개인정보 상시모니터링 운영 지침

2023. 9.

건강보험심사평가원
ICT전략실 정보보호부

개 정 이 력

버전	개정일 시행일	개 정 내 용	작성자	검토자	승인자
1.0	2023.9.26. 2023.9.26.	· 「개인정보 상시모니터링 운영 지침」 제정	장재성	김현수	신현석

목 차

Ⅰ 개요

1. 목적

○ 이 지침은 건강보험심사평가원(이하 '심사평가원')이 소관업무 수행 목적으로 보유하고 있는 개인정보를 업무 목적 외로 열람하거나 유출 등 오남용하는 것을 방지하고 개인정보를 취급하는 직원들의 업무처리 인식 제고를 위해 운영하는 개인정보 상시모니터링 운영 기준 및 절차를 정함을 목적으로 한다.

2. 관련 근거

○ 「개인정보 보호법」 제29조(안전조치의무), 제31조제2항제4호 '개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축'

○ 「개인정보의 안전성 확보조치 기준」 제2조, 제4조, 제8조

○ 보건복지부 개인정보보호센터 운영규정 제20조(개인정보 자체관제 활동)

○ 심사평가원 「개인정보 내부관리지침」 제47조(접속기록의 보관 및 위·변조 방지), 제47조의2(오남용 의심사례에 대한 소명 요청)

3. 다른 규정과의 관계

○ 「개인정보 내부관리지침」 제47조 및 제47조의2에서 정한 것을 제외하고는 이 지침을 적용한다.

4. 용어의 정의

○ 이 지침에서 사용하는 용어의 정의는 다음과 같으며 특별히 정하지 않은 경우 「개인정보 보호법」, 「개인정보 내부관리지침」 및

「개인정보보호센터 운영규정」 등의 용어 정의에 따른다.

○ ‘개인정보처리시스템’이란 개인정보를 처리할 수 있도록 체계적으로 구성한 정보시스템을 말한다.

○ ‘개인정보 모니터링’이란 개인정보 유출 및 오·남용 사고를 예방하기 위하여 개인정보처리시스템의 접속기록을 수집, 분석, 소명, 판정하는 등의 행위를 말한다.

○ ‘개인정보 상시모니터링시스템’이란 개인정보 오·남용을 방지하기 위해 접속기록 등을 확인 및 분석하고 소명 요청 할 수 있는 시스템을 말한다.

○ ‘접속기록’이란 개인정보취급자 등이 개인정보처리시스템에 접속하여 업무를 처리한 사실을 알 수 있는 계정, 접속일시, 접속자 정보, 처리한 정보주체 정보, 수행업무 등을 전자적으로 기록한 것을 말한다.

○ ‘개인정보취급자’란 건강보험심사평가원장의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 사람으로서 직접 개인정보에 관한 업무를 담당하는 사람과 그 밖에 업무상 필요에 따라 개인정보에 접근하여 처리하는 모든 사람을 말한다.

○ ‘열람유의대상자’란 언론·사회적으로 이슈가 되는 인물, 내부직원 등 개인정보 오·남용 가능성이 높은 대상자로 개인정보 보호책임자(CPO)가 지정한 대상자를 말한다.

○ ‘개인정보 오·남용’이란 개인정보를 수집된 업무처리 목적으로 사용하지 않고 다른 목적으로 사용하거나, 사용기준을 준수하지 않고 이용하는 행위 말한다.

○ ‘개인정보보호 위반자’란 개인정보보호 위반으로 주의·경고 등

징계를 받은 자를 말한다.

○ ‘모니터링 담당관’이란 개인정보 상시모니터링 업무를 수행하는 개인정보 보호관리자를 말한다.

○ ‘모니터링 담당자’란 개인정보 상시모니터링 업무를 수행하는 담당 직원을 말한다.

○ ‘추출조건’이란 개인정보 이용내역 중에서 오·남용 의심 건을 선별하기 위해 추출기준 등을 적용하여 만든 조건을 말한다.

○ ‘소명’이란 개인정보 열람 사유 및 근거자료 등을 상시모니터링 시스템에 등록하는 행위를 말한다.

○ ‘소명대상자’란 열람사유 소명요청을 받은 직원을 말한다.

II 상시모니터링 업무 처리

1. 모니터링 대상자 및 대상시스템

○ 대상자: 전 임직원(개인정보취급자)

○ 대상시스템: 개인정보처리시스템

〈상시모니터링 업무처리 흐름도〉

2. 접속기록 수집 · 분석

○ 개인정보처리시스템 내 화면 이벤트에 대한 접속기록 수집

- 개인정보처리시스템에 저장 후 개인정보 상시모니터링시스템으로 수집

○ 고유식별정보(주민등록번호)가 포함된 화면 조회, 엑셀저장 등 일부 이벤트에 대한 열람사유 입력 팝업 생성

○ 개인정보 열람사유 미입력 또는 모니터링 기준에 해당하는 건을 추출하여 필요한 경우 소명 요청

3. 모니터링 기준

○ 모니터링 세부 기준(<첨부1> 참고)

4. 열람사유 등록

가. 열람사유 등록 요청

○ 개인정보 오·남용이 의심되는 개인정보 조회 건에 대하여 열람 목적을 확인하기 위하여 열람자에게 직접 열람사유 등록 요청

- 시스템 자동 소명요청, 모니터링 담당자 수동 소명요청
- 개인정보 상시모니터링 시스템을 통해 열람직원에게 소명요청

나. 열람사유 등록(<첨부2> 참고)

○ 요청사유 또는 추출조건을 확인하여 피 열람자에 대한 개인정보 조회 목적(업무 연계성)을 구체적으로 기술

○ 열람사유 등록 기간: 소명 요청일로부터 **10일** 이내

○ 열람사유 등록 방법

① 통합로그인

② HiraNet 메인화면에서 “개인정보이용소명” 건수를 확인

③ 건수링크를 클릭하여 “개인정보 상시모니터링 소명시스템” 화면으로 이동

④ 소명요청제목, 요청기준, 요청내용, 요청일자, 답변기한, 열람내용, 소명등록 결과, 판정결과, 확인 결과 등이 표출

⑤ “열람사유등록” 화면에서 처리자명, 처리부서, 처리일자, 업무근거, 경과내용, 소명의견 입력

⑦ “열람사유등록” 화면에서 답변자, 답변자 담당업무, 전화번호, 증빙자료 첨부 여부 등을 확인 후 소명 답변 저장

〈 열람사유 등록 예시 〉

(예시 1) 요양급여 심사를 위한 청구명세서 조회 및 인력현황 조회

- 청구명세서 조회는 중복청구, 착오 청구 확인하기 위함. 인력현황 확인은 해당기관에 전문의가 있는 경우 타 기관 진찰료 조정하기 위하여 조회함

(예시 2) ’행위 빈도 구축, 관리 업무’를 수행 중 청구빈도가 발생하지 않은 특정 요양기관의 폐업여부를 확인하였음

- 열람한 해당기관은 산부인과 의원으로 20XX년 이후로 분만행위의 청구빈도가 없어 폐업여부를 별도 확인

5. 적정성 판정

가. 열람사유 등록 건에 대한 판정 요청

○ 소명 답변 저장 후 모니터링 담당자가 “개인정보 상시모니터링 소명시스템” 내 소명내역에서 확인

나. 모니터링 담당자의 1차 판정

○ 판정 등록

- 소속직원이 등록한 열람사유에 대해 구체적인 사실여부(구두 진술, 업무일지, 관련문서 등)를 확인
- 판정 의견을 기재한 후 “개인정보 오·남용 판정 기준”에 따라 적정, 부적정 판정 등록

○ 판정 기간: 열람사유 등록일로부터 **20일** 이내

다. 모니터링 담당 부서장 2차 판정(내부 보고)

○ 개인정보 상시모니터링 운영결과 보고(매월)

6. 사실관계 조사

○ 1차 판정 결과 부적정으로 확인한 경우 필요 시 현장점검 실시

○ 점검 방법

- 모니터링 담당부서에서 열람자 및 소속부장 면담 등을 통해 사실관계 확인(열람사유 등록내용, 업무처리내역, 개인정보보호 교육여부, 출력물, 업무분장, 열람로그기록 등을 확인)

○ 점검 결과

- 현장조사 결과 부적정 열람내역으로 확인될 시 소명·로그 분석 자료, 사실관계 확인서를 참고하여 2차 판정에 활용

< 첨부3 >「사실관계 확인서(열람자용/소속부장용)」참고

7. 접속기록 파기

○ 개인정보 상시모니터링시스템의 접속기록 중 2년이 지난 접속기록은 파기함

Ⅲ 개인정보 오·남용 판정 기준

부적정 유형	부적정 판정기준	주요 사례
목적 외 이용 **(법* 제18조)**	• 개인정보의 사적 이용	• 호기심으로 유명인 정보 조회 • 사적 이익을 위해 개인정보 조회
	• 수집목적 외 이용	• 만족도 조사, 사용자 교육, 무단 테스트 등 수집 목적과 관련 없는 업무 처리를 위해 개인정보 조회 • 목적 외 이용 가능 범위를 초과한 개인정보 조회 (법적 요건을 갖추지 못한 수사기관의 요청 등)
접근 통제 위반 **(지침** 제44조)**	• 정당한 권한 없이 이용	• 인사이동, 휴·퇴직자가 권한 없이 개인정보 조회 • 권한 없는 직원이 개인정보취급자를 대신하여 개인정보 조회 • 개인정보처리시스템 사용자계정·인증수단을 권한 없는 자에게 대여·공유 또는 대신 업무처리 지시
	• 허용된 권한을 초과하여 이용	• 개인정보 취급권한이 없는 관리자(시스템관리자, 사용자 승인권자)가 무단으로 개인정보 조회 • 업무 권한 범위를 벗어난 개인정보 조회
불성실 소명 **(지침** 제47조의2)**	• 기한 내 소명하지 않은 경우	• 보건복지부「개인정보보호센터 운영규정」 제19조(추가 소명요청)에도 불구하고 기한 내 소명하지 않는 행위
	• 허위 또는 불성실 소명한 경우	• '기억이 안 난다', '조회한 적 없다' 등 불성실한 소명을 반복하여 점검 의무를 수행하기 어렵게 하는 행위 • 상식을 벗어난 소명 답변(ㅎㅎ, ㅋㅋ 등)을 하는 행위

* 「개인정보 보호법」 제18조(개인정보의 목적 외 이용·제공 제한)

** 「개인정보 내부관리지침」 제44조(접근 권한의 관리), 제47조의2(오남용 의심 사례에 대한 소명요청)

Ⅳ 개인정보 오·남용 사후 조치

1. 부적정 판정 건에 대한 조치 사항

○ 판정 결과 부적정으로 확인된 모니터링대상자는 개인정보 상시 모니터링 담당부서 및 소속부서 내부 보고

○ 해당 개인정보 처리가 가능한 화면 접근권한 회수

2. 개인정보 오·남용 관련 징계양정기준

○ 심사평가원「인사규정 시행세칙」개인정보 관련 징계양정기준

〈 징계양정기준 세부 내용 〉

비위의 정도 및 과실 여부 / 비위의 유형	비위의 정도가 심하고 고의가 있는 경우	비위의 정도가 심하고 중과실이거나, 비위의 정도가 약하고 고의가 있는 경우	비위의 정도가 심하고 경과실이거나, 비위의 정도가 약하고 중과실인 경우	비위의 정도가 약하고 경과실인 경우
5. 비밀엄수의무 위반				
가. 비밀의 누설·유출	파면	파면.해임	강등.정직	감봉.견책
나. 개인정보 부정이용 및 무단유출	파면.해임	해임.강등	정직.감봉	감봉.견책
다. 비밀 분실 또는 해킹 등에 의한 비밀침해 및 비밀 유기 또는 무단방치	파면.해임	강등.정직	정직.감봉	감봉.견책
라. 개인정보 무단조회 열람 및 관리소홀 등	파면.해임	강등.정직	감봉	견책

3. 상시모니터링 결과 보고 및 통보

○ 매월 내부 보고 및 보건복지부 개인정보보호센터로 결과 송부

첨부1

모니터링 세부 기준(16건)

연번	추출기준명	추출기준 정의	상세조건	참고 정보	분석 대상기간	상세조건 임계치
1	열람유의 대상자 조회	열람유의자로 등록된 피열람자를 조회한 경우	조회된 정보주체 = 열람유의 대상자	열람유의 대상자	1~30일	-
2	직원정보 조회	직원 주민등록번호를 조회한 경우	조회된 정보주체 = 직원	인사정보	1~30일	-
3	사용자ID 공유	동일ID로 다른 PC에서 접속한 경우	동일한 직원번호에 IP 2개 이상	인사정보, 계정정보	1~30일	2
4	대표ID 사용 (개별ID 미발급)	부적합 직원명 사용(ID 공유)	관리자, admin 사용자 감지	계정정보	1~30일	-
5	동일IP에서 다수 ID접속	동일한 IP에서 직원번호가 2개 이상인 경우	동일한 IP에 사용자ID 2개 이상	인사정보, 계정정보	1~30일	2
6	접근 대역 외 접속	직원별 3개월 접속한 IP별 표준편차범위 벗어난 경우	접속한 IP가 표준편차 범위 벗어남	계정정보	90일	-
7	개인정보 과다 조회	직원별 1개월간 조회로그 표준편차 이상 조회	당일 로그 > 표준편차		30일	-
8	개인정보 과다 저장	직원별 3개월간 저장로그 이상 저장	당일 저장 > 표준편차		90일	-
9	개인정보 과다 출력	직원별 3개월간 출력로그 이상 저장	당일 출력 > 표준편차		90일	-
10	동일정보주체 과다조회	장기간 동일인 조회	특정개인 조회 > 소속직원들이 조회		30일	-
11	권한 제한자의 개인정보 처리	휴직자, 퇴직자의 업무처리	재직구분이 휴직, 퇴직인 경우	인사정보	1~30일	-
12	장기간 미사용자의 업무처리	마지막 로그발생이력으로부터 1개월 이후 발생	로그 발생일 – 마지막 로그 발생일		30일	-
13	보안 취약자의 개인정보 처리	징계 또는 오남용 이력이 있는 직원이 조회	보안취약자로 분류된 직원		1~30일	-
14	업무시간 외 개인정보 처리	휴일, 심야시간, 업무시간 외 조회	휴일, 19시 이후 조회		1~30일	-
15	특정 업무를 이용한 개인정보 처리	열람사유 유형분석, 단순 조회 등	열람사유에 ....,1111,asdf 등		1~30일	-
16	성명을 이용한 주민번호 조회	동일성명 다수 주민번호 변경 조회	이름은 같은데 주민등록번호가 다름		1~30일	2

첨부2 열람사유 등록 화면

첨부3 **사실관계 확인서(열람자용/소속부장용)**

사 실 관 계 확 인 서

소 속			
성 명		직 급	

※ 사실관계 등 진술 사항 기재 (열람자용)

상기 진술한 내용이 틀림이 없음을 확인합니다.

년 월 일

확인자 (인)

입회자 (인)

사 실 관 계　확 인 서

소　속			
성　명		직　급	

※ 사실관계 등 진술 사항 기재 (소속부장용)

상기 진술한 내용이 틀림이 없음을 확인합니다.

년　　월　　일

확인자　　(인)