이 법의 해당 규정을 인용한 것으로 본다.

(개인정보보호위원회) 표준 개인정보 보호지침

[시행 2020. 8. 11.] [개인정보보호위원회고시 제2020-1호, 2020. 8. 11., 제정.]

제1장 총칙

제1조(목적) 이 지침은 「개인정보 보호법」(이하 "법"이라 한다) 제12조제1항에 따른 개인정보의 처리에 관한 기준, 개인정보 침해의 유형 및 예방조치 등에 관한 세부적인 사항을 규정함을 목적으로 한다.

제2조(용어의 정의) 이 지침에서 사용하는 용어의 뜻은 다음과 같다.

1. "개인정보 처리"란 개인정보를 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.
2. "개인정보처리자"란 업무를 목적으로 법 제2조제4호에 따른 개인정보파일을 운용하기 위하여 개인정보를 처리하는 모든 공공기관, 영리목적의 사업자, 협회·동창회 등 비영리 기관·단체, 개인 등을 말한다.
3. "공공기관"이란 법 제2조제6호 및 「개인정보 보호법 시행령」(이하 "영"이라 한다) 제2조에 따른 기관을 말한다.
4. "친목단체"란 학교, 지역, 기업, 인터넷 커뮤니티 등을 단위로 구성되는 것으로서 자원봉사, 취미, 정치, 종교 등 공통의 관심사나 목표를 가진 사람간의 친목도모를 위한 각종 동창회, 동호회, 향우회, 반상회 및 동아리 등의 모임을 말한다.
5. "개인정보 보호책임자"란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지는 자로서 영 제32조제2항에 해당하는 자를 말한다.
6. "개인정보취급자"란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을 말한다.
7. "개인정보처리시스템"이란 데이터베이스 시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 응용시스템을 말한다.
8. "영상정보처리기기"란 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 일체의 장치로서 영 제3조에 따른 폐쇄회로 텔레비전 및 네트워크 카메라를 말한다.
9. "개인영상정보"란 영상정보처리기기에 의하여 촬영·처리되는 영상정보 중 개인의 초상, 행동 등과 관련된 영상으로서 해당 개인을 식별할 수 있는 정보를 말한다.
10. "영상정보처리기기운영자"란 법 제25조제1항 각 호에 따라 영상정보처리기기를 설치·운영하는 자를 말한다.
11. "공개된 장소"란 공원, 도로, 지하철, 상가 내부, 주차장 등 불특정 또는 다수가 접근하거나 통행하는 데에 제한을 받지 아니하는 장소를 말한다.

제3조(적용범위) 이 지침은 전자적 파일과 인쇄물, 서면 등 모든 형태의 개인정보파일을 운용하는 개인정보처리자에게 적용된다.

제4조(개인정보 보호 원칙) ① 개인정보처리자는 개인정보 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.

② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.

③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성과 최신성을 유지하도록 하여야 하고, 개인정보를 처리하는 과정에서 고의 또는 과실로 부당하게 변경 또는 훼손되지 않도록 하여야 한다.

④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 그에 상응하는 적절한 관리적·기술적 및 물리적 보호조치를 통하여 개인정보를 안전하게 관리하여야 한다.

⑤ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리가 보장될 수 있도록 합리적인 절차와 방법 등을 마련하여야 한다.

⑥ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적법하게 개인정보를 처리하는 경우에도 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.

⑦ 개인정보처리자는 개인정보를 적법하게 수집한 경우에도 익명에 의하여 업무 목적을 달성할 수 있으면 개인정보를 익명에 의하여 처리될 수 있도록 하여야 한다.

⑧ 개인정보처리자는 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.

제5조(다른 지침과의 관계) 중앙행정기관의 장이 소관 분야의 개인정보 처리와 관련한 개인정보 보호지침을 정하는 경우에는 이 지침에 부합되도록 하여야 한다.

제2장 개인정보 처리 기준

제1절 개인정보의 처리

제6조(개인정보의 수집·이용) ① 개인정보의 "수집"이란 정보주체로부터 직접 이름, 주소, 전화번호 등의 개인정보를 제공받는 것뿐만 아니라 정보주체에 관한 모든 형태의 개인정보를 취득하는 것을 말한다.

② 개인정보처리자는 다음 각 호의 경우에 개인정보를 수집할 수 있으며, 그 수집 목적의 범위에서 이용할 수 있다.

1. 정보주체로부터 사전에 동의를 받은 경우
2. 법률에서 개인정보를 수집·이용할 수 있음을 구체적으로 명시하거나 허용하고 있는 경우

3. 법령에서 개인정보처리자에게 구체적인 의무를 부과하고 있고, 개인정보처리자가 개인정보를 수집·이용하지 않고는 그 의무를 이행하는 것이 불가능하거나 현저히 곤란한 경우
4. 공공기관이 개인정보를 수집·이용하지 않고는 법령 등에서 정한 소관 업무를 수행하는 것이 불가능하거나 현저히 곤란한 경우
5. 개인정보를 수집·이용하지 않고는 정보주체와 계약을 체결하고, 체결된 계약의 내용에 따른 의무를 이행하는 것이 불가능하거나 현저히 곤란한 경우
6. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자(정보주체를 제외한 그 밖의 모든 자를 말한다)의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
7. 개인정보처리자가 법령 또는 정보주체와의 계약 등에 따른 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 다만, 이 경우 개인정보의 수집·이용은 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니한 경우에 한한다.

③ 개인정보처리자는 정보주체로부터 직접 명함 또는 그와 유사한 매체(이하 "명함등"이라 함)를 제공받음으로써 개인정보를 수집하는 경우 명함등을 제공하는 정황 등에 비추어 사회통념상 동의 의사가 있었다고 인정되는 범위 내에서만 이용할 수 있다.

④ 개인정보처리자는 인터넷 홈페이지 등 공개된 매체 또는 장소(이하 "인터넷 홈페이지 등"이라 함)에서 개인정보를 수집하는 경우 정보주체의 동의 의사가 명확히 표시되거나 인터넷 홈페이지등의 표시 내용에 비추어 사회통념상 동의 의사가 있었다고 인정되는 범위 내에서만 이용할 수 있다.

⑤ 개인정보처리자는 계약 등의 상대방인 정보주체가 대리인을 통하여 법률행위 또는 의사표시를 하는 경우 대리인의 대리권 확인을 위한 목적으로만 대리인의 개인정보를 수집·이용할 수 있다.

⑥ 근로자와 사용자가 근로계약을 체결하는 경우 「근로기준법」에 따른 임금지급, 교육, 증명서 발급, 근로자 복지제공을 위하여 근로자의 동의 없이 개인정보를 수집·이용할 수 있다.

제7조(개인정보의 제공) ① 개인정보의 "제공"이란 개인정보의 저장 매체나 개인정보가 담긴 출력물·책자 등을 물리적으로 이전하거나 네트워크를 통한 개인정보의 전송, 개인정보에 대한 제3자의 접근권한 부여, 개인정보처리자와 제3자의 개인정보 공유 등 개인정보의 이전 또는 공동 이용 상태를 초래하는 모든 행위를 말한다.

② 법 제17조의 "제3자"란 정보주체와 정보주체에 관한 개인정보를 수집·보유하고 있는 개인정보처리자를 제외한 모든 자를 의미하며, 정보주체의 대리인(명백히 대리의 범위 내에 있는 것에 한한다)과 법 제26조제2항에 따른 수탁자는 제외한다(이하 같다).

③ 개인정보처리자가 법 제17조제2항제1호에 따라 정보주체에게 개인정보를 제공받는 자

를 알리는 경우에는 그 성명(법인 또는 단체인 경우에는 그 명칭)과 연락처를 함께 알려야 한다.

제8조(개인정보의 목적 외 이용·제공) ① 개인정보처리자가 법 제18조제2항에 따라 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 개인정보를 제공받는 자에게 이용 목적, 이용 방법, 이용 기간, 이용 형태 등을 제한하거나, 개인정보의 안전성 확보를 위하여 필요한 구체적인 조치를 마련하도록 문서(전자문서를 포함한다. 이하 같다)로 요청하여야 한다. 이 경우 요청을 받은 자는 그에 따른 조치를 취하고 그 사실을 개인정보를 제공한 개인정보처리자에게 문서로 알려야 한다.

② 법 제18조제2항에 따라 개인정보를 목적 외의 용도로 제3자에게 제공하는 자는 해당 개인정보를 제공받는 자와 개인정보의 안전성 확보 조치에 관한 책임관계를 명확히 하여야 한다.

③ 개인정보처리자가 법 제18조제3항제1호에 따라 정보주체에게 개인정보를 제공받는 자를 알리는 경우에는 그 성명(법인 또는 단체인 경우에는 그 명칭)과 연락처를 함께 알려야 한다.

제9조(개인정보 수집 출처 등 고지) ① 개인정보처리자가 정보주체 이외로부터 수집한 개인정보를 처리하는 때에는 정당한 사유가 없는 한 정보주체의 요구가 있은 날로부터 3일 이내에 법 제20조제1항 각 호의 모든 사항을 정보주체에게 알려야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니 하다.

1. 고지를 요구하는 대상이 되는 개인정보가 법 제32조제2항 각 호의 어느 하나에 해당하는 개인정보파일에 포함되어 있는 경우
2. 고지로 인하여 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우

② 개인정보처리자는 제1항 단서에 따라 제1항 전문에 따른 정보주체의 요구를 거부하는 경우에는 정당한 사유가 없는 한 정보주체의 요구가 있은 날로부터 3일 이내에 그 거부의 근거와 사유를 정보주체에게 알려야 한다.

제10조(개인정보의 파기방법 및 절차) ① 개인정보처리자는 개인정보의 보유 기간이 경과하거나 개인정보의 처리 목적 달성, 해당 서비스의 폐지, 사업의 종료 등 그 개인정보가 불필요하게 되었을 때에는 정당한 사유가 없는 한 그로부터 5일 이내에 그 개인정보를 파기하여야 한다.

② 영 제16조제1항제1호의 '복원이 불가능한 방법'이란 현재의 기술수준에서 사회통념상 적정한 비용으로 파기한 개인정보의 복원이 불가능하도록 조치하는 방법을 말한다.

③ 개인정보처리자는 개인정보의 파기에 관한 사항을 기록·관리하여야 한다.

④ 개인정보 보호책임자는 개인정보 파기 시행 후 파기 결과를 확인하여야 한다.

⑤ 개인정보처리자 중 공공기관의 개인정보파일 파기에 관하여는 제55조 및 제56조를 적용한다.

제11조(법령에 따른 개인정보의 보존) ① 개인정보처리자가 법 제21조제1항 단서에 따라 법

령에 근거하여 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 물리적 또는 기술적 방법으로 분리하여서 저장·관리하여야 한다.

② 제1항에 따라 개인정보를 분리하여 저장·관리하는 경우에는 개인정보 처리방침 등을 통하여 법령에 근거하여 해당 개인정보 또는 개인정보파일을 저장·관리한다는 점을 정보주체가 알 수 있도록 하여야 한다.

제12조(동의를 받는 방법) ① 개인정보처리자가 개인정보의 처리에 대하여 정보주체의 동의를 받을 때에는 정보주체의 동의 없이 처리할 수 있는 개인정보와 정보주체의 동의가 필요한 개인정보를 구분하여야 하며, 정보주체의 동의는 동의가 필요한 개인정보에 한한다. 이 경우 동의 없이 처리할 수 있는 개인정보라는 입증책임은 개인정보처리자가 부담한다.

② 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체에게 법 제18조제3항 각 호의 사항을 알리고 동의를 받아야 한다.

1. 개인정보를 수집·이용하고자 하는 경우로서 법 제15조제1항제2호 내지 제6호에 해당하지 않은 경우
2. 법 제18조제2항에 따라 개인정보를 수집 목적 외의 용도로 이용하거나 제공하고자 하는 경우
3. 법 제22조제3항에 해당하여 정보주체에게 재화나 서비스를 홍보하거나 판매를 권유하고자 하는 경우
4. 주민등록번호 외의 고유식별정보 처리가 필요한 경우로서 법령에 고유식별정보 처리 근거가 없는 경우
5. 민감정보를 처리하고자 하는 경우로서 법령에 민감정보 처리 근거가 없는 경우

③ 개인정보처리자는 제2항 각 호에 해당하여 개인정보를 처리하고자 하는 경우에는 정보주체에게 동의 또는 동의 거부를 선택할 수 있음을 명시적으로 알려야 한다.

④ 개인정보처리자는 법 제15조제1항제2호 내지 제6호에 따라 정보주체의 동의 없이 개인정보를 수집하는 경우에는 개인정보를 수집할 수 있는 법적 근거 등을 정보주체에게 알리기 위해 노력하여야 한다.

⑤ 개인정보처리자가 영 제17조제1항제2호의 규정에 따라 전화에 의한 동의와 관련하여 통화내용을 녹취할 때에는 녹취사실을 정보주체에게 알려야 한다.

⑥ 개인정보처리자가 친목단체를 운영하기 위하여 다음 각 호의 어느 하나에 해당하는 개인정보를 수집하는 경우에는 정보주체의 동의 없이 개인정보를 수집·이용할 수 있다.

1. 친목단체의 가입을 위한 성명, 연락처 및 친목단체의 회칙으로 정한 공통의 관심사나 목표와 관련된 인적 사항
2. 친목단체의 회비 등 친목유지를 위해 필요한 비용의 납부현황에 관한 사항
3. 친목단체의 활동에 대한 구성원의 참석여부 및 활동내용에 관한 사항
4. 기타 친목단체의 구성원 상호 간의 친교와 화합을 위해 구성원이 다른 구성원에게 알리기를 원하는 생일, 취향 및 가족의 애경사 등에 관한 사항

⑦ 개인정보처리자가 정보주체의 동의를 받기 위하여 동의서를 작성하는 경우에는 「개인

정보 수집·제공 동의서 작성 가이드라인」을 준수하여야 한다.

제13조(법정대리인의 동의) ① 영 제17조제3항에 따라 개인정보처리자가 법정대리인의 성명·연락처를 수집할 때에는 해당 아동에게 자신의 신분과 연락처, 법정대리인의 성명과 연락처를 수집하고자 하는 이유를 알려야 한다.

② 개인정보처리자는 법 제22조제5항에 따라 수집한 법정대리인의 개인정보를 법정대리인의 동의를 얻기 위한 목적으로만 이용하여야 하며, 법정대리인의 동의 거부가 있거나 법정대리인의 동의 의사가 확인되지 않는 경우 수집일로부터 5일 이내에 파기해야 한다.

제14조(정보주체의 사전 동의를 받을 수 없는 경우) 개인정보처리자가 법 제15조제1항제5호 및 법 제18조제2항제3호에 따라 정보주체의 사전 동의 없이 개인정보를 수집·이용 또는 제공한 경우 당해 사유가 해소된 때에는 개인정보의 처리를 즉시 중단하여야 하며, 정보주체에게 사전 동의 없이 개인정보를 수집·이용 또는 제공한 사실과 그 사유 및 이용내역을 알려야 한다.

제15조(개인정보취급자에 대한 감독) ① 개인정보처리자는 개인정보취급자를 업무상 필요한 한도 내에서 최소한으로 두어야 하며, 개인정보취급자의 개인정보 처리 범위를 업무상 필요한 한도 내에서 최소한으로 제한하여야 한다.

② 개인정보처리자는 개인정보 처리시스템에 대한 접근권한을 업무의 성격에 따라 당해 업무수행에 필요한 최소한의 범위로 업무담당자에게 차등 부여하고 접근권한을 관리하기 위한 조치를 취해야 한다.

③ 개인정보처리자는 개인정보취급자에게 보안서약서를 제출하도록 하는 등 적절한 관리·감독을 해야 하며, 인사이동 등에 따라 개인정보취급자의 업무가 변경되는 경우에는 개인정보에 대한 접근권한을 변경 또는 말소해야 한다.

제2절 개인정보 처리의 위탁

제16조(수탁자의 선정 시 고려사항) 개인정보의 처리 업무를 위탁하는 개인정보처리자(이하 "위탁자"라 한다)가 개인정보 처리 업무를 위탁받아 처리하는 자(이하 "수탁자"라 한다)를 선정할 때에는 인력과 물적 시설, 재정 부담능력, 기술 보유의 정도, 책임능력 등 개인정보 처리 및 보호 역량을 종합적으로 고려하여야 한다.

제17조(개인정보 보호 조치의무) 수탁자는 위탁받은 개인정보를 보호하기 위하여 「개인정보의 안전성 확보조치 기준 고시」에 따른 관리적·기술적·물리적 조치를 하여야 한다.

제3절 개인정보 처리방침 작성

제18조(개인정보 처리방침의 작성기준 등) ① 개인정보처리자가 개인정보 처리방침을 작성하는 때에는 법 제30조제1항 각 호 및 영 제31조제1항 각 호의 사항을 명시적으로 구분하되, 알기 쉬운 용어로 구체적이고 명확하게 표현하여야 한다.

② 개인정보처리자는 처리하는 개인정보가 개인정보의 처리 목적에 필요한 최소한이라는 점을 밝혀야 한다.

제19조(개인정보 처리방침의 기재사항) 개인정보처리자가 개인정보 처리방침을 작성할 때에는 법 제30조제1항에 따라 다음 각 호의 사항을 모두 포함하여야 한다.

1. 개인정보의 처리 목적
2. 처리하는 개인정보의 항목
3. 개인정보의 처리 및 보유 기간
4. 개인정보의 제3자 제공에 관한 사항(해당하는 경우에만 정한다)
5. 개인정보의 파기에 관한 사항
6. 개인정보 처리 수탁자 담당자 연락처, 수탁자의 관리 현황 점검 결과 등 개인정보처리 위탁에 관한 사항(해당하는 경우에만 정한다)
7. 영 제30조제1항에 따른 개인정보의 안전성 확보조치에 관한 사항
8. 개인정보의 열람, 정정·삭제, 처리정지 요구권 등 정보주체의 권리·의무 및 그 행사방법에 관한 사항
9. 개인정보 처리방침의 변경에 관한 사항
10. 개인정보 보호책임자에 관한 사항
11. 개인정보의 열람청구를 접수·처리하는 부서
12. 정보주체의 권익침해에 대한 구제방법

제20조(개인정보 처리방침의 공개) ① 개인정보처리자가 법 제30조제2항에 따라 개인정보 처리방침을 수립하는 경우에는 인터넷 홈페이지를 통해 지속적으로 게재하여야 하며, 이 경우 "개인정보 처리방침"이라는 명칭을 사용하되, 글자 크기, 색상 등을 활용하여 다른 고지사항과 구분함으로써 정보주체가 쉽게 확인할 수 있도록 하여야 한다.

② 개인정보처리자가 인터넷 홈페이지를 운영하지 않는 경우 또는 인터넷 홈페이지 관리상의 하자가 있는 경우에는 영 제31조제3항 각 호의 어느 하나 이상의 방법으로 개인정보 처리방침을 공개하여야 한다. 이 경우에도 "개인정보 처리방침"이라는 명칭을 사용하되, 글자 크기, 색상 등을 활용하여 다른 고지사항과 구분함으로써 정보주체가 쉽게 확인할 수 있도록 하여야 한다.

③ 개인정보처리자가 영 제31조제3항제3호의 방법으로 개인정보 처리방침을 공개하는 경우에는 간행물·소식지·홍보지·청구서 등이 발행될 때마다 계속하여 게재하여야 한다.

제21조(개인정보 처리방침의 변경) 개인정보처리자가 개인정보 처리방침을 변경하는 경우에는 변경 및 시행의 시기, 변경된 내용을 지속적으로 공개하여야 하며, 변경된 내용은 정보주체가 쉽게 확인할 수 있도록 변경 전·후를 비교하여 공개하여야 한다.

제4절 개인정보 보호책임자

제22조(개인정보 보호책임자의 공개) ① 개인정보처리자가 개인정보 보호책임자를 지정하거나 변경하는 경우 개인정보 보호책임자의 지정 및 변경 사실, 성명과 부서의 명칭, 전화번호 등 연락처를 공개하여야 한다.

② 개인정보처리자는 개인정보 보호책임자를 공개하는 경우 개인정보 보호와 관련한 고충

처리 및 상담을 실제로 처리할 수 있는 연락처를 공개하여야 한다. 이 경우 개인정보 보호책임자와 개인정보 보호 업무를 처리하는 담당자의 성명, 부서의 명칭, 전화번호 등 연락처를 함께 공개할 수 있다.

제23조(개인정보 보호책임자의 교육) 영 제32조제4항에 따라 보호위원회가 개설 운영할 수 있는 개인정보 보호책임자에 대한 교육의 내용은 다음 각 호와 같다.

1. 개인정보 보호 관련 법령 및 제도의 내용
2. 법 제31조제2항 및 영 제32조제1항 각 호의 업무수행에 필요한 사항
3. 그 밖에 개인정보처리자의 개인정보 보호를 위하여 필요한 사항

제24조(교육계획의 수립 및 시행) ① 보호위원회는 매년 초 당해 연도 개인정보 보호책임자 교육계획을 수립하여 시행한다.

② 보호위원회는 제1항의 교육계획에 따라 사단법인 한국개인정보보호협의회 등의 단체에 개인정보 보호책임자 교육을 실시하게 할 수 있다.

③ 보호위원회는 개인정보 보호책임자가 지리적·경제적 여건에 구애받지 않고 편리하게 교육을 받은 수 있는 여건 조성을 위해 노력하여야 한다.

제5절 개인정보 유출 통지 및 신고 등

제25조(개인정보의 유출) 개인정보의 유출은 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고, 정보주체의 개인정보에 대하여 개인정보처리자가 통제를 상실하거나 권한 없는 자의 접근을 허용한 것으로서 다음 각 호의 어느 하나에 해당하는 경우를 말한다.

1. 개인정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터 등을 분실하거나 도난당한 경우
2. 개인정보가 저장된 데이터베이스 등 개인정보처리시스템에 정상적인 권한이 없는 자가 접근한 경우
3. 개인정보처리자의 고의 또는 과실로 인해 개인정보가 포함된 파일 또는 종이문서, 기타 저장 매체가 권한이 없는 자에게 잘못 전달된 경우
4. 기타 권한이 없는 자에게 개인정보가 전달된 경우

제26조(유출 통지시기 및 항목) ① 개인정보처리자는 개인정보가 유출되었음을 알게 된 때에는 정당한 사유가 없는 한 5일 이내에 해당 정보주체에게 다음 각 호의 사항을 알려야 한다. 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 그로부터 5일 이내에 정보주체에게 알릴 수 있다.

1. 유출된 개인정보의 항목
2. 유출된 시점과 그 경위
3. 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
4. 개인정보처리자의 대응조치 및 피해구제절차

5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

② 개인정보처리자는 제1항 각 호의 사항을 모두 확인하기 어려운 경우에는 정보주체에게 다음 각 호의 사실만을 우선 알리고, 추후 확인되는 즉시 알릴 수 있다.

1. 정보주체에게 유출이 발생한 사실
2. 제1항의 통지항목 중 확인된 사항

③ 개인정보처리자는 개인정보 유출 사고를 인지하지 못해 유출 사고가 발생한 시점으로부터 5일 이내에 해당 정보주체에게 개인정보 유출 통지를 하지 아니한 경우에는 실제 유출 사고를 알게 된 시점을 입증하여야 한다.

제27조(유출 통지방법) ① 개인정보처리자는 정보주체에게 제26조제1항 각 호의 사항을 통지할 때에는 서면, 전자우편, 모사전송, 전화, 휴대전화 문자전송 또는 이와 유사한 방법을 통하여 지체 없이 정보주체에게 알려야 한다.

② 개인정보처리자는 제1항의 통지방법과 동시에, 홈페이지 등을 통하여 제26조제1항 각 호의 사항을 공개할 수 있다.

제28조(개인정보 유출신고 등) ① 개인정보처리자는 1천명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 정보주체에 대한 통지 및 조치결과를 5일 이내에 보호위원회 또는 영 제39조제2항의 전문기관에게 신고하여야 한다.

② 제1항에 따른 신고는 별지 제1호서식에 따른 개인정보 유출신고서를 통하여 하여야 한다.

③ 개인정보처리자는 전자우편, 팩스 또는 영 제39조제2항에 따른 전문기관의 인터넷 사이트를 통하여 유출신고를 할 시간적 여유가 없거나 그밖에 특별한 사정이 있는 때에는 먼저 전화를 통하여 제26조제1항의 사항을 신고한 후, 별지 제1호서식에 따른 개인정보 유출신고서를 제출할 수 있다.

④ 개인정보처리자는 1천명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 제26조제1항에 따른 통지와 함께 인터넷 홈페이지 등에 정보주체가 알아보기 쉽도록 제26조제1항 각 호의 사항을 7일 이상 게재하여야 한다.

제29조(개인정보 유출 사고 대응 매뉴얼 등) ① 다음 각 호의 어느 하나에 해당하는 개인정보처리자는 유출 사고 발생 시 신속한 대응을 통해 피해 발생을 최소화하기 위해 「개인정보 유출 사고 대응 매뉴얼」을 마련하여야 한다.

1. 법 제2조제6호에 따른 공공기관
2. 그 밖에 1천명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리자

② 제1항에 따른 개인정보 유출 사고 대응 매뉴얼에는 유출 통지·조회 절차, 영업점·인터넷회선 확충 등 고객 민원 대응조치, 현장 혼잡 최소화 조치, 고객불안 해소조치, 피해자 구제조치 등을 포함하여야 한다.

③ 개인정보처리자는 개인정보 유출에 따른 피해복구 조치 등을 수행함에 있어 정보주체의 불편과 경제적 부담을 최소화할 수 있도록 노력하여야 한다.

제30조(개인정보 침해 사실의 신고 처리 등) ① 개인정보처리자의 개인정보 처리로 인하여 개

인정보에 관한 권리 또는 이익을 침해받은 사람은 법 제62조제2항에 따른 개인정보침해 신고센터에 침해 사실을 신고할 수 있다.

② 제1항에 따른 개인정보침해 신고센터는 다음 각 호의 업무를 수행한다.

1. 개인정보 처리와 관련한 신고의 접수·상담
2. 개인정보 침해 신고에 대한 사실 조사·확인 및 관계자의 의견 청취
3. 개인정보처리자에 대한 개인정보 침해 사실 안내 및 시정 유도
4. 사실 조사 결과가 정보주체의 권리 또는 이익 침해 사실이 없는 것으로 판단되는 경우 신고의 종결 처리
5. 법 제43조에 따른 개인정보 분쟁조정위원회 조정 안내 등을 통한 고충 해소 지원

제6절 정보주체의 권리 보장

제31조(개인정보 열람 연기 사유의 소멸) ① 개인정보처리자가 법 제35조제3항 후문에 따라 개인정보의 열람을 연기한 후 그 사유가 소멸한 경우에는 정당한 사유가 없는 한 사유가 소멸한 날로부터 10일 이내에 열람하도록 하여야 한다.

② 정보주체로부터 영 제41조제1항제4호의 규정에 따른 개인정보의 제3자 제공 현황의 열람청구를 받은 개인정보처리자는 국가안보에 긴요한 사안으로 법 제35조제4항제3호마목의 규정에 따른 업무를 수행하는데 중대한 지장을 초래하는 경우, 제3자에게 열람청구의 허용 또는 제한, 거부와 관련한 의견을 조회하여 결정할 수 있다.

제32조(개인정보의 정정·삭제) ① 개인정보처리자가 법 제36조제1항에 따른 개인정보의 정정·삭제 요구를 받았을 때는 정당한 사유가 없는 한 요구를 받은 날로부터 10일 이내에 그 개인정보를 조사하여 정보주체의 요구에 따라 정정·삭제 등 필요한 조치를 한 후 그 결과를 정보주체에게 알려야 한다.

② 정보주체의 정정·삭제 요구가 법 제36조제1항 단서에 해당하는 경우에는 정당한 사유가 없는 한 요구를 받은 날로부터 10일 이내에 삭제를 요구할 수 없는 근거법령의 내용을 정보주체에게 알려야 한다.

제33조(개인정보의 처리정지) ① 개인정보처리자가 정보주체로부터 법 제37조제1항에 따라 개인정보처리를 정지하도록 요구받은 때에는 정당한 사유가 없는 한 요구를 받은 날로부터 10일 이내에 개인정보 처리의 일부 또는 전부를 정지하여야 한다. 다만, 법 제37조제2항 단서에 해당하는 경우에는 정보주체의 처리정지 요구를 거절할 수 있다.

② 개인정보처리자는 정보주체의 요구에 따라 처리가 정지된 개인정보에 대하여 정당한 사유가 없는 한 처리정지의 요구를 받은 날로부터 10일 이내에 해당 개인정보의 파기 등 정보주체의 요구에 상응하는 조치를 취하고 그 결과를 정보주체에게 알려야 한다.

제34조(권리행사의 방법 및 절차) ① 개인정보처리자는 정보주체가 법 제38조제1항에 따른 열람등요구를 하는 경우에는 개인정보를 수집하는 방법과 동일하거나 보다 쉽게 정보주체가 열람요구 등 권리를 행사할 수 있도록 간편한 방법을 제공하여야 하며, 개인정보의 수집시에 요구되지 않았던 증빙서류 등을 요구하거나 추가적인 절차를 요구할 수 없다.

② 제1항의 규정은 영 제46조에 따라 본인 또는 정당한 대리인임을 확인하고자 하는 경우와 영 제47조에 따른 수수료와 우송료의 정산에도 준용한다.

제3장 영상정보처리기기 설치·운영

제1절 영상정보처리기기의 설치

제35조(적용범위) 이 장은 영상정보처리기기운영자가 공개된 장소에 설치·운영하는 영상정보처리기기와 이 기기를 통하여 처리되는 개인영상정보를 대상으로 한다.

제36조(영상정보처리기기 운영·관리 지침) ① 영상정보처리기기 운영·관리 지침을 수립하거나 변경하는 경우에는 정보주체가 쉽게 확인할 수 있도록 공개하여야 한다.

② 영상정보처리기기 운영·관리 지침을 마련한 경우에는 법 제30조에 따른 개인정보 처리방침을 정하지 아니하거나, 영상정보처리기기 설치·운영에 관한 사항을 법 제30조에 따른 개인정보 처리방침에 포함하여 정할 수 있다.

제37조(관리책임자의 지정) ① 영상정보처리기기운영자는 개인영상정보의 처리에 관한 업무를 총괄해서 책임질 관리책임자를 지정하여야 한다.

② 제1항의 관리책임자는 법 제31조제2항에 따른 개인정보 보호책임자의 업무에 준하여 다음 각 호의 업무를 수행한다.

1. 개인영상정보 보호 계획의 수립 및 시행
2. 개인영상정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인영상정보 처리와 관련한 불만의 처리 및 피해구제
4. 개인영상정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
5. 개인영상정보 보호 교육 계획 수립 및 시행
6. 개인영상정보 파일의 보호 및 파기에 대한 관리·감독
7. 그 밖에 개인영상정보의 보호를 위하여 필요한 업무

③ 법 제31조에 따른 개인정보 보호책임자가 지정되어 있는 경우에는 그 개인정보 보호책임자가 관리책임자의 업무를 수행할 수 있다.

제38조(사전의견 수렴) 영상정보처리기기의 설치 목적 변경에 따른 추가 설치 등의 경우에도 영 제23조제1항에 따라 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다.

제39조(안내판의 설치) ① 영상정보처리기기운영자는 정보주체가 영상정보처리기기가 설치·운영 중임을 쉽게 알아볼 수 있도록 법 제25조제4항 본문에 따라 다음 각 호의 사항을 기재한 안내판 설치 등 필요한 조치를 하여야 한다.

1. 설치목적 및 장소
2. 촬영범위 및 시간
3. 관리책임자의 성명 또는 직책 및 연락처
4. 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우, 수탁자의 명칭 및 연락처

② 제1항에 따른 안내판은 촬영범위 내에서 정보주체가 알아보기 쉬운 장소에 누구라도 용이하게 판독할 수 있게 설치되어야 하며, 이 범위 내에서 영상정보처리기기운영자가 안

내판의 크기, 설치위치 등을 자율적으로 정할 수 있다.

③ 공공기관의 장이 기관 내 또는 기관 간에 영상정보처리기기의 효율적 관리 및 정보 연계 등을 위해 용도별·지역별 영상정보처리기기를 물리적·관리적으로 통합하여 설치·운영(이하 '통합관리'라 한다)하는 경우에는 설치목적 등 통합관리에 관한 내용을 정보주체가 쉽게 알아볼 수 있도록 제1항에 따른 안내판에 기재하여야 한다.

제2절 개인영상정보의 처리

제40조(개인영상정보 이용·제3자 제공 등 제한 등) ① 영상정보처리기기운영자는 다음 각 호의 경우를 제외하고는 개인영상정보를 수집 목적 이외로 이용하거나 제3자에게 제공하여서는 아니 된다. 다만 제5호부터 제9호까지의 경우는 공공기관의 경우로 한정한다.

1. 정보주체에게 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 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(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우

제41조(보관 및 파기) ① 영상정보처리기기운영자는 수집한 개인영상정보를 영상정보처리기기 운영·관리 방침에 명시한 보관 기간이 만료한 때에는 지체 없이 파기하여야 한다. 다만, 다른 법령에 특별한 규정이 있는 경우에는 그러하지 아니하다.

② 영상정보처리기기운영자가 그 사정에 따라 보유 목적의 달성을 위한 최소한의 기간을 산정하기 곤란한 때에는 보관 기간을 개인영상정보 수집 후 30일 이내로 한다.

③ 개인영상정보의 파기 방법은 다음 각 호의 어느 하나와 같다.

1. 개인영상정보가 기록된 출력물(사진 등) 등은 파쇄 또는 소각
2. 전자기적(電磁氣的) 파일 형태의 개인영상정보는 복원이 불가능한 기술적 방법으로 영구 삭제

제42조(이용·제3자 제공·파기의 기록 및 관리) ① 영상정보처리기기운영자는 개인영상정보를 수집 목적 이외로 이용하거나 제3자에게 제공하는 경우에는 다음 각 호의 사항을 기록하고 이를 관리하여야 한다.

1. 개인영상정보 파일의 명칭
2. 이용하거나 제공받은 자(공공기관 또는 개인)의 명칭
3. 이용 또는 제공의 목적
4. 법령상 이용 또는 제공근거가 있는 경우 그 근거
5. 이용 또는 제공의 기간이 정하여져 있는 경우에는 그 기간
6. 이용 또는 제공의 형태

② 영상정보처리기기운영자가 개인영상정보를 파기하는 경우에는 다음 사항을 기록하고 관리하여야 한다.

1. 파기하는 개인영상정보 파일의 명칭
2. 개인영상정보 파기 일시 (사전에 파기 시기 등을 정한 자동 삭제의 경우에는 파기 주기 및 자동 삭제 여부에 관한 확인 시기)
3. 개인영상정보 파기 담당자

제43조(영상정보처리기기 설치 및 관리 등의 위탁) ① 영상정보처리기기운영자가 영 제26조제1항에 따라 영상정보처리기기의 설치·운영에 관한 사무를 제3자에게 위탁하는 경우에는 그 내용을 정보주체가 언제든지 쉽게 확인할 수 있도록 영 제24조에 따른 안내판 및 영 제27조에 따른 영상정보처리기기 운영·관리 방침에 수탁자의 명칭 등을 공개하여야 한다.

② 영상정보처리기기운영자가 영 제26조제1항에 따라 영상정보처리기기의 설치·운영에 관한 사무를 제3자에게 위탁할 경우에는 그 사무를 위탁받은 자가 개인영상정보를 안전하게 처리하고 있는지를 관리·감독하여야 한다.

제3절 개인영상정보의 열람등 요구

제44조(정보주체의 열람등 요구) ① 정보주체는 영상정보처리기기운영자가 처리하는 개인영상정보에 대하여 열람 또는 존재확인(이하 "열람등"이라 한다)을 해당 영상정보처리기기운영자에게 요구할 수 있다. 이 경우 정보주체가 열람등을 요구할 수 있는 개인영상정보는 정보주체 자신이 촬영된 개인영상정보 및 명백히 정보주체의 급박한 생명, 신체, 재산의 이익을 위하여 필요한 개인영상정보에 한한다.

② 영상정보처리기기운영자가 공공기관인 경우에는 해당 기관의 장에게 별지 제2호서식에 따른 개인영상정보 열람·존재확인 청구서(전자문서를 포함한다)로 하여야 한다.

③ 영상정보처리기기운영자는 제1항에 따른 요구를 받았을 때에는 지체 없이 필요한 조치를 취하여야 한다. 이때에 영상정보처리기기운영자는 열람등 요구를 한 자가 본인이거나 정당한 대리인인지를 주민등록증·운전면허증·여권 등의 신분증명서를 제출받아 확인하여야 한다.

④ 제3항의 규정에도 불구하고 다음 각 호에 해당하는 경우에는 영상정보처리기기운영자는 정보주체의 개인영상정보 열람등 요구를 거부할 수 있다. 이 경우 영상정보처리기기운영자는 10일 이내에 서면 등으로 거부 사유를 정보주체에게 통지하여야 한다.

1. 범죄수사·공소유지·재판수행에 중대한 지장을 초래하는 경우(공공기관에 한함)
2. 개인영상정보의 보관기간이 경과하여 파기한 경우

3. 기타 정보주체의 열람등 요구를 거부할 만한 정당한 사유가 존재하는 경우

⑤ 영상정보처리기기운영자는 제3항 및 제4항에 따른 조치를 취하는 경우 다음 각 호의 사항을 기록하고 관리하여야 한다.

1. 개인영상정보 열람등을 요구한 정보주체의 성명 및 연락처
2. 정보주체가 열람등을 요구한 개인영상정보 파일의 명칭 및 내용
3. 개인영상정보 열람등의 목적
4. 개인영상정보 열람등을 거부한 경우 그 거부의 구체적 사유
5. 정보주체에게 개인영상정보 사본을 제공한 경우 해당 영상정보의 내용과 제공한 사유

⑥ 정보주체는 영상정보처리기기운영자에게 정보주체 자신의 개인영상정보에 대한 파기를 요구하는 때에는 제1항에 의하여 보존을 요구하였던 개인영상정보에 대하여만 그 파기를 요구할 수 있다. 영상정보처리기기운영자가 해당 파기조치를 취한 경우에는 그 내용을 기록하고 관리하여야 한다.

제45조(개인영상정보 관리대장) 제42조제1항 및 제2항, 제44조제5항 및 제6항에 따른 기록 및 관리는 별지 제3호서식에 따른 '개인영상정보 관리대장'을 활용할 수 있다.

제46조(정보주체 이외의 자의 개인영상정보 보호) 영상정보처리기기운영자는 제44조제2항에 따른 열람등 조치를 취하는 경우, 만일 정보주체 이외의 자를 명백히 알아볼 수 있거나 정보주체 이외의 자의 사생활 침해의 우려가 있는 경우에는 해당되는 정보주체 이외의 자의 개인영상정보를 알아볼 수 없도록 보호조치를 취하여야 한다.

제4절 개인영상정보 보호 조치

제47조(개인영상정보의 안전성 확보를 위한 조치) 영상정보처리기기운영자는 개인영상정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 법 제29조 및 영 제30조제1항에 따라 안전성 확보를 위하여 다음 각 호의 조치를 하여야 한다.

1. 개인영상정보의 안전한 처리를 위한 내부 관리계획의 수립·시행, 다만 「개인정보의 안전성 확보조치 기준 고시」 제2조제4호에 따른 '소상공인'은 내부관리계획을 수립하지 아니할 수 있다.
2. 개인영상정보에 대한 접근 통제 및 접근 권한의 제한 조치
3. 개인영상정보를 안전하게 저장·전송할 수 있는 기술의 적용 (네트워크 카메라의 경우 안전한 전송을 위한 암호화 조치, 개인영상정보파일 저장시 비밀번호 설정 등)
4. 처리기록의 보관 및 위조·변조 방지를 위한 조치 (개인영상정보의 생성 일시 및 열람할 경우에 열람 목적·열람자·열람 일시 등 기록·관리 조치 등)
5. 개인영상정보의 안전한 물리적 보관을 위한 보관시설 마련 또는 잠금장치 설치

제48조(개인영상정보처리기기의 설치·운영에 대한 점검) ① 공공기관의 장이 영상정보처리기기를 설치·운영하는 경우에는 이 지침의 준수 여부에 대한 자체점검을 실시하여 다음 해 3월 31일까지 그 결과를 보호위원회에게 통보하고 영 제34조제3항에 따른 시스템에 등록하여야 한다. 이 경우 다음 각 호의 사항을 고려하여야 한다.

1. 영상정보처리기기의 운영·관리 방침에 열거된 사항
2. 관리책임자의 업무 수행 현황
3. 영상정보처리기기의 설치 및 운영 현황
4. 개인영상정보 수집 및 이용·제공·파기 현황
5. 위탁 및 수탁자에 대한 관리·감독 현황
6. 정보주체의 권리행사에 대한 조치 현황
7. 기술적·관리적·물리적 조치 현황
8. 영상정보처리기 설치·운영의 필요성 지속 여부 등

② 공공기관의 장은 제1항과 제3항에 따른 영상정보처리기기 설치·운영에 대한 자체점검을 완료한 후에는 그 결과를 홈페이지 등에 공개하여야 한다.

③ 공공기관 외의 영상정보처리기기운영자는 영상정보처리기기 설치·운영으로 인하여 정보주체의 개인영상정보의 침해가 우려되는 경우에는 자체점검 등 개인영상정보의 침해 방지를 위해 적극 노력하여야 한다.

제4장 공공기관 개인정보파일 등록·공개

제1절 총칙

제49조(적용대상) 이 장의 적용대상은 다음과 같다.

1. 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다) 및 그 소속 기관, 지방자치단체
2. 「국가인권위원회법」에 따른 국가인권위원회
3. 「공공기관의 운영에 관한 법률」에 따른 공공기관
4. 「지방공기업법」에 따른 지방공사 및 지방공단
5. 특별법에 의하여 설립된 특수법인
6. 「초·중등교육법」, 「고등교육법」 및 그 밖의 다른 법률에 따라 설치된 각급 학교

제50조(적용제외) 이 장은 다음 각 호의 어느 하나에 해당하는 개인정보파일에 관하여는 적용하지 아니한다.

1. 국회, 법원, 헌법재판소, 중앙선거관리위원회(그 소속기관을 포함한다)에서 관리하는 개인정보파일
2. 법 제32조제2항에 따라 적용이 제외되는 다음 각목의 개인정보파일
   가. 국가안전, 외교상 비밀, 그 밖에 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일
   나. 범죄의 수사, 공소의 제기 및 유지, 형 및 감호의 집행, 교정처분, 보호처분, 보안관찰처분과 출입국 관리에 관한 사항을 기록한 개인정보파일
   다. 「조세범처벌법」에 따른 범칙행위 조사 및 「관세법」에 따른 범칙행위 조사에 관한 사항을 기록한 개인정보파일
   라. 공공기관의 내부적 업무처리만을 위하여 사용되는 개인정보파일
   마. 다른 법령에 따라 비밀로 분류된 개인정보파일

3. 법 제58조제1항에 따라 적용이 제외되는 다음 각목의 개인정보파일
   가. 공공기관이 처리하는 개인정보 중 「통계법」에 따라 수집되는 개인정보파일
   나. 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보파일
   다. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보파일
4. 영상정보처리기기를 통하여 처리되는 개인영상정보파일
5. 자료·물품 또는 금전의 송부, 1회성 행사 수행 등의 목적만을 위하여 운용하는 경우로서 저장하거나 기록하지 않고 폐기할 목적으로 수집된 개인정보파일
6. 「금융실명거래 및 비밀보장에 관한 법률」에 따른 금융기관이 금융업무 취급을 위해 보유하는 개인정보파일

제2절 개인정보파일의 등록주체와 절차

제51조(개인정보파일 등록 주체) ① 개인정보파일을 운용하는 공공기관의 개인정보 보호책임자는 그 현황을 보호위원회에 등록하여야 한다.

② 중앙행정기관, 광역자치단체, 특별자치시도, 기초자치단체는 보호위원회에 직접 등록하여야 한다.

③ 교육청 및 각급 학교 등은 교육부를 통하여 보호위원회에 등록하여야 한다.

④ 중앙행정기관 및 지방자치단체의 소속기관, 기타 공공기관은 상위 관리기관을 통하여 보호위원회에 등록하여야 한다.

제52조(개인정보파일 등록 및 변경 신청) ① 개인정보파일을 운용하는 공공기관의 개인정보취급자는 해당 공공기관의 개인정보 보호책임자에게 개인정보파일 등록을 신청하여야 한다.

② 개인정보파일 등록 신청 사항은 다음의 각 호와 같다. 신청은 「개인정보 보호법 고시」(이하 "고시"라 한다) 제3조제2항에 따른 별지 제2호서식의 '개인정보파일 등록·변경등록 신청서'를 활용할 수 있다.

1. 개인정보파일을 운용하는 공공기관의 명칭
2. 개인정보파일의 명칭
3. 개인정보파일의 운영 근거 및 목적
4. 개인정보파일에 기록되는 개인정보의 항목
5. 개인정보파일로 보유하고 있는 개인정보의 정보주체 수
6. 개인정보의 처리 방법
7. 개인정보의 보유 기간
8. 개인정보를 통상적 또는 반복적으로 제공하는 경우에는 그 제공받는 자
9. 해당 공공기관에서 개인정보 처리 관련 업무를 담당하는 부서
10. 개인정보의 열람 요구를 접수·처리하는 부서
11. 개인정보파일의 개인정보 중 법 제35조제4항에 따라 열람을 제한하거나 거절할 수 있는 개인정보의 범위 및 제한 또는 거절 사유

12. 법 제33조제1항에 따른 개인정보 영향평가를 받은 개인정보파일의 경우에는 그 영향평가의 결과

③ 개인정보취급자는 등록한 사항이 변경된 경우에는 고시 제3조제2항에 따른 별지 제2호서식의 '개인정보파일 등록·변경등록 신청서'를 활용하여 개인정보 보호책임자에게 변경을 신청하여야 한다.

제53조(개인정보파일 등록 및 변경 확인) ① 개인정보파일 등록 또는 변경 신청을 받은 개인정보 보호책임자는 등록·변경 사항을 검토하고 그 적정성을 판단한 후 보호위원회에 등록하여야 한다.

② 교육청 및 각급 학교 등의 개인정보 보호책임자는 교육부에 제1항에 따른 등록·변경 사항의 검토 및 적정성 판단을 요청한 후, 교육부의 확인을 받아 보호위원회에 등록하여야 한다.

③ 중앙행정기관 및 지방자치단체의 소속기관, 기타 공공기관은 상위 관리기관에 제1항에 따른 등록·변경 사항의 검토 및 적정성 판단을 요청한 후, 상위 관리기관의 확인을 받아 보호위원회에 등록하여야 한다.

④ 제1항부터 제3항의 등록은 60일 이내에 하여야 한다.

제54조(개인정보파일 표준목록 등록과 관리) ① 특별지방행정기관, 지방자치단체, 교육기관(학교 포함) 등 전국적으로 단일한 공통업무를 집행하고 있는 기관은 각 중앙행정기관에서 제공하는 '개인정보파일 표준목록'에 따라 등록해야 한다.

② 전국 단일의 공통업무와 관련된 개인정보파일 표준목록은 해당 중앙부처에서 등록·관리해야 한다.

제55조(개인정보파일의 파기) ① 공공기관은 개인정보파일의 보유기간 경과, 처리 목적 달성 등 개인정보파일이 불필요하게 되었을 때에는 지체 없이 그 개인정보파일을 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.

② 공공기관은 개인정보파일의 보유기간, 처리 목적 등을 반영한 개인정보 파기계획을 수립·시행하여야 한다. 다만, 영 제30조제1항제1호에 따른 내부 관리계획이 수립되어 있는 경우에는 내부 관리계획에 개인정보 파기계획을 포함하여 시행할 수 있다.

③ 개인정보취급자는 보유기간 경과, 처리 목적 달성 등 파기 사유가 발생한 개인정보파일을 선정하고, 별지 제4호서식에 따른 개인정보파일 파기요청서에 파기 대상 개인정보파일의 명칭, 파기방법 등을 기재하여 개인정보 보호책임자의 승인을 받아 개인정보를 파기하여야 한다.

④ 개인정보 보호책임자는 개인정보 파기 시행 후 파기 결과를 확인하고 별지 제5호서식에 따른 개인정보파일 파기 관리대장을 작성하여야 한다.

제56조(개인정보파일 등록 사실의 삭제) ① 개인정보취급자는 제55조에 따라 개인정보파일을 파기한 경우, 법 제32조에 따른 개인정보파일의 등록사실에 대한 삭제를 개인정보 보호책임자에게 요청해야 한다.

② 개인정보파일 등록의 삭제를 요청받은 개인정보 보호책임자는 그 사실을 확인하고, 지

체 없이 등록 사실을 삭제한 후 그 사실을 보호위원회에 통보한다.

제57조(등록·파기에 대한 개선권고) ① 공공기관의 개인정보 보호책임자는 제53조제1항에 따라 검토한 개인정보파일이 과다하게 운용되고 있다고 판단되는 경우에는 개선을 권고할 수 있다.

② 교육청 및 각급 학교, 중앙행정기관 및 지방자치단체의 소속기관, 기타 공공기관의 개인정보 보호책임자는 제53조제2항 및 제53조제3항에 따라 검토한 개인정보파일이 과다하게 운용된다고 판단되거나, 등록되지 않은 파일이 있는 것으로 확인되는 경우에는 개선을 권고할 수 있다.

③ 보호위원회는 개인정보파일의 등록사항과 그 내용을 검토하고 다음 각 호의 어느 하나에 해당되는 경우에는 법 제32조제3항에 따라 해당 공공기관의 개인정보 보호책임자에게 개선을 권고할 수 있다.

1. 개인정보파일이 과다하게 운용된다고 판단되는 경우
2. 등록하지 않은 개인정보파일이 있는 경우
3. 개인정보파일 등록 사실이 삭제되었음에도 불구하고 개인정보파일을 계속 보유하고 있는 경우
4. 개인정보 영향평가를 받은 개인정보파일을 보유하고 있음에도 그 결과를 등록사항에 포함하지 않은 경우
5. 기타 법 제32조에 따른 개인정보파일의 등록 및 공개에 위반되는 사항이 있다고 판단되는 경우

④ 보호위원회는 제3항에 따라 개선을 권고한 경우에는 그 내용 및 결과에 대하여 개인정보 보호위원회의 심의·의결을 거쳐 공표할 수 있다.

⑤ 보호위원회는 공공기관의 개인정보파일 등록·파기 현황에 대한 점검을 실시할 수 있다.

제3절 개인정보파일의 관리 및 공개

제58조(개인정보파일대장 작성) 공공기관은 1개의 개인정보파일에 1개의 개인정보파일대장을 작성해야 한다.

제59조(개인정보파일 이용·제공 관리) 공공기관은 법 제18조제2항 각 호에 따라 제3자가 개인정보파일의 이용·제공을 요청한 경우에는 각각의 이용·제공 가능 여부를 확인하고 별지 제6호서식의 ‘개인정보 목적 외 이용·제공대장’에 기록하여 관리해야 한다.

제60조(개인정보파일 보유기간의 산정) ① 보유기간은 전체 개인정보가 아닌 개별 개인정보의 수집부터 삭제까지의 생애주기로서 보유목적에 부합된 최소기간으로 산정하되, 개별 법령의 규정에 명시된 자료의 보존기간에 따라 산정해야 한다.

② 개별 법령에 구체적인 보유기간이 명시되어 있지 않은 경우에는 개인정보 보호책임자의 협의를 거쳐 기관장의 결재를 통하여 산정해야 한다. 다만, 보유기간은 별표 1의 개인정보파일 보유기간 책정 기준표에서 제시한 기준과 「공공기록물 관리에 관한 법률 영」에

따른 기록관리기준표를 상회할 수 없다.

③ 정책고객, 홈페이지회원 등의 홍보 및 대국민서비스 목적의 외부고객 명부는 특별한 경우를 제외하고는 2년을 주기로 정보주체의 재동의 절차를 거쳐 동의한 경우에만 계속하여 보유할 수 있다.

제61조(개인정보파일 현황 공개 및 방법) ① 공공기관의 개인정보 보호책임자는 개인정보파일의 보유·파기현황을 주기적으로 조사하여 그 결과를 해당 공공기관의 개인정보 처리방침에 포함하여 관리해야 한다.

② 보호위원회는 개인정보파일 등록 현황을 누구든지 쉽게 열람할 수 있도록 공개하여야 한다.

③ 보호위원회는 전 공공기관의 개인정보파일 등록 및 삭제 현황을 종합하여 매년 공개해야 하며, 개인정보파일 현황 공개에 관한 업무를 전자적으로 처리하기 위하여 정보시스템을 구축·운영할 수 있다.

제5장 보칙

제62조(친목단체에 대한 벌칙조항의 적용배제) ① 친목단체의 개인정보처리자에 대하여는 법 제75조제1항제1호, 법 제75조제2항제1호, 법 제75조제4항제8호 및 법 제75조제4항제8호의 벌칙을 적용하지 아니한다.

② 제1항에서 규정한 사항을 제외한 벌칙규정은 친목단체의 개인정보처리자에 대하여도 적용한다.

제63조(처리 중인 개인정보에 관한 경과조치) ① 법 시행 전에 근거법령 없이 개인정보를 수집한 경우 당해 개인정보를 보유하는 것은 적법한 처리로 본다. 다만, 이 법 시행 이후 기존의 수집목적 범위 내에서 이용하는 경우를 제외하고 개인정보를 새롭게 처리하는 경우에는 법, 영, 고시 및 이 지침에 따라야 한다.

② 법 시행 전에 법률의 근거 또는 정보주체의 동의 없이 제3자로부터 개인정보를 제공받아 목적 외의 용도로 이용하고 있는 개인정보처리자는 정보주체의 동의를 받아야 한다.

③ 법 시행 전에 개인정보를 수집한 개인정보처리자는 기존의 수집목적 범위에도 불구하고 제1항 단서 및 제2항을 준수하기 위하여 새롭게 정보주체의 동의를 받을 목적으로 법 시행 전에 수집한 개인정보를 이용할 수 있다.

부칙 <제2020-1호, 2020. 8. 11.>

이 고시는 고시한 날부터 시행한다.

(개인정보보호위원회) 개인정보의 안전성 확보조치 기준

[시행 2021. 9. 15.] [개인정보보호위원회고시 제2021-2호, 2021. 9. 15., 일부개정.]

제1조(목적) 이 기준은 「개인정보 보호법」(이하 "법"이라 한다) 제23조제2항, 제24조제3항 및 제29조와 같은 법 시행령(이하 "영"이라 한다) 제21조 및 제30조에 따라 개인정보처리자가 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치에 관한 최소한의 기준을 정하는 것을 목적으로 한다.

제2조(정의) 이 기준에서 사용하는 용어의 뜻은 다음과 같다.

1. "정보주체"란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
2. "개인정보파일"이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.
3. "개인정보처리자"란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
4. "대기업"이란 「독점규제 및 공정거래에 관한 법률」 제14조에 따라 공정거래위원회가 지정한 기업집단을 말한다.
5. "중견기업"이란 「중견기업 성장촉진 및 경쟁력 강화에 관한 특별법」 제2조에 해당하는 기업을 말한다.
6. "중소기업"이란 「중소기업기본법」 제2조 및 동법 시행령 제3조에 해당하는 기업을 말한다.
7. "소상공인"이란 「소상공인 보호 및 지원에 관한 법률」 제2조에 해당하는 자를 말한다.
8. "개인정보 보호책임자"란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지는 자로서 영 제32조제2항에 해당하는 자를 말한다.
9. "개인정보취급자"란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을 말한다.
10. "개인정보처리시스템"이란 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템을 말한다.
11. "위험도 분석"이란 개인정보 유출에 영향을 미칠 수 있는 다양한 위험요소를 식별·평가하고 해당 위험요소를 적절하게 통제할 수 있는 방안 마련을 위한 종합적으로 분석하는 행위를 말한다.
12. "비밀번호"란 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망 등에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공

개되지 않는 정보를 말한다.

13. "정보통신망"이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다.
14. "공개된 무선망"이란 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.
15. "모바일 기기"란 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿PC 등 개인정보처리에 이용되는 휴대용 기기를 말한다.
16. "생체정보"란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 인증·식별하거나 개인에 관한 특징을 알아보기 위해 일정한 기술적 수단을 통해 처리되는 정보를 말한다.
16의2. "생체인식정보"란 생체정보 중 특정 개인을 인증 또는 식별할 목적으로 일정한 기술적 수단을 통해 처리되는 정보를 말한다.
17. "보조저장매체"란 이동형 하드디스크, USB메모리, CD(Compact Disk), DVD(Digital Versatile Disk) 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 용이하게 연결·분리할 수 있는 저장매체를 말한다.
18. "내부망"이란 물리적 망분리, 접근 통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.
19. "접속기록"이란 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무내역에 대하여 개인정보취급자 등의 계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우 "접속"이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신이 가능한 상태를 말한다.
20. "관리용 단말기"란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리시스템에 직접 접속하는 단말기를 말한다.

제3조(안전조치 기준 적용) 개인정보처리자가 개인정보의 안전성 확보에 필요한 조치를 하는 경우에는 [별표] 개인정보처리자 유형 및 개인정보 보유량에 따른 안전조치 기준을 적용하여야 한다. 이 경우 개인정보처리자가 어느 유형에 해당하는지에 대한 입증책임은 당해 개인정보처리자가 부담한다.

제4조(내부 관리계획의 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 개인정보보호책임자는 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부 관리계획의 이행 실태를 연1회 이상으로 점검·관리 하여야 한다.

제5조(접근 권한의 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.

③ 개인정보처리자는 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.

제7조(개인정보의 암호화) ① 개인정보처리자는 고유식별정보, 비밀번호, 생체인식정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

② 개인정보처리자는 비밀번호 및 생체인식정보는 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

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 1년 이상 보관·관리하여야 한다. 다만, 5만명 이상의 정보주체에 관하여 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다.

② 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 특히 개인정보를 다운로드한 것이 발견되었을 경우에는 내부관리 계획으로 정하는 바에 따라 그 사유를 반드시 확인하여야 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

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(개인정보의 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

제14조(재검토 기한) 개인정보보호위원회는 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 이 고시에 대하여 2020년 8월 11일을 기준으로 매 3년이 되는 시점(매 3년째의 8월 10일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부칙 <제2021-2호, 2021. 9. 15.>

이 고시는 고시한 날부터 시행한다.

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

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

(개인정보보호위원회) 개인정보의 기술적·관리적 보호조치 기준

[시행 2021. 9. 15.] [개인정보보호위원회고시 제2021-3호, 2021. 9. 15., 일부개정.]

제1조(목적) ① 이 기준은 「개인정보 보호법」(이하 "법"이라 한다) 제29조 및 같은 법 시행령 제48조의2제3항에 따라 정보통신서비스 제공자등(법 제39조의14에 따라 준용되는 자를 포함한다. 이하 같다)이 이용자의 개인정보를 처리함에 있어서 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성 확보를 위하여 필요한 기술적·관리적 보호조치의 최소한의 기준을 정하는 것을 목적으로 한다.

② 정보통신서비스 제공자등은 사업규모, 개인정보 보유 수 등을 고려하여 스스로의 환경에 맞는 개인정보 보호조치 기준을 수립하여 시행하여야 한다.

제2조(정의) 이 기준에서 사용하는 용어의 뜻은 다음과 같다.

1. "개인정보 보호책임자"란 이용자의 개인정보보호 업무를 총괄하거나 업무처리를 최종 결정하는 임직원을 말한다.
2. "개인정보취급자"란 이용자의 개인정보를 수집, 보관, 처리, 이용, 제공, 관리 또는 파기 등의 업무를 하는 자를 말한다.
3. "내부관리계획"이라 함은 정보통신서비스 제공자등이 개인정보의 안전한 처리를 위하여 개인정보보호 조직의 구성, 개인정보취급자의 교육, 개인정보 보호조치 등을 규정한 계획을 말한다.
4. "개인정보처리시스템"이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다.
5. "망분리"라 함은 외부 인터넷망을 통한 불법적인 접근과 내부정보 유출을 차단하기 위해 업무망과 외부 인터넷망을 분리하는 망 차단조치를 말한다.
6. "비밀번호"라 함은 이용자 및 개인정보취급자 등이 시스템 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 말한다.
7. "접속기록"이라 함은 이용자 또는 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 식별자, 접속일시, 접속지를 알 수 있는 정보, 수행업무 등 접속한 사실을 전자적으로 기록한 것을 말한다.
8. "생체정보"라 함은 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 인증·식별하거나 개인에 관한 특징을 알아보기 위해 일정한 기술적 수단을 통해 처리되는 정보를 말한다.

8의2. "생체인식정보"라 함은 생체정보 중 특정 개인을 인증 또는 식별할 목적으로 일정한 기술적 수단을 통해 처리되는 정보를 말한다.

9. "P2P(Peer to Peer)"라 함은 정보통신망을 통해 서버의 도움 없이 개인과 개인이 직접 연결되어 파일을 공유하는 것을 말한다.

10. "공유설정"이라 함은 컴퓨터 소유자의 파일을 타인이 조회 · 변경 · 복사 등을 할 수 있도록 설정하는 것을 말한다.
11. "보안서버"라 함은 정보통신망에서 송 · 수신하는 정보를 암호화하여 전송하는 웹서버를 말한다.
12. "인증정보"라 함은 개인정보처리시스템 또는 정보통신망을 관리하는 시스템 등이 요구한 식별자의 신원을 검증하는데 사용되는 정보를 말한다.
13. "모바일 기기"란 스마트폰, 태블릿PC 등 무선망을 이용할 수 있는 휴대용 기기를 말한다.
14. "보조저장매체"란 이동형 하드디스크(HDD), USB메모리, CD(Compact Disk) 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 쉽게 분리 · 접속할 수 있는 저장매체를 말한다.

제3조(내부관리계획의 수립 · 시행) ① 정보통신서비스 제공자등은 다음 각 호의 사항을 정하여 개인정보보호 조직을 구성 · 운영하여야 한다.

1. 개인정보 보호책임자의 자격요건 및 지정에 관한 사항
2. 개인정보 보호책임자와 개인정보취급자의 역할 및 책임에 관한 사항
3. 개인정보 내부관리계획의 수립 및 승인에 관한 사항
4. 개인정보의 기술적 · 관리적 보호조치 이행 여부의 내부 점검에 관한 사항
5. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
6. 개인정보의 분실 · 도난 · 유출 · 위조 · 변조 · 훼손 등이 발생한 경우의 대응절차 및 방법에 관한 사항
7. 그 밖에 개인정보보호를 위해 필요한 사항

② 정보통신서비스 제공자등은 다음 각 호의 사항을 정하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 사업규모, 개인정보 보유 수 등을 고려하여 필요한 교육을 정기적으로 실시하여야 한다.

1. 교육목적 및 대상
2. 교육 내용
3. 교육 일정 및 방법

③ 정보통신서비스 제공자등은 제1항 및 제2항에 대한 세부 계획, 제4조부터 제8조까지의 보호조치 이행을 위한 세부적인 추진방안을 포함한 내부관리계획을 수립 · 시행하여야 한다.

제4조(접근통제) ① 정보통신서비스 제공자등은 개인정보처리시스템에 대한 접근권한을 서비스 제공을 위하여 필요한 개인정보 보호책임자 또는 개인정보취급자에게만 부여한다.

② 정보통신서비스 제공자등은 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소한다.

③ 정보통신서비스 제공자등은 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 5년간 보관한다.

④ 정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용하여야 한다.

⑤ 정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 시스템을 설치·운영하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지

⑥ 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상이거나 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 정보통신서비스 제공자등은 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등을 물리적 또는 논리적으로 망분리 하여야 한다.

⑦ 정보통신서비스 제공자등은 이용자가 안전한 비밀번호를 이용할 수 있도록 비밀번호 작성규칙을 수립하고, 이행한다.

⑧ 정보통신서비스 제공자등은 개인정보취급자를 대상으로 다음 각 호의 사항을 포함하는 비밀번호 작성규칙을 수립하고, 이를 적용·운용하여야 한다.

1. 영문, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성
2. 연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고
3. 비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경

⑨ 정보통신서비스 제공자등은 처리중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다.

⑩ 정보통신서비스 제공자등은 개인정보처리시스템에 대한 개인정보취급자의 접속이 필요한 시간 동안만 최대 접속시간 제한 등의 조치를 취하여야 한다.

제5조(접속기록의 위·변조방지) ① 정보통신서비스 제공자등은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록을 보존·관리하여야 한다.

② 단, 제1항의 규정에도 불구하고 「전기통신사업법」 제5조의 규정에 따른 기간통신사업자의 경우에는 보존·관리해야할 최소 기간을 2년으로 한다.

③ 정보통신서비스 제공자등은 개인정보취급자의 접속기록이 위·변조되지 않도록 별도의 물리적인 저장 장치에 보관하여야 하며 정기적인 백업을 수행하여야 한다.

제6조(개인정보의 암호화) ① 정보통신서비스 제공자등은 비밀번호는 복호화 되지 아니하도록 일방향 암호화하여 저장한다.

② 정보통신서비스 제공자등은 다음 각 호의 정보에 대해서는 안전한 암호알고리듬으로 암호화하여 저장한다.

1. 주민등록번호
2. 여권번호
3. 운전면허번호
4. 외국인등록번호
5. 신용카드번호
6. 계좌번호
7. 생체인식정보

③ 정보통신서비스 제공자등은 정보통신망을 통해 이용자의 개인정보 및 인증정보를 송·수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 이를 암호화해야 한다. 보안서버는 다음 각 호 중 하나의 기능을 갖추어야 한다.

1. 웹서버에 SSL(Secure Socket Layer) 인증서를 설치하여 전송하는 정보를 암호화하여 송·수신하는 기능
2. 웹서버에 암호화 응용프로그램을 설치하여 전송하는 정보를 암호화하여 송·수신하는 기능

④ 정보통신서비스 제공자등은 이용자의 개인정보를 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 이를 암호화해야 한다.

제7조(악성프로그램 방지) 정보통신서비스 제공자등은 악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 하며, 다음 각호의 사항을 준수하여야 한다.

1. 보안 프로그램의 자동 업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지
2. 악성프로그램관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시

제8조(물리적 접근 방지) ① 정보통신서비스 제공자등은 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소에 대한 출입통제 절차를 수립·운영하여야 한다.

② 정보통신서비스 제공자등은 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.

③ 정보통신서비스 제공자등은 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하여야 한다.

제9조(출력·복사시 보호조치) ① 정보통신서비스 제공자등은 개인정보처리시스템에서 개인정보의 출력시(인쇄, 화면표시, 파일생성 등) 용도를 특정하여야 하며, 용도에 따라 출력 항목을 최소화 한다.

② 정보통신서비스 제공자등은 개인정보가 포함된 종이 인쇄물, 개인정보가 복사된 외부

저장매체 등 개인정보의 출력·복사물을 안전하게 관리하기 위해 출력·복사 기록 등 필요한 보호조치를 갖추어야 한다.

제10조(개인정보 표시 제한 보호조치) 정보통신서비스 제공자등은 개인정보 업무처리를 목적으로 개인정보의 조회, 출력 등의 업무를 수행하는 과정에서 개인정보보호를 위하여 개인정보를 마스킹하여 표시제한 조치를 취할 수 있다.

제11조(재검토 기한) 개인정보보호위원회는 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 이 고시에 대하여 2020년 8월 11일을 기준으로 매 3년이 되는 시점(매 3년째의 8월 10일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부칙 <제2021-3호, 2021. 9. 15.>

이 고시는 고시한 날부터 시행한다

건강보험심사평가원

HEALTH INSURANCE REVIEW & ASSESSMENT SERVICE