개인정보 내부관리지침

ICT전략실 정보보호부

전부개정 2018. 6. 28. 지침 제255호
개정 2019. 6. 28. 지침 제274호
개정 2020. 2. 5. 지침 제295호
개정 2020. 10. 13. 지침 제310호
개정 2021. 9. 23. 지침 제343호
개정 2022. 10. 25. 지침 제376호
개정 2023. 11. 28. 지침 제409호
개정 2024. 10. 10. 지침 제432호

제1장 총칙

제1조(목적) 이 지침은 「개인정보 보호법」 제12조 및 제29조에 따라 건강보험심사평가원의 개인정보 처리에 관한 기준 및 절차, 개인정보 침해의 유형 및 예방조치 등에 관한 세부적인 사항을 규정함을 목적으로 한다. <개정 2023.11.28.>

제2조(정의) 이 지침에서 사용하는 용어의 뜻은 다음과 같다. <개정 2020.10.13., 2022.10.25., 2023.11.28., 2024.10.10.>

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 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.

3. "정보주체"란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.

4. "개인정보처리자"란 업무를 목적으로 「개인정보 보호법」(이하 "법"이라 한다) 제2조제4호에 따른 개인정보파일을 운용하기 위하여 개인정보를 처리하는 건강보험심사평가원(이하 "심사평가원"이라 한다)을 말한다.

5. "개인정보 보호책임자"란 심사평가원의 개인정보 처리에 관한 업무를 총괄해서 책임지는 자를 말한다.

6. "개인정보 보호관리자"란 개인정보 보호책임자의 업무를 보좌하기 위하여 개인정보 보호에 관한 실무를 수행하고 관리하는 자를 말한다.

7. "부서별 개인정보책임자"란 개인정보를 처리하는 부서에서 개인정보 처리에 관한 업무를 총괄해서 책임지거나 의사결정을 하는 자를 말한다.

8. "개인정보취급자"란 직접 개인정보에 관한 업무를 담당하거나 그 밖에 업무상 필요에 의하여 개인정보에 접근하여 처리하는 임직원, 파견근로자,

시간제근로자 등을 말한다.

9. “개인정보 처리시스템”이란 데이터베이스 시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템을 말한다.

10. “고정형 영상정보처리기기”란 일정한 공간에 설치되어 지속적 또는 주기적으로 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 일체의 장치로서 개인정보 보호법 시행령(이하 “영”이라 한다) 제3조제1항에 따른 폐쇄회로 텔레비전 및 네트워크 카메라를 말한다.

10의2. “이동형 영상정보처리기기”란 사람이 신체에 착용 또는 휴대하거나 이동 가능한 물체에 부착 또는 거치하여 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 영 제3조제2항에 따른 착용형, 휴대형, 부착·거치형, 그 밖에 이와 유사한 기능을 가지는 장치를 말한다.

11. “개인영상정보”란 법 제2조제1호에 따른 개인정보 중 고정형 또는 이동형 영상정보처리기기에 의하여 촬영·처리되는 영상 형태의 개인정보 중 개인의 초상, 행동 등과 관련된 영상으로서 해당 개인을 식별할 수 있는 정보를 말한다.

12. “개인영상정보 관리책임자”란 개인영상정보의 처리에 관한 업무를 총괄해서 책임지는 자를 말한다.

13. “개인정보파일”이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.

14. “정보통신망”이란 「전기통신사업법」 제2조제2호에 따른 전기통신설비를

이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다.

15. “접속기록”이란 개인정보처리시스템에 접속하는 자가 개인정보처리시스템에 접속하여 수행한 업무내역에 대하여 식별자, 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.
16. “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.
17. “개인정보 영향평가”란 「개인정보 보호법 시행령」 제35조에 해당하는 개인정보파일의 운용에 따라 정보주체의 개인정보 침해가 우려되는 경우에 그 위험요인의 분석과 개선 사항 도출을 위한 평가를 말한다.
18. “모바일 기기”란 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿PC 등 개인정보 처리에 이용되는 휴대용 기기를 말한다.
19. “공개된 무선망”이란 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.
20. 삭제 <2024.10.10.>
21. “이용자”란 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제4호에 따른 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자를 말한다.
22. “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.

23. “생체인식정보”란 생체정보 중 특정 개인을 인증 또는 식별할 목적으로 일정한 기술적 수단을 통해 처리되는 정보를 말한다.

제3조(적용 범위) 이 지침은 전자적 파일과 인쇄물, 서면 등 모든 형태의 개인정보 처리와 이를 취급하는 내부직원 및 외부업체 직원 등에 대하여 적용한다.

제4조(개인정보 보호 원칙) ① 개인정보처리자는 개인정보 처리 목적을 명확하게 하여야 하고, 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다. <개정 2020.10.13.>

② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니된다. <개정 2020.10.13.>

③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 하고, 개인정보를 처리하는 과정에서 고의 또는 과실로 부당하게 변경 또는 훼손되지 않도록 하여야 한다. <개정 2020.10.13.>

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. <개정 2020.10.13.>

⑤ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개

하여야 하며, 열람청구권 등 정보주체의 권리가 보장될 수 있도록 합리적인 절차와 방법 등을 마련하여야 한다. <신설 2023.11.28.>

⑥ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적법하게 개인정보를 처리하는 경우에도 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다. <신설 2023.11.28.>

⑦ 개인정보처리자는 개인정보를 적법하게 수집한 경우에도 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. <신설 2020.10.13., 개정 2023.11.28.>

⑧ 개인정보처리자는 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다. <신설 2023.11.28.>

제5조(다른 규정과의 관계) 개인정보의 처리 및 보호 등에 관하여 다른 특별한 규정이 있는 경우를 제외하고는 이 지침이 정하는 바에 따른다.

제2장 개인정보의 처리기준

제1절 개인정보의 처리

제6조(개인정보의 수집·이용) ① 심사평가원은 다음 각 호의 어느 하나에 해당하는 경우 개인정보를 수집할 수 있으며, 그 수집 목적의 범위에서 이용할 수 있다. <개정 2023.11.28., 2024.10.10.>

1. 정보주체로부터 사전에 동의를 받은 경우

2. 법률에서 개인정보를 수집·이용할 수 있음을 구체적으로 명시하거나 허용하고 있는 경우
3. 법령에서 심사평가원에 구체적인 의무를 부과하고 있고, 심사평가원이 개인정보를 수집·이용하지 않고는 그 의무를 이행하는 것이 불가능하거나 현저히 곤란한 경우
4. 심사평가원이 개인정보를 수집·이용하지 않고는 법령 등에서 정한 소관업무를 수행하는 것이 불가능하거나 현저히 곤란한 경우
5. 정보주체와 체결한 계약을 이행하거나 계약을 체결하는 과정에서 정보주체의 요청에 따른 조치를 이행하기 위하여 필요한 경우
6. 명백히 정보주체 또는 제3자(정보주체를 제외한 그 밖의 모든 자를 말한다)의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
7. 심사평가원이 법령 또는 정보주체와의 계약 등에 따른 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 다만, 심사평가원의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니한 경우에 한한다.
8. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우

② 심사평가원은 인터넷 홈페이지 등 공개된 매체 또는 장소(이하 “홈페이지 등”이라 함)에서 개인정보를 수집하는 경우 정보주체의 동의 의사가 명확히 표시되거나 홈페이지 등의 표시 내용에 비추어 사회통념상 동의 의사가 있었다고 인정되는 범위 내에서만 개인정보를 이용할 수 있다.

③ 심사평가원은 계약 등의 상대방인 정보주체가 대리인을 통하여 법률행위 또는 의사표시를 하는 경우 대리인의 대리권 확인을 위한 목적으

로만 대리인의 개인정보를 수집·이용할 수 있다.

④ 근로자와 사용자가 근로계약을 체결하는 경우 「근로기준법」에 따른 임금지급, 교육, 증명서 발급, 근로자 복지제공을 위하여 근로자의 동의 없이 개인정보를 수집·이용할 수 있다.

⑤ 개인정보처리자는 법 제15조제3항에 따라 당초 수집목적과 합리적으로 관련된 범위에서 정보주체에게 불이익이 발생하는지 여부, 가명처리 또는 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 대통령령 제14조의2에서 정하는 바에 따라 정보주체의 동의 없이 개인정보를 이용할 수 있다. <신설 2020.10.13., 개정 2023.11.28.>

제7조(개인정보의 제공) ① 법 제17조의 “제3자”란 정보주체와 정보주체에 관한 개인정보를 수집·보유하고 있는 심사평가원을 제외한 모든 자를 의미하며, 정보주체의 대리인(명백히 대리의 범위 내에 있는 것에 한한다)과 법 제26조제2항에 따른 수탁자는 제외한다(이하 같다).

② 심사평가원이 법 제17조제2항제1호에 따라 정보주체에게 개인정보를 제공받는 자를 알리는 경우에는 그 성명(법인 또는 단체인 경우에는 그 명칭)과 연락처를 함께 알려야 한다.

③ 개인정보처리자가 개인정보를 국외의 제3자에게 제공할 때에는 법 제28조의8 제1항에 따라야 하며, 제1항1호에 따라 정보주체에게 동의를 받아야 하는 경우에는 법 제28조의8 제2항 각 호에 따른 사항을 정보주체에게 알려야 하며, 법을 위반하는 내용으로 개인정보의 국외 이전에 관한 계약을 체결하여서는 아니 된다. <신설 2020.10.13.> <개정 2023.11.28.>

④ 개인정보처리자는 법 제17조제4항에 따라 당초 수집목적과 합리적으

로 관련된 범위에서 정보주체에게 불이익이 발생하는지 여부, 가명처리 또는 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 대통령령 제14조의2에서 정하는 바에 따라 정보주체의 동의 없이 개인정보를 제공할 수 있다. <신설 2020.10.13.> <개정 2023.11.28.>

제8조(개인정보의 목적 외 이용·제공 제한) ① 부서별 개인정보책임자는 법 제18조제2항에 따라 개인정보를 목적 외의 용도로 이용하거나 제3자에게 제공하는 경우에는 그 내역을 별지 제1호서식 개인정보의 목적 외 이용 및 제3자 제공 대장에 기록하여 개인정보 보호관리자에게 통보하여야 한다. <개정 2021.9.23.>

② 부서별 개인정보책임자는 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 개인정보의 안전성 확보를 위하여 필요한 조치를 하여야 한다.

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

④ 삭제 <2021. 9. 23.>

제9조(정보주체 이외로부터 수집한 개인정보의 수집출처 등 통지)

① 부서별 개인정보책임자는 정보주체 이외로부터 수집한 개인정보를 처리하는 때에는 정보주체의 요구가 있으면 3일 이내 다음 각 호의 모든 사항을 정보주체에게 알려야 한다. <개정 2023.11.28., 2024.10.10.>

1. 개인정보의 수집 출처
2. 개인정보의 처리 목적
3. 법 제37조에 따라 개인정보의 처리 정지를 요구하거나 동의를 철회할 권리가 있다는 사실

② 부서별 개인정보책임자는 타 기관의 개인정보처리자로부터 개인정보를 제공받은 경우(정보주체의 개인정보를 제3자에게 제공하겠다는 동의를 받은 경우에 한함), 제공받은 날로부터 3개월 이내에 서면·전화·문자전송·전자우편 등 정보주체가 쉽게 알 수 있는 방법으로 제1항 각 호의 모든 사항을 정보주체에게 알려야 한다. 다만, 제공받은 자료 중 연락처 등 정보주체에게 알릴 수 있는 개인정보가 포함되지 아니한 경우에는 그러하지 아니하다.

③ 제2항에 따라 알리는 경우 다음 각 호의 사항을 해당 개인정보를 파기할 때까지 보관·관리하여야 한다.

1. 정보주체에게 알린 사실
2. 알린 시기
3. 알린 방법

④ 제1항 또는 제2항의 본문은 다음 각 호의 어느 하나에 해당하는 경우에는 적용하지 아니한다. 다만, 「개인정보보호법」에 따른 정보주체의 권리보다 명백히 우선하는 경우에 한한다. <개정 2024.10.10.>

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

[전문개정 2019. 6. 28.] [제목개정 2023.11.28.]

제9조의2(개인정보 이용·제공내역의 통지) ① 심사평가원은 법에 따라 수집한 개인정보의 이용·제공내역이나 이용·제공 내역을 확인할 수 있는 정보시스템에 접속하는 방법을 주기적으로 정보주체에게 통지하여야 한다. 다만, 연락처 등 정보주체에게 통지할 수 있는 개인정보를 수집·보유하지 아니한 경우에는 통지하지 아니할 수 있다.

② 정보주체에게 통지해야 하는 정보는 다음 각 호와 같다.

1. 개인정보의 수집 이용 목적 및 수집한 개인정보의 항목
2. 개인정보를 제공받은 자와 그 제공 목적 및 제공한 개인정보의 항목

③ 통지는 서면, 전자우편, 전화, 문자전송, 알림창 등 정보주체가 쉽게 알 수 있는 방법으로 연 1회 이상 해야 한다.

④ 통지의 대상이 되는 정보주체는 다음 각 호의 정보주체를 제외한 정보주체로 한다.

1. 통지에 대한 거부의사를 표시한 정보주체
2. 우리원이 업무수행을 위해 우리원에 소속된 임직원의 개인정보를 처리한 경우 해당 임직원
3. 우리원이 업무수행을 위해 다른 공공기관, 법인, 단체의 임직원 또는 개인의 연락처 등의 개인정보를 처리한 경우 해당 정보주체
4. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 이용·제공한 개인정보의 정보주체
5. 우리원이 법령 등에서 정하는 소관 업무의 수행을 위하여 이용·제공한 개인정보의 정보주체

[본조신설 2023.11.28.]

제10조(개인정보의 파기방법 및 절차) ① 심사평가원은 개인정보의 보유기간이 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. 다만, 「공공기록물 관리에 관한 법률」 및 심사평가원 「기록물관리규정」 등에 따라 보존하여야 하는 경우에는 그러하지 아니하다.

② 제1항에 따라 심사평가원이 개인정보를 파기할 경우 다음 각 호 중 어느 하나의 조치를 하여야 한다. <개정 2023.11.28.>

1. 전자적 파일형태인 경우: 복원이 불가능한 방법으로 영구 삭제. 다만, 기술적 특성으로 영구 삭제가 현저히 곤란한 경우에는 법 제58조의2에 해당하는 정보로 처리하여 복원이 불가능하도록 조치해야 한다.
2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우: 파쇄 또는 소각

③ 심사평가원이 개인정보의 일부만을 파기하는 경우, 제2항의 방법으로 파기하는 것이 어려울 때에는 다음 각 호의 조치를 하여야 한다. <개정 2022.10.25., 2023.11.28.>

1. 전자파일: 삭제 후 복구 및 재생되지 않도록 관리, 감독
2. 기록물, 인쇄물, 서면: 마스킹, 천공 등의 방법으로 삭제

④ 개인정보 보호책임자는 개인정보의 파기 에 관한 사항을 기록·관리하여야 하며, 개인정보 파기 절차·파기 여부의 확인 등을 포함하는 파기계획을 수립하고 주기적으로 점검하는 등 필요한 조치를 하여야 한다. <개정 2023.11.28.>

⑤ 개인정보파일 파기에 관하여는 제62조를 준용한다. <개정

2023.11.28.>

제11조(고유식별정보·민감정보의 처리 등) ① 심사평가원은 다음 각 호의 어느 하나에 해당하는 경우에는 고유식별정보 또는 민감정보를 처리할 수 있다.

1. 정보주체에게 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 구체적으로 고유식별정보 또는 민감정보의 처리를 요구하거나 허용하는 경우

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

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

③ 제1항에도 불구하고 심사평가원은 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리(온라인·오프라인을 포함한다. 이하 같다)할 수 없다. <개정 2020.10.13.>

1. 법령에서 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 주민등록번호의 처리가 불가피한 경우로서

개인정보보호위원회가 고시로 정하는 경우

제11조의2(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 2020.10.13.]

제11조의3(가명정보의 결합 제한) ① 결합을 수행한 기관 외부로 결합된 정보를 반출하려는 개인정보처리자는 가명정보 또는 법 제58조의2에 해당하는 정보로 처리한 뒤 원장의 승인을 받아야 한다. <개정 2024.10.10.>

② 기타 가명정보의 결합에 대해서는 「가명정보의 결합 및 반출 등에 관한 업무지침」에 따른다. <신설 2023.11.28.>

[본조신설 2020.10.13.]

제11조의4(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 대통령령 제29조의5에서 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

② 개인정보처리자는 법 제28조의2 또는 제28조의3에 따라 가명정보를 처리하는 경우 처리목적 등을 고려하여 가명정보의 처리 기간을 별도로 정할 수 있다. <개정 2023.11.28.>

③ 개인정보처리자는 가명정보를 처리하고자 하는 경우에는 가명정보의 처리 목적, 제3자 제공 시 제공받는 자 등 가명정보의 처리 내용을 관리하기 위하여 대통령령으로 정하는 다음 각 호의 사항에 대한 관련 기록을 작성하여 보관하여야 하며, 가명정보를 파기한 경우에는 파기한 날로부터 3년 이상 보관하여야 한다. <신설 2023.11.28.>

[본조신설 2020.10.13.]

제11조의5(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 2020.10.13.]

제12조(법령에 따른 개인정보의 보존) ① 개인정보 보호책임자가 법 제21조 제1항 단서에 따라 법령에 근거하여 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 물리적 또는 기술적 방법으로 분리하여서 저장·관리하여야 한다.

② 개인정보 보호책임자가 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.

제13조(동의를 받는 방법) ① 심사평가원이 개인정보의 처리에 대하여 정보주체의 동의를 받을 때에는 정보주체의 동의 없이 처리할 수 있는 개인정보와 정보주체의 동의가 필요한 개인정보를 구분하여야 하며, 정보주체

의 동의는 동의가 필요한 개인정보에 한한다. 이 경우 동의 없이 처리할 수 있는 개인정보인지 여부에 대하여는 개인정보 보호책임자가 입증책임을 부담한다.

② 심사평가원은 다음 각 호의 어느 하나에 해당하는 경우에는 동의사항을 구분하여 각각 동의를 받아야 한다. <개정 2023.11.28.>

1. 개인정보를 수집·이용하고자 하는 경우로서 법 제15조제1항제2호부터 제7호까지에 해당하지 않은 경우
2. 개인정보를 제3자에게 제공하는 경우로서 법 제17조제1항2호에 해당되지 않는 경우
3. 개인정보를 수집 목적 외의 용도로 이용하거나 제공하고자 하는 경우로서 법 제18조제2항제2호부터 제10호까지에 해당되지 않는 경우
4. 심사평가원 외부의 개인정보처리자로부터 개인정보를 제공받아 제공받은 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우로서 다른 법률에 처리 근거가 없는 경우
5. 민감정보를 처리하고자 하는 경우로서 법령에 민감정보 처리 근거가 없는 경우
6. 주민등록번호 외의 고유식별정보 처리가 필요한 경우로서 법령에 고유식별정보 처리 근거가 없는 경우
7. 법 제22조제1항제7호에 따라 정보주체에게 재화나 서비스를 홍보하거나 판매를 권유하고자 하는 경우

③ 심사평가원은 제2항 각 호의 어느 하나에 해당하여 개인정보를 처리하고자 하는 경우에는 정보주체에게 동의 또는 동의 거부를 선택할 수 있음을 명시적으로 알려야 한다.

④ 심사평가원은 법 제15조제1항제2호부터 제7호까지에 따라 정보주체의 동의 없이 처리할 수 있는 개인정보에 대해서는 그 항목과 처리의 법적 근거를 정보주체의 동의를 받아 처리하는 개인정보와 구분하여 개인정보처리방침에 공개하거나 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법(“서면등의 방법”이라 한다)으로 정보주체에게 알려야 한다. 이 경우 동의없이 처리할 수 있는 개인정보라는 입증책임은 개인정보처리자가 부담한다. <개정 2023.11.28.>

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

⑥ 심사평가원이 정보주체의 동의를 받기 위하여 동의서를 작성하는 경우에는 「알기쉬운 개인정보 처리 동의 안내서」를 준수하여야 한다. <개정 2020.10.13., 2022.10.25., 2023.11.28.>

⑦ 법에 따른 정보주체의 동의가 적법하기 위해서는 다음 각 호의 조건을 충족하여야 한다. <신설 2023.11.28.>

1. 정보주체가 자유로운 의사에 따라 동의 여부를 결정할 수 있을 것
2. 동의 내용이 구체적이고 명확할 것
3. 평이하고 이해하기 쉬운 문구를 사용할 것
4. 정보주체에게 동의 여부에 대한 의사를 명확하게 표시할 수 있는 방법을 제공할 것

제14조(법정대리인의 동의) ① 심사평가원이 영 제17조제2항에 따라 법정대리인의 성명·연락처를 수집할 때에는 해당 아동에게 자신의 신분과 연락처, 법정대리인의 성명과 연락처를 수집하고자 하는 이유를 알려야 한다. <개정 2023.11.28.>

② 심사평가원은 법 제22조의2제2항에 따라 수집한 법정대리인의 개인정보를 법정대리인의 동의를 얻기 위한 목적으로만 이용하여야 하며, 법정대리인의 동의 거부가 있거나 법정대리인의 동의 의사가 확인되지 않는 경우 수집일로부터 5일 이내에 파기하여야 한다. <개정 2023.11.28.>

제15조(정보주체의 사전 동의를 받을 수 없는 경우) 심사평가원이 법 제15조제1항제5호 및 법 제18조제2항제3호에 따라 정보주체의 사전 동의없이 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.

제16조(개인정보취급자에 대한 감독) ① 부서별 개인정보책임자는 개인정보취급자를 업무상 필요한 한도 내에서 최소한으로 두어야 하며, 개인정보취급자의 개인정보 처리 범위를 업무상 필요한 한도 내에서 최소한으로 제한하여야 한다.

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

③ 부서별 개인정보책임자는 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

제17조(개인정보의 처리 업무 위탁 시 조치사항) ① 심사평가원이 제3자에게 개인정보의 처리 업무를 위탁하는 경우 다음 각 호의 내용이 포함된

문서에 의하여야 한다.

1. 위탁업무 수행목적 외 개인정보의 처리금지에 관한 사항
2. 개인정보의 기술적·관리적 보호조치에 관한 사항
3. 위탁업무의 목적 및 범위
4. 재위탁 제한에 관한 사항
5. 개인정보에 대한 접근 제한 등 안전성 확보조치에 관한 사항
6. 위탁업무와 관련하여 보유하고 있는 개인정보의 관리현황 점검 등 감독에 관한 사항
7. 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

② 제1항에 따라 개인정보의 처리 업무를 위탁하는 경우 심사평가원은 정보주체가 쉽게 확인할 수 있도록 홈페이지에 위탁하는 업무의 내용과 수탁자를 지속적으로 게재하여야 한다.

③ 심사평가원은 제2항에 따라 홈페이지에 게재할 수 없는 경우에는 다음 각 호 중 어느 하나 이상의 방법으로 위탁하는 업무의 내용과 수탁자를 공개하여야 한다.

1. 심사평가원의 보기 쉬운 장소에 게시하는 방법
2. 같은 제목으로 연 2회 이상 발행하여 정보주체에게 배포하는 간행물·소식지·홍보지 또는 청구서 등에 지속적으로 싣는 방법
3. 관보나 일반일간신문, 일반주간신문 또는 인터넷신문에 싣는 방법
4. 재화나 용역을 제공하기 위하여 심사평가원과 정보주체가 작성한 계약서 등에 실어 정보주체에게 발급하는 방법

④ 심사평가원은 정보주체의 개인정보가 분실·도난·유출·변조 또는

훼손이 되지 않도록 수탁자를 교육하여야 한다.

⑤ 수탁자는 심사평가원으로부터 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하여서는 아니 된다. <신설 2024.10.10.>

⑥ 수탁자는 위탁받은 개인정보의 처리 업무를 제3자에게 다시 위탁하려는 경우에는 심사평가원의 동의를 받아야 한다. <신설 2024.10.10.>

⑦ 수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 법을 위반하여 발생한 손해배상책임에 대하여는 수탁자를 심사평가원의 소속 직원으로 본다. <신설 2024.10.10.>

제18조(개인정보보호 조치의무) 수탁자는 위탁받은 개인정보를 보호하기 위하여 개인정보보호위원회 「개인정보의 안전성 확보조치 기준」에 따른 관리적·기술적·물리적 조치를 하여야 한다. <개정 2020.10.13., 2024.10.10.>

제3절 개인정보 처리방침의 수립 및 공개

제19조(개인정보 처리방침의 작성기준 등) ① 개인정보 보호책임자는 개인정보 처리방침을 작성하는 때에는 법 제30조제1항 각 호 및 법 시행령 제31조제1항 각 호의 사항을 명시적으로 구분하되, 알기 쉬운 용어로 구체적이고 명확하게 표현하여야 한다.

② 개인정보 처리방침에는 처리하는 개인정보가 개인정보의 처리 목적에 필요 최소한이라는 점을 밝혀야 한다.

제20조(개인정보 처리방침의 기재사항) 개인정보 보호책임자가 개인정보

처리방침을 작성할 때에는 법 제30조제1항에 따라 다음 각 호의 사항을 모두 포함하여야 한다. <개정 2024.10.10.>

1. 개인정보의 처리 목적
2. 처리하는 개인정보의 항목
3. 개인정보의 처리 및 보유기간
4. 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다)
5. 개인정보의 파기절차 및 파기방법
6. 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다)
7. 개인정보의 안전성 확보조치에 관한 사항
8. 정보주체의 권리·의무 및 그 행사방법에 관한 사항
9. 개인정보 처리방침의 변경에 관한 사항
10. 개인정보 보호책임자의 성명 또는 개인정보 보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처
11. 개인정보의 열람청구를 접수·처리하는 부서
12. 정보주체의 권익침해에 대한 구제방법
13. 민감정보의 공개 가능성 및 비공개를 선택하는 방법(해당되는 경우에만 정한다)
14. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항(해당되는 경우에만 정한다)

제21조(개인정보 처리방침의 공개) ① 개인정보 보호책임자는 개인정보 처리방침을 수립하거나 변경하는 경우 홈페이지를 통하여 지속적으로 게재하여야 한다. 이 경우 “개인정보 처리방침”이라는 명칭을 사용하되, 글자의 크기·색상 등을 활용하여 다른 고지사항과 구분함으로써 정보

주체가 쉽게 확인할 수 있도록 하여야 한다.

② 개인정보 보호책임자가 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 보호체계

제22조(개인정보 보호책임자) ① 개인정보 보호책임자는 심사평가원 「직제규정」에 따라 개인정보 보호에 관한 사항을 관장하는 상임이사로 한다.

② 개인정보 보호책임자는 심사평가원이 처리하는 개인정보와 관련된 다음 각 호의 업무를 수행한다. <개정 2023.11.28.>

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 오·남용 방지를 위한 내부통제시스템의 구축
5. 개인정보 보호 교육 계획의 수립 및 시행
6. 개인정보파일의 보호 및 관리·감독
7. 개인정보 처리방침의 수립·변경 및 시행
8. 개인정보 보호 관련 자료의 관리
9. 처리목적이 달성되거나 보유기간이 경과한 개인정보의 파기 및 관리·감독
10. 개인정보 처리시스템 운영 및 위탁 업무 총괄 관리
11. 개인정보 처리시스템의 안전성 확보를 위한 기술적·관리적·물리적

보호조치 총괄

12. 삭제 <2023.11.28.>

13. 부서별 개인정보책임자 지휘・감독

14. “개인정보 보호의 날” 지정 및 운영

15. 그 밖에 개인정보 보호를 위하여 필요한 사항

제23조(개인정보 보호관리자) ① 개인정보 보호관리자는 심사평가원 「직제규정」에 따라 개인정보 보호에 관한 업무를 담당하는 부서의 장으로 한다.

② 개인정보 보호관리자는 심사평가원이 처리하는 개인정보와 관련된 다음 각 호의 업무를 수행한다. <개정 2019. 6. 28.>

1. 개인정보 보호 계획 및 개인정보 처리방침의 운영

2. 개인정보 침해 대응

3. 개인정보 처리실태 관리 및 관련자료 수집

4. 개인정보 처리시스템 연계 등 시스템 관련 업무

5. 개인정보 관련 법령 및 지침 등 기준 검토

6. 개인정보 관제 결과에 대한 소명 및 부적정 현황 관리

7. 그 밖에 개인정보 보호책임자가 위임한 사항

제24조(부서별 개인정보책임자) ① 부서별 개인정보책임자는 개인정보를 처리하는 각 부서의 장으로 한다.

② 부서별 개인정보책임자는 소관 개인정보파일 및 개인정보 처리시스템 등에 대하여 다음 각 호의 업무를 수행한다.

1. 개인정보취급자의 지정・관리・감독・교육

2. 개인정보파일의 지정・관리・등록・공개・파기

3. 개인정보 보호 관련 자료 관리 및 제출

4. 개인정보와 관련한 요구 처리 및 피해 구제
5. 개인정보 관련 개선, 권고, 시정 등 조치사항 이행
6. 개인정보 처리시스템의 사용자 권한설정 및 관리
7. 개인정보 처리 사항에 대한 기록 관리
8. 개인정보 처리시스템의 운영 및 위탁 업무의 관리
9. 개인정보 처리시스템의 안전성 확보를 위한 기술적·관리적·물리적 보호조치 수행
10. 개인정보 보호책임자에 대한 개인정보 처리현황 수시 보고
11. 그 밖에 개인정보 보호를 위하여 필요한 사항

③ 부서별 개인정보책임자는 개인정보취급자를 업무상 필요한 한도 내에서 최소한으로 두어야 하며, 개인정보취급자의 개인정보 처리 범위를 업무상 필요한 한도 내에서 최소한으로 제한하여야 한다.

제25조(개인정보취급자) 개인정보취급자는 제24조에 따른 부서별 개인정보책임자의 지휘·감독 하에 부서책임자의 업무를 보좌하며 다음 각 호의 업무를 수행한다.

1. 개인정보파일 보호 및 관리(개인정보 수집·보유·이용·제공·파기의 모든 단계에 해당한다)
2. 개인정보파일의 등록·변경·파기 신청
3. 웹사이트에 게재되는 개인정보의 안전 관리
4. 개인정보의 열람·정정·삭제 시 보호 관리
5. 그 밖에 개인정보 보호를 위하여 필요한 사항

제26조(개인정보보호 심의위원회 구성) ① 개인정보의 처리 및 보호에 관한 다음 각 호의 사항을 심의하기 위하여 개인정보보호 심의위원회(이하

“위원회”라 한다)를 둔다.

1. 개인정보 보호 관련 제도의 개선에 관한 사항
2. 개인정보 이용 또는 제공(건강・질병정보 등의 원시자료, MOU 등 업무협약에 따른 정보 제공을 포함한다)에 관한 사항
3. 그 밖에 개인정보 보호를 위하여 심의가 필요한 사항

② 위원회의 위원장은 개인정보 보호책임자로 한다.

③ 위원회는 위원장을 포함한 5인 이내의 위원으로 구성하며, 위원은 다음 각 호에 해당하는 자 중 회의 개최 시마다 위원장이 지명한다.

1. 개인정보 보호관리자
2. 법규 업무를 담당하는 부서의 장
3. 안건 관련 부서별 개인정보책임자
4. 학계・변호사(심사평가원 촉탁직 변호사를 포함한다) 등 개인정보 보호 관련 전문가
5. 그 밖에 위원회 참석이 필요하다고 위원장이 인정하는 자

④ 위원회 관련 사무를 처리하기 위하여 간사를 둔다. 이 경우 간사는 「직제규정 시행세칙」에 따라 개인정보 보호에 관한 업무를 담당하는 부의 장으로 한다.

제27조(개인정보보호 심의위원회 운영) ① 위원장은 필요하다고 인정하는 경우에 위원회의 회의를 소집하고 그 의장이 된다.

② 위원회의 회의는 위원 3분의 2이상의 출석으로 개의하고, 출석위원 과반수의 찬성으로 의결한다.

③ 제2항에도 불구하고 위원장은 사안이 경미하거나 긴급하다고 인정하는 경우 서면결의를 할 수 있다. 이 경우 위원 과반수의 찬성으로 의결한다.

④ 위원회의 심의·의결은 별지 제2호서식 의결서에 따르며, 서면결의의 경우에는 별지 제3호서식 서면결의서에 따른다.

⑤ 부서별 개인정보책임자는 개인정보의 처리 및 보호와 관련하여 판단하기 곤란한 사안이 있는 경우 별지 제4호서식 안건부의서에 따라 위원회에 심의·의결을 요청할 수 있다.

⑥ 위원장은 심의·의결에 필요한 경우 해당 부서에 자료를 요구하거나 직원으로 하여금 회의에 참석하여 진술하도록 할 수 있다. 이 경우 요청을 받은 부서 또는 직원은 특별한 사유가 없는 한 이에 응하여야 한다.

⑦ 간사는 회의 개최 시 회의록을 작성하여 출석위원 전원의 서명을 받아 보관하여야 한다.

⑧ 위원 또는 관련자는 외부에 공표된 것을 제외하고는 위원회 회의 등을 통해 알게 된 사항을 누설하여서는 아니 된다.

⑨ 위원회의 회의에 참석한 외부위원에 대하여는 예산의 범위 내에서 수당 및 필요한 경비를 지급할 수 있다.

⑩ 그 밖에 위원회 운영에 필요한 사항은 위원장이 정한다.

제5절 개인정보 보호 교육 등

제28조(개인정보 보호 교육) ① 개인정보 보호책임자는 매년 초 해당 연도의 개인정보 보호 교육계획을 수립한다. 이 경우 교육계획에는 다음 각 호의 사항을 포함되어야 한다.

1. 교육 목적 및 대상
2. 교육 내용

3. 교육 일정 및 방법

② 개인정보 보호 교육은 정기교육과 수시교육으로 구분하여 다음 각 호에 따라 실시한다.

1. 정기교육: 연 1회 이상 전 직원 대상으로 실시

2. 수시교육: 개인정보 보호를 위하여 필요한 경우 실시

③ 개인정보 보호책임자는 교육의 품질 향상을 위하여 다음 각 호의 방법으로 교육을 실시할 수 있다. <개정 2020.10.13.>

1. 개인정보 보호 관련 전문강사 초청 교육

2. 외부기관 또는 심사평가원 자체 온라인 교육

3. 개인정보보호위원회, 한국인터넷진흥원 등에서 실시하는 교육과정 참여

제29조(개인정보 보호의 날) 개인정보 보호책임자는 개인정보 보호 관련 법령 및 심사평가원 제규정 등 이행여부를 주기적으로 점검하기 위하여 매월 「개인정보 보호의 날」을 지정하여 운영한다.

제30조(개인정보 보호 조치) ① 개인정보 보호책임자는 개인정보 보호의 자체점검을 위한 점검 대상·절차 및 방법 등 점검의 실시에 관하여 필요한 경우 별도의 계획을 수립하여 시행할 수 있다.

② 개인정보 보호책임자는 개인정보의 관리·운영상 문제점이나 이 지침에 대한 위반사항을 발견한 때에는 그에 대한 시정, 개선 등 필요한 조치를 하여야 한다.

③ 개인정보 보호책임자는 제2항의 시정, 개선 등 조치가 이행되지 아니하거나 개인정보 보호에 심각한 영향을 초래할 수 있다고 판단되는 경우에는 개인정보취급자 등에 대한 인사발령 요청 등 필요한 추가 조치를 할 수 있다.

제6절 개인정보 유출등의 통지 및 신고 등

제31조(개인정보의 유출등) 개인정보의 분실·도난·유출(이하 “유출등”이라 한다)은 다음 각 호의 어느 하나에 해당하는 경우를 말한다. <개정 2024.10.10.>

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. 개인정보가 포함된 파일 또는 종이문서, 그 밖의 저장매체가 권한이 없는 자에게 잘못 전달된 경우
4. 그 밖에 권한이 없는 자에게 개인정보가 전달된 경우

[제목개정 2023.11.28., 2024.10.10.]

제32조(유출등의 통지시기 및 항목) ① 개인정보 보호책임자는 개인정보가 유출등이 되었음을 알게 된 때에는 정당한 사유가 없는 한 72시간 이내에 해당 정보주체에게 다음 각 호의 사항을 알려야 한다. <개정 2023.11.28., 2024.10.10.>

1. 유출등이 된 개인정보의 항목
2. 유출등이 된 시점과 그 경위
3. 유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
4. 심사평가원의 대응조치 및 피해구제절차
5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서

및 연락처

② 제1항에도 불구하고 개인정보 보호책임자는 유출등이 된 개인정보의 확산 및 추가 유출등을 방지하기 위하여 접속경로의 차단, 취약점 점검 보완, 유출된 개인정보의 삭제 등 긴급한 조치가 필요한 경우에는 그 조치를 한 후 그로부터 72시간 이내에 정보주체에게 알릴 수 있다. <개정 2023.11.28., 2024.10.10.>

③ 개인정보 보호책임자는 제1항 각 호의 사항을 모두 확인하기 어려운 경우에는 정보주체에게 다음 각 호의 사실만을 우선 알리고, 추후 확인되는 즉시 알릴 수 있다. <개정 2023.11.28., 2024.10.10.>

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

④ 개인정보 보호책임자는 개인정보 유출등의 사고를 인지하지 못해 유출등의 사고가 발생한 시점으로부터 72시간 이내에 해당 정보주체에게 개인정보 유출등의 통지를 하지 아니한 경우에는 실제 유출등의 사고를 알게 된 시점을 입증하여야 한다. <신설 2024.10.10.>

[제목개정 2023.11.28., 2024.10.10.]

제33조(유출등의 통지방법) ① 개인정보 보호책임자는 정보주체에게 제32조제1항 각 호의 사항을 통지할 때에는 서면 등의 방법을 통하여 정보주체에게 알려야 한다. <개정 2023.11.28.>

② 개인정보 보호책임자는 제1항에 따라 통지하는 경우 홈페이지 등을 통하여 제32조제1항 각 호의 사항을 공개할 수 있다.

③ 다만 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 제32조제1항 각 호의 사항을 심사평가원 홈페이지에 30일 이

상 게시하는 것으로 제1항의 통지를 갈음할 수 있다. <신설 2023.11.28.>

[제목개정 2023.11.28., 2024.10.10.]

제34조(개인정보 유출등의 신고) ① 개인정보 보호책임자는 다음 각 호의 어느 하나에 해당하는 경우로서 개인정보가 유출등이 되었음을 알게 되었을 때에는 정당한 사유가 없는 한 서면 등의 방법으로 72시간 이내에 법 34조제1항 각 호의 사항을 보건복지부장관에게 보고하고, 개인정보보호위원회 또는 한국인터넷진흥원에 신고하여야 한다. 이 경우 별지 제5호서식 개인정보 유출등 신고서를 작성하여 보고 및 신고하여야 한다. 다만, 개인정보 유출등의 경로가 확인되어 해당 개인정보를 회수, 삭제하는 등의 조치를 통해 정보주체의 권익 침해 가능성이 현저히 낮은 경우에는 그러하지 아니하다. <개정 2020.10.13., 2023.11.28., 2024.10.10.>

1. 1천명 이상의 정보주체에 관한 개인정보가 유출등이 된 경우
2. 민감정보, 고유식별정보가 유출등이 된 경우
3. 개인정보처리시스템 또는 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대한 외부로부터의 불법적인 접근에 의해 개인정보가 유출등이 된 경우

② 제1항에도 불구하고 개인정보 보호책임자는 제1항에 따른 신고를 하려는 경우에는 법 제34조제1항제1호 또는 2호의 사항에 관한 구체적인 내용을 확인하지 못한 경우에는 그때까지 확인된 내용 및 같은 항 제3호부터 제5호까지의 사항을 서면등의 방법으로 우선 신고한 후 추가로 확인되는 내용에 대해서는 확인되는 즉시 신고해야 한다. <개정 2023.11.28.>

[제목개정 2023.11.28., 2024.10.10.]

제35조(개인정보 위험도 분석) ① 개인정보 보호책임자는 개인정보 유출에 영향을 미칠 수 있는 다양한 위험요소를 식별·평가하는 등 위험도 분석을 통해 개인정보 유출에 대비하여야 한다. <개정 2019. 6. 28.>

② 심사시스템, 데이터시스템 등 개인정보처리시스템 운영부서의 부서별 개인정보책임자는 연 1회 파일 단위로 위험도 분석을 실시한 후, 결과보고서를 작성하여 보관하여야 한다. 다만, 개인정보파일을 외부 기관에 위탁한 경우에는 위험도 분석, 결과보고서 작성 및 보관을 수탁 기관에서 수행하여야 한다.

③ 위험도 분석은 다음 각 호의 절차를 따른다.

1. 위험도 분석을 위한 개인정보파일 및 고유식별정보 보유 여부 등 현황조사
2. 개인정보 파일 단위로 위험도 분석 항목별 점검 수행
3. 위험도 분석 결과보고서를 작성하여 내부결재를 받은 후 보관
4. 점검 결과에 따라 고유식별정보 암호화 등 수행

[제목개정, 전문개정 2019. 6. 28.]

제35조의2(유출등 사고 대응 매뉴얼) ① 개인정보 보호책임자는 유출등 사고 발생 시 신속한 대응을 통해 피해 발생을 최소화하기 위하여 개인정보 유출등 사고 대응 매뉴얼을 마련하여야 한다. <개정 2023.11.28., 2024.10.10.>

② 제1항에 따른 개인정보 유출등 사고 대응 매뉴얼에는 유출등 사고 통지·조회 절차, 인터넷회선 확충 등 고객 민원 대응조치, 현장 혼잡 최소화 조치, 고객불안 해소조치, 피해자 구제조치 등을 포함하여야 한다. <개정 2023.11.28., 2024.10.10.>

③ 개인정보 보호책임자는 개인정보 유출등에 따른 피해복구 조치 등을 수행함에 있어 정보주체의 불편과 경제적 부담을 최소화할 수 있도록 노력하여야 한다. <신설 2024.10.10.>

[본조신설 2019. 6. 28.] [제목개정 2023.11.28., 2024.10.10.]

제36조(침해대응절차) ① 심사평가원 임직원은 개인정보에 대하여 침해가 발생한 것을 인지한 경우 또는 그러한 침해의 발생이 의심되는 경우에는 별지 제6호서식 개인정보 침해사실 신고서를 작성하여 지체 없이 개인정보 보호관리자에게 신고하여야 한다.

② 개인정보 보호관리자는 개인정보 침해신고를 접수한 즉시 개인정보 보호책임자에게 보고하여야 한다.

③ 개인정보 보호책임자는 노출 또는 제공된 개인정보의 종류에 따라 개인정보 침해사고 발생 부서의 부서별 개인정보책임자를 개인정보 침해사고 처리책임자(이하 “처리책임자”라 한다)로 지정하고 개인정보 침해사고 대응팀(이하 “대응팀”이라 한다)을 구성하여야 한다. 다만, 개인정보 침해사고 발생 부서를 특정하기 곤란하거나 부서별 개인정보책임자가 침해사고에 연루된 경우에는 개인정보 보호책임자가 처리책임자를 지정할 수 있다.

④ 대응팀은 다음 각 호에 따라 침해사고에 대한 분석을 수행한다.

1. 침해사실 여부 확인 후 사실로 확인된 경우 침해의 규모, 경위, 방법, 원인 및 관련자 등 조사
2. 필요한 경우 대응팀 또는 개인정보 보호책임자가 승인한 외부 전문가의 지원을 받아 증거자료 수집

⑤ 처리책임자는 침해의 정도에 따라 해당 개인정보를 파기, 회수 또는

복구하기 위한 조치를 하거나 정보주체의 사후 동의를 받아 근거를 마련하여야 한다.

⑥ 대응팀은 다음 각 호의 절차를 통하여 침해사고에 대한 모든 행위를 종료할 수 있다.

1. 처리책임자는 별지 제7호서식 개인정보 침해사고 처리결과 통지서를 작성하여 개인정보 보호책임자에게 제출하고, 개인정보 보호 책임자는 개인정보 침해사고 결과보고서 검토 및 원장 보고
2. 개인정보 보호책임자는 개인정보 침해사고 관련자에 대한 처분을 심사평가원 「직제규정」에 따라 감사업무를 담당하는 부서에 통지

제37조(피해구제절차) ① 처리책임자는 개인정보 침해사고 발생 시 정보주체에게 개인정보의 열람·정정·삭제 청구권 및 불복 절차를 안내하여야 한다.

② 처리책임자는 개인정보 침해신고가 접수된 경우 접수일로부터 7일 이내에 신고인에 대한 상담 및 안내를 실시하여야 한다.

③ 처리책임자는 제2항에 따른 상담 및 안내를 한 날부터 30일 이내에 개인정보 침해사고의 경위, 피해범위 등을 조사하고 그 결과를 통지하여야 한다.

제7절 정보주체의 권리 보장

제38조(개인정보의 열람) ① 개인정보 보호책임자는 정보주체로부터 별지 제8호서식 개인정보 열람요구서를 받은 경우 해당 개인정보를 직접 보유·운영하는 부서의 부서별 개인정보책임자에게 이를 처리하도록 하여야 한다.

② 제1항에 따라 부서별 개인정보책임자가 개인정보 열람요구서를 처리하는 때에는 개인정보 열람요구서가 접수된 날부터 10일 이내에 개인정보 열람에 필요한 조치를 취하고 별지 제9호서식 개인정보 열람/일부열람/열람연기/열람거절 통지서에 따른 그 결과를 정보주체에게 알려야 한다.

③ 제2항의 기간 내에 개인정보를 열람할 수 없는 정당한 사유가 있는 경우 부서별 개인정보책임자는 별지 제9호서식 개인정보 열람/일부열람/열람연기/열람거절 통지서에 따라 정보주체에게 그 사유를 알리고 열람을 연기할 수 있으며, 그 사유가 소멸한 경우에는 사유가 소멸한 날로부터 10일 이내에 열람하도록 하여야 한다.

제39조(개인정보의 열람 제한 및 거절) ① 부서별 개인정보책임자는 개인정보 열람 요구사항이 법 제35조제4항 각 호의 어느 하나에 해당하는 경우에는 그 일부에 대하여 열람을 제한하거나 거절할 수 있다.

② 제1항에 따라 열람을 제한하거나 거절하는 경우에는 부서별 개인정보책임자는 개인정보 열람요구서가 접수된 날부터 10일 이내에 별지 제9호서식의 개인정보 열람/일부열람/열람연기/열람거절 통지서에 따라 그 사유 및 이의제기방법을 정보주체에게 알려야 한다.

제40조(개인정보의 정정·삭제 및 처리정지 등) ① 개인정보 보호책임자는 제38조에 따라 개인정보를 열람한 정보주체로부터 정정·삭제 및 처리정지 요구 또는 처리에 대한 동의 철회를 받은 경우 해당 개인정보를 직접 보유·운영하는 부서의 부서별 개인정보책임자에게 이를 처리하도록 하여야 한다. <개정 2023.11.28.>

② 제1항에 따라 부서별 개인정보책임자가 개인정보 정정·삭제 및 처리정지 요구 또는 처리에 대한 동의 철회를 처리하는 때에는 개인정보 정

정·삭제 및 처리정지 요구 또는 동의 철회를 받은 날부터 10일 이내에 필요한 조치를 취하고 별지 제10호서식 개인정보 정정·삭제, 처리정지 요구 또는 동의 철회에 대한 결과 통지서에 따라 그 결과를 정보주체에게 알려야 한다. 다만, 법 제37조제2항 단서에 해당하는 경우에는 부서별 개인정보책임자는 정보주체의 처리정지 요구 또는 동의 철회를 거절할 수 있다. <개정 2023.11.28.>

[제목개정 2023.11.28.]

제8절 개인정보의 안전성 확보조치

제41조(안전조치 기준 적용) 삭제 <2024.10.10.>

제42조(개인정보처리시스템) 심사평가원이 관리·운영하는 개인정보처리시스템은 다음 각 호와 같다.

1. 홈페이지 회원가입, 온라인 신청 등 개인정보를 수집하는 웹 서버
2. 그 밖에 데이터베이스 내에 개인정보를 포함한 시스템

제43조(내부 관리계획의 수립·시행) <삭제 2019. 6. 28.>

제44조(접근 권한의 관리) ① 부서별 개인정보책임자는 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 각 업무별 개인정보취급자에게 차등 부여하여야 한다. <개정 2019. 6. 28.>

② 개인정보 보호책임자는 전보 또는 퇴직 등 인사이동으로 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하여야 한다.

③ 개인정보 보호책임자는 제1항 및 제2항에 따른 권한 부여, 변경 또는

말소에 대한 내역을 기록하여 3년간 보관하여야 한다.

④ 개인정보 보호책임자는 개인정보처리시스템에 접속할 수 있는 사용자 계정을 개인정보취급자별로 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

⑤ 부서별 개인정보책임자는 개인정보취급자 또는 정보주체의 인증수단을 안전하게 적용하고 관리하여야 한다. <개정 2019. 6. 28., 2024.10.10.>

⑥ 개인정보 보호책임자는 권한있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 하여야 하며, 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우에는 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다.

⑦ 개인정보 보호책임자는 개인정보처리시스템에 대하여 다음 각 호의 내용이 포함된 권한관리지침을 수립하여 운영하여야 한다.

1. 권한에 대한 총괄 관리책임자 지정에 관한 사항
2. 사용자 등록, 권한 부여・변경・중지 등에 관한 사항
3. 사용자 및 정보 중요도별 접근권한 차등 부여에 관한 사항
4. 외부인력 및 업무보조자의 권한 관리에 관한 사항
5. 접근권한 관리이력 보관에 관한 사항
6. 보안서약서 징구 등에 관한 사항

제45조(접근 통제) ① 개인정보 보호책임자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위하여 다음 각 호의 기능을 포함한 시스템을 설치・운영하여야 한다.

1. 개인정보처리시스템에 대한 접속권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한

2. 개인정보처리시스템에 접속한 IP주소 등을 분석하여 불법적인 개인정보 유출시도 탐지

② 개인정보 보호책임자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 인증서, 보안토큰, 일회용 비밀번호 등 안전한 인증수단을 적용하여야 한다. 다만, 이용자가 아닌 정보주체의 개인정보를 처리하는 개인정보처리시스템의 경우 가상사설망 등 안전한 접속수단 또는 안전한 인증수단을 적용할 수 있다. <개정 2024.10.10.>

③ 개인정보 보호책임자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 등에 접근통제 등에 관한 조치를 하여야 한다. <개정 2024.10.10.>

④ 개인정보 보호책임자가 업무용 PC를 이용하여 개인정보를 처리하는 경우에는 운영체제의 방화벽이나 보안 프로그램 등에서 제공하는 접근통제기능을 이용하여야 한다.

⑤ 개인정보 보호책임자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하여야 한다.

제46조(개인정보의 암호화) ① 부서별 개인정보책임자는 비밀번호, 생체인식정보 등 인증정보를 저장 또는 정보통신망을 통하여 송·수신하는 경우에 이를 안전한 암호 알고리즘으로 암호화하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다. <개정 2019.6.28., 2022.10.25., 2024.10.10.>

② 부서별 개인정보책임자는 다음 각 호의 해당하는 이용자의 개인정보에 대해서는 안전한 암호 알고리즘으로 암호화하여 저장하여야 한다. <개정 2019.6.28., 2022.10.25., 2024.10.10.>

1. 주민등록번호
2. 여권번호
3. 운전면허번호
4. 외국인등록번호
5. 신용카드번호
6. 계좌번호
7. 생체인식정보

③ 부서별 개인정보책임자는 개인정보를 정보통신망을 통하여 인터넷망 구간으로 송·수신하는 경우에는 이를 안전한 암호 알고리즘으로 암호화하여야 한다. <개정 2019.6.28., 2024.10.10.>

④ 부서별 개인정보책임자는 이용자가 아닌 정보주체의 개인정보를 다음 각 호와 같이 저장하는 경우에는 암호화하여야 한다. <개정 2019.6.28., 2024.10.10.>

1. 인터넷망 구간 및 인터넷망 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우
2. 내부망에 고유식별정보를 저장하는 경우(다만, 주민등록번호 외의 고유식별정보를 저장하는 경우에는 다음 각 목의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다)

가. 법 제33조에 따른 개인정보 영향평가의 결과

나. 암호화 미적용시 위험도 분석에 따른 결과

⑤ 부서별 개인정보책임자는 이용자의 개인정보 또는 이용자가 아닌 정보주체의 고유식별정보, 생체인식정보를 개인정보취급자의 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 안전한 암호 알고리즘을 사용하여 암호화한 후 저장하여야 한다. <개정 2024.10.10.>

제47조(접속기록의 보관 및 위·변조 방지) ① 개인정보 보호책임자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하고, 매 월 1회 이상 점검하여야 한다. 다만, 5만 명 이상의 정보주체에 관하여 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다. <개정 2019. 6. 28., 2020. 2. 5.>

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

③ 개인정보취급자는 「개인정보 상시모니터링 운영 지침」 및 「개인정보 내부 관리계획」 등에서 정한 바에 따라 개인정보처리시스템에서 개인정보를 포함한 파일 다운로드 시 사유를 입력하여야 하며, 개인정보 보호책임자는 그 사유를 확인하여야 한다. <신설 2020. 2. 5.> <개정 2024.10.10.>

제47조의2(오남용 의심사례에 대한 소명요청)

① 개인정보 보호관리자는 접속기록을 근거로 개인정보취급자에게 해당 접속기록의 적정성에 대한 소명을 요청할 수 있다. <개정 2024.10.10.>

② 제1항에 따른 소명요청을 받은 대상자(이하‘소명대상자’라 한다)는 요청을 받은 날로부터 10일 이내에 해당 접속기록의 업무수행 관련성 등에 대해 사실에 입각한 상세한 답변을 개인정보 보호관리자에게 제출하

여야 한다. <개정 2024.10.10.>

③ 개인정보 보호관리자는 제2항에 따라 소명답변을 제출받은 날로부터 20일 이내에 소명대상자 답변의 적정성을 검토·판정하여야 한다. <개정 2024.10.10.>

④ 개인정보 보호관리자는 소명대상자의 소명답변이 지연되거나 그 내용이 불충분한 경우 현장 점검 등을 통해 현황을 파악할 수 있다. 이 경우 소명대상자는 현장 점검에 성실히 협조하여야 한다. <개정 2024.10.10.>

[본조신설 2021. 9. 23.]

제48조(보안프로그램의 설치 및 운영) 개인정보 보호책임자는 악성프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안프로그램을 설치·운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.

1. 보안프로그램의 자동 업데이트 기능을 사용하거나 또는 일 1회 이상 업데이트를 실시하여 최신 상태로 유지
2. 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트 실시

제49조(관리용 단말기의 안전조치) 삭제 <2024.10.10.>

제50조(물리적 안전조치) ① 개인정보 보호책임자는 전산실, 자료보관실 등 개인정보를 보관하는 물리적 보관 장소에 대하여 출입통제 절차를 수립·운영하여야 한다.

② 개인정보 보호책임자는 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 수립·운영하여야 한다.

③ 개인정보 보호책임자는 개인정보가 포함된 서류, 보조저장매체 등은 잠금장치가 있는 안전한 장소에 보관하여야 한다.

제51조(재해·재난 대비 안전조치) ① 개인정보 보호책임자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검하여야 한다.

② 개인정보 보호책임자는 재해·재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하여야 한다.

제51조의2(출력·복사시 안전조치) ① 개인정보 보호책임자는 개인정보처리시스템에서 개인정보의 출력시(인쇄, 화면표시, 파일생성 등) 용도를 특정하여야 하며, 용도에 따라 출력 항목을 최소화하여야 한다.

② 개인정보 보호책임자는 개인정보가 포함된 종이 인쇄물, 개인정보가 복사된 외부 저장매체 등 개인정보의 출력·복사물을 안전하게 관리하기 위해 필요한 안전조치를 하여야 한다.

[본조신설 2024.10.10.]

제3장 고정형·이동형 영상정보처리기기 운영 및 관리

제52조(적용범위) 이 장은 심사평가원이 공개된 장소에 설치·운영하는 고정형·이동형 영상정보처리기기와 이 기기를 통하여 처리되는 개인영상정보를 대상으로 한다. <개정 2023.11.28., 2024.10.10.>

제53조(고정형·이동형 영상정보처리기기 운영·관리 방침) 개인정보 보호책임자는 고정형·이동형 영상정보처리기기 운영·관리방침을 수립하거나 변경하는 경우에는 정보주체가 쉽게 확인할 수 있도록 공개하여야 한다.

<개정 2023.11.28., 2024.10.10.>

[제목개정 2023.11.28., 2024.10.10.]

제54조(개인영상정보 관리책임자) ① 개인영상정보 관리책임자는 심사평가원 「직제규정 시행세칙」에 따라 고정형·이동형 영상정보처리기기의 설치·운영 등 사옥 관리업무를 담당하는 부의 장으로 한다. <개정 2023.11.28., 2024.10.10.>

② 개인영상정보 관리책임자는 개인영상정보의 처리에 관한 업무를 총괄해서 책임지며 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

제55조(사전의견 수렴) 개인영상정보 관리책임자는 고정형·이동형 영상정보처리기기의 설치 목적 변경에 따른 추가 설치 등의 경우에 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다. <개정 2023.11.28., 2024.10.10.>

제56조(안내판의 설치) ① 개인영상정보 관리책임자는 고정형 영상정보처리기기가 설치·운영 중임을 쉽게 알아볼 수 있도록 다음 각 호의 사항을 기재한 안내판 설치 등 필요한 조치를 하여야 한다. <개정 2023.11.28.>

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

② 제1항에 따른 안내판은 촬영범위 내에 정보주체가 알아보기 쉬운 장소에 누구라도 쉽게 판독할 수 있게 설치되어야 하며, 이 범위 내에서 개인영상정보 관리책임자는 안내판의 크기, 설치위치 등을 자율적으로 정할 수 있다.

제56조의2(이동형 영상정보처리기기 촬영 사실 표시 등) 개인영상정보 관리책임자는 이동형 영상정보처리기기로 사람 또는 그 사람과 관련된 사물의 영상을 촬영하는 경우에는 불빛, 소리, 안내판, 안내서면, 안내방송 또는 그 밖에 이에 준하는 수단이나 방법으로 정보주체가 촬영 사실을 쉽게 알 수 있도록 표시하고 알려야 한다. 다만, 드론을 이용한 항공촬영 등 촬영 방법의 특성으로 인해 정보주체에게 촬영 사실을 알리기 어려운 경우에는 개인정보 보호위원회가 구축하는 인터넷 사이트에 공지하는 방법으로 알릴 수 있다.

[본조신설 2024.10.10.]

제57조(개인영상정보 이용·제3자 제공 등의 제한) ① 개인영상정보 관리책임자는 다음 각 호를 제외하고는 개인영상정보를 수집 목적 이외로 이용하거나 제3자에게 제공하여서는 아니 된다. <개정 2020.10.13.>

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 개인정보보호위원회의 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

② 개인영상정보 관리책임자는 개인영상정보를 수집 목적 이외로 이용하거나 제3자에게 제공하는 경우에는 다음 각 호의 사항을 별지 제11호 서식 개인영상정보 관리대장에 기록하고 이를 관리하여야 한다.

1. 개인영상정보 파일의 명칭
2. 이용하거나 제공받은 자(공공기관 또는 개인을 포함한다)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

제58조(고정형·이동형 영상정보처리기기 설치 및 관리 등의 위탁) ① 개

인영상정보 관리책임자는 고정형·이동형 영상정보처리기기의 설치·운영에 관한 사무를 제3자에게 위탁하는 경우에는 그 내용을 정보주체가 언제든지 쉽게 확인할 수 있도록 안내판 및 고정형·이동형 영상정보처리기기 운영·관리 방침에 따른 수탁자의 명칭 등을 공개하여야 한다. <개정 2024.10.10.>

② 개인영상정보 관리책임자는 고정형·이동형 영상정보처리기기의 설치·운영에 관한 사무를 제3자에게 위탁할 경우에는 그 사무를 위탁받은 자가 개인영상정보를 안전하게 처리하고 있는지를 관리·감독하여야 한다. <개정 2024.10.10.>

[제목개정 2024.10.10.]

제59조(개인영상정보의 안전성 확보조치 및 보관·파기) ① 개인영상정보 관리책임자는 개인영상정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 다음 각 호의 조치를 하여야 한다.

1. 개인영상정보의 안전한 처리를 위한 내부관리계획의 수립·시행
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 저장 시 비밀번호 설정 등)
4. 처리기록의 보관 및 위·변조 방지를 위한 조치(개인영상정보의 생성 일시, 열람 시 열람목적·열람자·열람일시 등에 대한 기록·관리 조치 등)
5. 개인영상정보의 안전한 물리적 보관을 위한 보관시설 마련 또는 잠금장치 설치

② 개인영상정보는 이를 수집한 날부터 30일 동안 보유하는 것을 원칙

으로 한다. 다만, 「영유아보육법」에 따라 심사평가원 내 어린이집에서 수집한 개인영상정보는 60일 이상 보유하여야 한다.

③ 개인영상정보의 보유기간이 경과한 때에 개인영상정보 관리책임자는 24시간 이내에 이를 파기하여야 한다. 이 경우 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) 파일형태의 개인영상정보는 복원이 불가능한 기술적 방법으로 영구삭제

④ 개인영상정보 관리책임자는 제3항에 따라 개인영상정보를 파기하는 경우 다음 각 호의 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 대한 확인 시기)
3. 개인영상정보 파기 담당자

제4장 개인정보파일의 등록·관리 및 공개

제60조(개인정보파일의 등록 및 변경 신청) ① 개인정보파일을 운용하는 개인정보취급자는 개인정보 보호책임자에게 개인정보파일 등록을 신청하여야 한다.

② 개인정보취급자는 등록한 사항이 변경된 경우에는 개인정보 보호책임자에게 변경 등록을 신청하여야 한다.

③ 개인정보취급자가 제1항 및 제2항에 따른 신청을 하는 경우에는 별지

제12호서식 개인정보파일 등록, 변경등록 신청서를 작성·제출하여야 한다.

④ 법 제33조제1항에 따른 개인정보 영향평가를 받은 개인정보파일의 경우에는 그 영향평가의 결과를 함께 첨부하여야 한다.

제61조(개인정보파일의 등록 및 변경 확인) ① 개인정보 보호책임자는 개인정보파일 등록 또는 변경 신청을 받은 경우 그 내역을 검토하고 적정성을 판단한 후 보건복지부의 확인을 받아 개인정보보호위원회에 등록하여야 한다. <개정 2020.10.13.>

② 제1항의 등록은 60일 이내에 하여야 한다.

제62조(개인정보파일의 파기 및 등록 사실 삭제) ① 개인정보 보호책임자는 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 개인정보 보호책임자는 개인정보파일의 보유기간, 처리목적 등을 반영한 개인정보 파기계획을 수립·시행하여야 한다. 다만, 영 제30조제1항제1호에 따른 내부 관리계획이 수립되어 있는 경우에는 개인정보 보호책임자는 내부 관리계획에 개인정보 파기계획을 포함하여 시행할 수 있다.

③ 개인정보취급자는 보유기간 경과, 처리목적 달성 등 파기사유가 발생한 개인정보파일을 선정하고 별지 제13호서식 개인정보파일 파기요청서에 파기대상 개인정보파일의 명칭, 파기방법 등을 기재하여 개인정보 보호책임자의 승인을 받아 개인정보파일을 파기하여야 한다.

④ 개인정보 보호책임자는 개인정보 파기 시행 후 파기결과를 확인하고 별지 제14호서식 개인정보파일 파기 관리대장을 작성하여야 한다.

⑤ 제1항에 따라 개인정보파일을 파기한 경우, 개인정보 보호책임자는 그 사실을 확인하고 지체 없이 개인정보파일 등록 사실을 삭제한 후 그 내역을 보건복지부 및 개인정보보호위원회에 통보하여야 한다. <개정 2020.10.13.>

제63조(개인정보파일대장 작성) ① 부서별 개인정보책임자는 소관 개인정보파일 보유현황을 별지 제15호서식 개인정보파일대장에 기록하고 관리하여야 한다.

② 개인정보파일대장은 부서별 개인정보책임자가 개인정보파일을 수집하거나 다른 기관으로부터 제공받아 보유하는 경우 작성하며, 1개의 개인정보파일에 1개의 개인정보파일대장을 작성하여야 한다.

제64조(개인정보파일 보유기간의 산정) ① 보유기간은 전체 개인정보가 아닌 개별 개인정보의 보유부터 삭제까지의 생애주기로서 보유목적에 부합하는 최소기간으로 산정하여야 한다.

② 개별 법령에 구체적인 보유기간이 명시되어 있지 않은 경우에는 개인정보 보호책임자의 협의를 거쳐 원장 결재를 통해 구체적인 보유기간을 산정하여야 한다. 다만, 보유기간은 「보건복지부 개인정보 보호지침」의 개인정보파일 보유기간 책정 기준표와 「공공기록물 관리에 관한 법률 시행령」의 기록관리기준표를 상회할 수 없다.

③ 정책고객, 홈페이지회원 등의 홍보 및 대국민서비스 목적의 외부고객 명부는 특별한 경우를 제외하고는 2년을 주기로 정보주체의 재동의절차를 거쳐 동의한 경우에만 계속하여 보유할 수 있다.

제65조(개인정보파일 현황 공개 및 방법) 개인정보 보호책임자는 개인정보파일의 보유·파기현황을 주기적으로 조사하여 그 결과를 심사평가원

개인정보 처리방침에 포함하여 관리하여야 한다.

제66조(보칙) 이 지침에서 정하지 아니한 사항은 원장이 별도로 정한다.

부칙<지침 제255호, 2018. 6. 28.>

이 지침은 2018년 6월 29일부터 시행한다.

부칙<지침 제274호, 2019. 6. 28.>

이 지침은 2019년 7월 14일부터 시행한다.

부칙<지침 제295호, 2020. 2. 5.>

이 지침은 2020년 2월 22일부터 시행한다.

부칙<지침 제310호, 2020. 10. 13.>

이 지침은 2020년 10월 13일부터 시행한다.

부칙<지침 제343호, 2021. 9. 23.>

이 지침은 2021년 9월 27일부터 시행한다.

부칙<지침 제376호, 2022. 10. 25.>

이 지침은 2022년 10월 25일부터 시행한다.

부칙<지침 제409호, 2023. 11. 28.>

이 지침은 2023년 11월 30일부터 시행한다.

부칙<지침 제432호, 2024. 10. 10.>

이 지침은 2024년 10월 10일부터 시행한다.

[별지 제1호서식] (제8조제1항)

개인정보의 목적 외 이용 및 제3자 제공 대장

개인정보 또는 개인정보파일 명칭			
이용 또는 제공 구분	[ ] 목적 외 이용 [ ] 제3자 제공		
목적 외 이용기관의 명칭 (목적 외 이용의 경우)		담당자	소 속 성 명 전화번호
제공받는 기관의 명칭 (제3자 제공의 경우)		담당자	성 명 소 속 전화번호
이용하거나 제공한 날짜, 주기 또는 기간			
이용하거나 제공한 형태			
이용 또는 제공의 법적 근거			
이용 목적 또는 제공받는 목적			
이용하거나 제공한 개인정보의 항목			
「개인정보 보호법」 제18조제5항에 따라 제한을 하거나 필요한 조치를 마련할 것을 요청한 경우에는 그 내용			

210㎜× 297㎜[인쇄용지(특급) 34g/㎡]

[별지 제2호서식] (제27조제4항)

의 결 서

회의일시 :	심의요청부서 :
제 목 :	
1. 제안내용 2. 제안사유 3. 의결사항 첨 부 : 회의록	
위 의결사항을 명확히 하기 위하여 건강보험심사평가원 「개인정보 내부관리지침」 제27조제4항에 따라 각 위원이 서명 날인함 년 월 일 위 원 (인) 위 원 (인) 위 원 (인) 위 원 (인) 위 원 (인)	

210mm× 297mm[인쇄용지(특급) 34g/㎡]

[별지 제3호서식] (제27조제4항)

서 면 결 의 서

의 안 명:

의결주문:

제안사유:

위 의안을 건강보험심사평가원 「개인정보 내부관리지침」 제27조제4항에 따라 서면으로 위원회의 동의를 얻어 집행하고자 하오니 동의 여부를 아래의 해당란에 서명 날인하여 주시기 바랍니다.

년 월 일

위원장 (인)

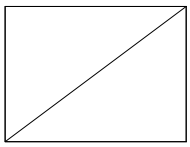
동의함		동의하지 않음	
위원	(인)	위원	(인)
위원	(인)	위원	(인)
위원	(인)	위원	(인)
위원	(인)	위원	(인)
위원	(인)	위원	(인)
		)	

210㎜× 297㎜[인쇄용지(특급) 34g/㎡]

[별지 제4호서식] (제27조제5항)

안 건 부 의 서

(앞면)



의안번호	제 호
의결일자	년 월 일

안건명	

소 관 부 서	
제출연월일	
제 안 자	

210㎜× 297㎜[인쇄용지(특급) 34g/㎡]

(뒷면)

의안명	

1. 의안요지

2. 요청근거

3. 요청사례

4. 소관부서 의견

210㎜× 297㎜[인쇄용지(특급) 34g/㎡]

[별지 제5호서식] <개정 2023.11.28.> (제34조제1항,제2항)

개인정보 유출 등 신고서

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

유출신고 접수기관	기관명	담당자명	연락처

[별지 제6호서식] (제36조제1항)

개인정보 침해사실 신고서

신고인	성명		
	생년월일		
	연락처	전화번호(휴대폰)	
		전자우편주소	
		주소	
피신고인	부서명		
	연락처	전화번호	
		주소	
신고내용			

위와 같이 개인정보 침해사실을 신고합니다.

붙임:

년 월 일

신고인: (서명 또는 인)

210㎜× 297㎜[일반용지 70g/㎡(재활용품)]

[별지 제7호서식] (제36조제6항)

개인정보 침해사고 처리결과 통지서

접수번호		처리기한		
처리부서명		담당자	직위/성명	
			연락처	
침해신고 주요내용				
처리결과				

귀하께서 신고하신 개인정보의 침해사실에 대하여 「개인정보 보호법」에 따라 처리결과를 통지합니다.

년 월 일

건 강 보 험 심 사 평 가 원 장 직인

210㎜× 297㎜[일반용지 70g/㎡(재활용품)]

[별지 제8호서식] <개정 2020.10.13.> (제38조제1항)

개인정보 열람 요구서

※ 아래 작성방법을 읽고 굵은 선 안쪽의 사항만 적어 주시기 바랍니다. (앞 쪽)

접수번호	접수일	처리기간 10일 이내

정보주체	성 명	전 화 번 호
	생년월일	
	주 소	

대리인	성 명	전 화 번 호
	생년월일	정보주체와의 관계
	주 소	

요구내용	[ ] 개인정보의 항목 및 내용 [ ] 개인정보 수집·이용의 목적 [ ] 개인정보 보유 및 이용 기간 [ ] 개인정보의 제3자 제공 현황 [ ] 개인정보 처리에 동의한 사실 및 내용

「개인정보 보호법」 제35조제2항과 같은 법 시행령 제41조제3항에 따라 위와 같이 요구합니다.

년 월 일

요구인 (서명 또는 인)

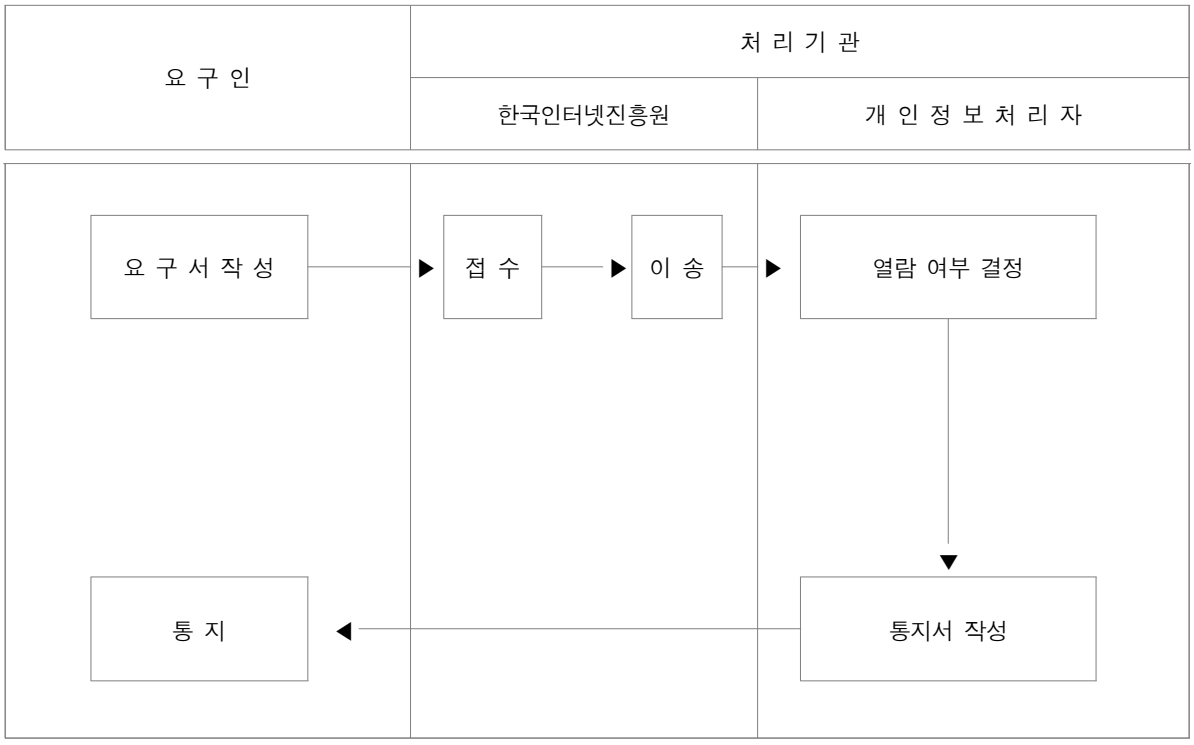
건강보험심사평가원장 귀하

작 성 방 법

1. '대리인' 란은 대리인이 요구인일 때에만 적습니다.
2. '요구내용' 란은 열람하려는 사항을 선택하여 [√] 표시를 합니다. 표시를 하지 않은 경우에는 해당 항목의 열람을 요구하지 않은 것으로 처리됩니다.

210㎜×297㎜[백상지(80g/㎡) 또는 중질지(80g/㎡)]

처리절차
이 요구서는 아래와 같이 처리됩니다.



[별지 제9호서식] (제38조제2항,3항, 제39조제2항)

개인정보 ([ ] 열람 [ ] 일부열람 [ ] 열람연기 [ ] 열람거절) 통지서

(앞 쪽)

수신자 (우편번호: , 주소:)

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

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

년 월 일

건 강 보 험 심 사 평 가 원 장 (직인)

210㎜×297㎜[신문용지 54g/㎡]

[별지 제10호서식] (제40조제2항)

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

수신자 (우편번호: , 주소:)

요구 내용	
□ 정정·삭제 □ 처리정지 조치 내용	
□ 정정·삭제 □ 처리정지 결정 사유	
이의제기방법	※ 개인정보처리자는 이의제기방법을 기재합니다.

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

년 월 일

건 강 보 험 심 사 평 가 원 장 (직인)

유의사항

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

210㎜×297㎜[신문용지 54g/㎡]

[별지 제11호서식] <개정 2023.11.28.> (제57조제2항)

개인영상정보 관리대장

번 호	구 분	일 시	파일명/형태	담 당 자	목적/사유	이용·제공받는 제3자/열람등 요구자	이용·제공 근거	이용·제공 형태	기간 및 파기 예정일자	파기 등 결과 및 처리일자	안전관리 요청 및 결과
1	□ 이용 □ 제공 □ 열람 □ 파기										
2	□ 이용 □ 제공 □ 열람 □ 파기										
3	□ 이용 □ 제공 □ 열람 □ 파기										
4	□ 이용 □ 제공 □ 열람 □ 파기										
5	□ 이용 □ 제공 □ 열람 □ 파기										
6	□ 이용 □ 제공 □ 열람 □ 파기										
7	□ 이용 □ 제공 □ 열람 □ 파기										
8	□ 이용 □ 제공 □ 열람 □ 파기										
9	□ 이용 □ 제공 □ 열람 □ 파기										

[별지 제12호서식] <개정 2020.10.13.> (제60조제3항)

개인정보파일 ([ ]등록 [ ]변경등록) 신청서

※ '변경정보 및 변경사유' 란은 변경등록 시에만 작성합니다.

접수번호	접수일	처리기간 7일

공공기관 명칭	주소	등록부서	전화번호

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

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

년 월 일

신청기관 (서명 또는 인)

개인정보보호위원회 귀중

210㎜× 297㎜[일반용지 70g/㎡(재활용품)]

[별지 제13호서식] (제62조제3항)

개인정보파일 파기 요청서

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

[별지 제14호서식] (제62조제4항)

개인정보파일 파기 관리대장

번호	개인정보 파일명	자료의 종류	생성일	폐기일	폐기사유	처리 담당자	처리 부서장

210㎜× 297㎜[인쇄용지(특급) 34g/㎡]

[별지 제15호서식] (제63조제1항)

개인정보파일대장

① 기 관 명		② 연 번	
③ 파 일 명			
④ 보 유 목 적			
⑤ 보 유 근 거			
⑥ 수 집 방 법			
⑦ 대상개인범위			
⑧ 대상 인원 수		⑨ 보유기간	
⑩ 기 록 항 목 (항목수)			