개인정보 처리 업무 위탁 관리지침

2024. 3.

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 처리 업무 위탁 관리지침」 제정	홍유정	김현수	신현석
2.0	2024.3.27. 2024.3.27.	・「개인정보 보호법」 개정 사항 반영 ・ 개인정보 처리 재위탁 동의서 [첨부 10] 추가	홍유정	김현수	신현석

목 차

Ⅰ 개요

1. 목적

○ 「개인정보 보호법」 제26조 및 건강보험심사평가원(이하 “심사평가원”) 「개인정보 내부관리지침」 제17조에 따라 심사평가원이 개인정보 처리가 수반되는 업무를 외부 업체·기관 등(이하 “수탁자”)에 위탁하는 경우 필요한 업무 처리 절차 및 기준 등에 관한 사항을 규정

2. 관련 근거

○ 「개인정보 보호법」 제26조(업무위탁에 따른 개인정보의 처리 제한)

○ 「개인정보 보호법 시행령」 제28조(개인정보의 처리 업무 위탁 시 조치)

○ 「표준 개인정보 보호지침」 제16조(수탁자의 선정 시 고려사항), 제17조(개인정보 보호 조치의무)

○ 「개인정보의 안전성 확보조치 기준」 제3조(안전조치의 적용 원칙)

○ 심사평가원 「개인정보 내부관리지침」 제17조(개인정보의 처리 업무 위탁 시 조치사항)

3. 적용 범위

○ 심사평가원이 개인정보 처리 업무를 수탁자에게 위탁하는 경우에 관하여 다른 법령 또는 규정, 지침 등에서 특별히 정한 것을 제외하고는 이 지침을 따름

4. 용어 정의

○ 처리

-「개인정보 보호법」제2조제2호에 따라 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 이와 유사한 행위를 의미

○ 위탁자

-「개인정보 보호법」제26조제1항에 따라 개인정보의 처리 업무를 위탁하는 개인정보처리자, 이 지침에서는 심사평가원을 의미

○ 위탁부

-「개인정보 보호법」제26조제1항에 따라 위탁자인 심사평가원에서 개인정보의 처리 업무 위탁을 담당하는 부를 의미

○ 수탁자

- 개인정보 처리 업무를 위탁받아 처리하는 자(외부 업체·기관 등)

○ 이외 이 지침에서 사용되는 용어는「개인정보 보호법」등 관련 법령 및 심사평가원「개인정보 내부관리지침」등에 따름

II 개인정보 처리 업무 위탁 개념 및 판단 기준

1. 개인정보 처리 업무 위탁 개념

○ 계약의 형태와 종류를 불문하고 개인정보 처리가 수반되는 업무의 전부 또는 일부를 심사평가원이 직접 수행하지 않고 수탁자에게 위탁하는 것을 의미

○ 개인정보 처리 업무 위탁과 제3자 제공의 구분

구분	업무 위탁	제3자 제공
관련 조항	「개인정보 보호법」 제26조	「개인정보 보호법」 제17조
예시	배송업무 위탁, TM 위탁 등	사업제휴, 개인정보 판매 등
이전 목적	위탁자의 이익을 위해 처리	제3자의 이익을 위해 처리
이전 방법	위탁 사실 공개 ※ 공개 경로: 심사평가원 국민 홈페이지	법에 따라 제공 목적 등 고지 후 정보주체의 동의 획득
관리·감독 의무	위탁자	제공받는 자(제3자)
손해배상책임	위탁자 및 수탁자 부담	제공받는 자(제3자) 부담

2. 개인정보 처리 업무 위탁 판단 기준

○ 수탁자에게 업무를 위탁 시, 아래의 기준에 따라 개인정보 처리 업무 위탁으로 판단되는 경우 이 지침에 따라 업무 수행

○ **(판단 주체)** 위탁부

○ **(판단 기준)**

기준	예시
심사평가원 업무 수행을 위해 보유 중인 개인정보를 수탁자에게 제공	물품 배송, 교육 위탁 운영 등
심사평가원 업무 수행을 위해 수탁자가 직접 개인정보를 수집, 관리(생성, 이용, 저장, 파기 등)	직원 채용, 설문 조사 위탁, 기록물 파기 등
(정보화사업) 수탁자가 심사평가원 개인정보처리시스템 DB 등에 접근하여 업무 수행 ※ 단순 시스템 유지보수도 수탁자에게 개인정보가 포함된 DB에 접근할 수 있는 권한이 부여되는 경우 개인정보 처리 업무 위탁임 ※ 단, 시스템의 부품만 교체하는 등 서버나 DB에 대한 접근 권한이 없는 경우 개인정보 처리 업무 위탁에 해당하지 않음	시스템 구축 · 개발 · 운영, 통합 유지보수, 프로그램 개발 등

Ⅲ 개인정보 처리 업무 위탁 절차 및 조치 사항

1. 개인정보 처리 업무 위탁 절차

절차	세부 내용	소관 부
1) 개인정보 처리 업무 위탁 계약 전	· 개인정보 처리 업무 위탁 여부(위험성 확인) 및 범위 결정 · 수탁자 선정 시 수탁자 개인정보 보호 역량 평가 · 개인정보 보호 계획 수립	위탁부
⇩		
2) 개인정보 처리 업무 위탁 계약 시	· 개인정보 처리 업무 위탁 문서(계약서) 작성 · 개인정보 처리 업무 위탁 사전 점검 · 개인정보 인수증 작성 · 계약 시 개인정보 처리 업무 위탁 내용을 정보보호부로 (간이)문서 통보 ※ (정보보호부) 개인정보 처리 업무 위탁 내용 국민 홈페이지에 공개	위탁부 정보보호부
⇩		
3) 개인정보 처리 업무 위탁 수행 중	· 수탁자 교육 실시 · 수탁자 관리·감독(개인정보 처리 현황 점검) · (재위탁 시) 개인정보 처리 업무 재위탁 동의서 작성	위탁부
⇩		
4) 개인정보 처리 업무 위탁 종료 시	· 개인정보 반환·파기 여부 등 점검(5일 이내)	위탁부
⇩		
5) 개인정보 처리 업무 위탁 현황 점검	· 개인정보 처리 업무 위탁 현황 점검	정보보호부

2. 개인정보 처리 업무 위탁 조치 사항

1) 개인정보 처리 업무 위탁 계약 전

○ **개인정보 처리 업무 위탁 여부(위험성 확인) 및 범위 결정**

- 위탁부는 개인정보 처리 업무 위탁 시 발생할 수 있는 위험을 고려하여 위탁 여부 및 범위를 결정

※ 개인정보 유출 시 위험성이 높다고 판단된 경우 위탁 여부 재검토, 수탁자 감독 강화, 사고 발생 시 책임소재 명확화 등의 대책 필요

- 특히, 대량의 개인정보 및 민감정보 등 처리가 포함된 업무는 유출 사고 발생 시 피해가 크므로 위탁 여부를 신중히 결정
- 위탁부는 필요 최소한의 개인정보가 처리될 수 있도록 수탁자와 사전협의 등을 통해 업무의 범위 명확화

○ **수탁자 개인정보 보호 역량 평가**

- 위탁부는 '수탁자 개인정보 보호 역량 분석 평가표[첨부1]'에 따라 수탁자의 개인정보 보호 역량을 평가하고 개인정보 위험성을 최소화할 수 있는 자를 선정*

* 계약부에서 수탁자를 선정하는 경우, 위탁부는 최종 선정된 수탁자에 대해 개인정보 보호 역량을 평가

○ **개인정보 보호 계획 수립**

- 위탁부는 개인정보 처리 업무 위탁 시 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 수탁자에 대한 교육 및 관리·감독 관련 내용을 포함한 개인정보 보호 계획을 수립

2) 개인정보 처리 업무 위탁 계약 시

○ **개인정보 처리 위탁 문서 작성**

- 위탁부는「개인정보 보호법」제26조제1항에 따라 개인정보 처리 업무 위탁 계약 시 아래의 내용을 포함한 '개인정보 처리 위탁 처리 업무 위탁 계약서[첨부2]'를 작성*

* 계약서 작성 주체는 위탁부(위탁부가 속한 부서의 장 서명·날인)

< 개인정보 처리 업무 위탁 계약서 포함 사항 >

(근거:「개인정보 보호법」 제26조제1항 및 동법 시행령 제28조제1항

① 위탁업무의 목적 및 범위(시행령 §28① 제1호)

② 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항(법 §26① 제1호)

③ 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항(시행령 §28① 제4호)

④ 개인정보의 기술적·관리적 보호조치에 관한 사항(법 §26① 제2호)

※ 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항(시행령 §28① 제3호)

⑤ 재위탁 제한에 관한 사항(시행령 §28① 제2호)

⑥ 수탁자가 준수하여야 할 의무 위반 시 손해배상 등 책임에 관한 사항(시행령 §28① 제5호)

⑦ (가명정보 위탁 시) 가명정보의 다른 정보와 결합을 통한 재식별 시도 금지에 관한 사항

⑧ (가명정보 위탁 시) 가명정보의 재식별 위험 발생 시 위탁자 통지에 관한 사항

※ 업무 위탁 종료 후 법률상 의무 이행, 민원 등의 목적으로 수탁자에게 개인정보의 보관 등 추가 처리가 필요한 경우 개인정보 처리 업무 위탁 계약서에 법률상 근거와 개인정보 보유 기간, 목적 등 해당 내용 명시

※ 업무 위탁 계약이 갱신되는 경우, 위탁 문서의 내용 재검토 및 수정 필요

- 수탁자는 '수탁자 개인정보 보호 서약서[첨부3]'를 작성

※ 수탁 직원 인원 등 변경 또는 재위탁 시에도 '수탁자 개인정보 보호 서약서' 작성

○ **개인정보 처리 업무 위탁 사전 점검**

- 위탁부는 계약 시 '개인정보 처리 업무 위탁 사전 점검표[첨부4]'에 따라 개인정보 처리 업무 위탁 전 위험 요인 차단

○ **개인정보 인수증 작성**

- 수탁자는 위탁부로부터 종이문서, 전자파일, 보안USB, CD 등의 형태로 개인정보를 제공받은 경우 '개인정보 인수증[첨부5]' 작성

○ **개인정보 처리 업무 위탁 내용 통보**

- **(위탁부)** 계약 시 위탁 내용을 정보보호부로 통보

· 통보 방법: '개인정보 처리 업무 위탁 내용 통보 서식[첨부6]' 참고하여 간이문서 시행(담당 전결)

· 통보 내용: 위탁명, 위탁 항목, 위탁 기간, 수탁자 정보(기관명, 담당자명, 연락처), (재위탁 시)재수탁자 정보(기관명, 담당자명, 연락처)

※ 위탁 내용 변경 사항 발생 즉시 정보보호부로 재통보

- **(정보보호부)** 통보 받은 위탁 내용을 심사평가원 국민 홈페이지 공개

· 공개 경로: 국민 홈페이지(www.hira.or.kr) → 개인정보 처리방침 → 개인정보 처리의 위탁

3) 개인정보 처리 업무 위탁 수행 중

○ **수탁자 교육 실시**

- **(수행 주체)** 위탁부
- **(교육 횟수)** 연 1회 이상(1년 미만 계약은 계약기간 내 1회 이상)
- **(교육 방법)** 현장, 서면, 교육 기관 활용 등 수탁자 협의 후 결정

※ 교육은 위탁부 직접 실시가 원칙이나, 예외적으로 수탁자 자체 실시 가능 단, 사전에 위탁부와 협의하고 교육 증빙 제출

< 수탁자 교육 방법 >

· 위탁부가 교육 자료 등 활용하여 수탁자 대상 직접 교육 실시
· 수탁자가 교육 자료 등 활용하여 자체 교육 실시 후 위탁부에 결과 제출
※ 교육 자료: 정보기술아키텍처(EA) → 업무매뉴얼 → 수탁자 개인정보 보호 교육
· 수탁자가 정부 주관 온라인 교육 수강 후 위탁부로 수료증 등 제출
※ 정부 주관 온라인 교육: 개인정보 포털(www.privacy.go.kr) → 교육 → 온라인교육(개인수강) → 교육과정(사업자) → 공공 및 일반사업자 → 1개 과정 수강

- **(교육 내용)** 개인정보 분실·도난·유출·위조·변조·훼손 방지 관련 사항, 수탁자 법적 의무 사항 등

○ **수탁자 관리·감독(개인정보 처리 현황 점검)**

- (수행 주체) 위탁부
- (점검 횟수) 연 1회 이상(1년 미만 계약은 계약기간 내 1회 이상)
- (점검 방법) 위탁부는 '개인정보 처리 업무 위탁 현황 점검표[첨부7]'에 따라 수탁자 점검

※ 위탁부가 수탁자를 감독하는 방법에 대하여 법률에 특별히 규정된 바는 없으므로 자료제출 요구, 현장 방문, 점검 도구 배포 등 합리적인 수단을 다양하게 활용할 수 있음

※ 위탁부는 수탁자의 개인정보 처리 현황에 대한 감독을 위하여 수탁자와 협의하여 정기적 보고를 요청할 수 있음

4) 개인정보 처리 업무 위탁 종료 시

○ 개인정보 반환 · 파기

- 수탁자는 위탁 문서에 명시된 개인정보 처리 기간이 종료되었거나 개인정보 처리 목적이 사라진 경우, 지체 없이(5일 이내) 개인정보를 위탁부에 반환하거나 파기 후 '개인정보 반환·파기 확인서[첨부8]' 작성
- 위탁부는 수탁자가 개인정보를 파기하였는지를 확인하고 반환·파기 관련 증빙 자료를 보관

< 개인정보 파기 방법 >

수탁자는 개인정보를 파기할 때에는 복구 또는 재생되지 않도록 다음 중 어느 하나의 조치를 해야 함

① 완전 파괴(소각, 파쇄 등)

※ 예시: 종이 문서, 하드디스크나 자기테이프는 파쇄기로 파기하거나 용해, 또는 소각장·소각로에서 태워서 파기

② 전용 소자장비를 이용하여 삭제

※ 예시: 디가우저(Degausser)를 이용해 하드디스크나 자기테이프에 저장된 개인정보 삭제

③ 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

※ 예시: 개인정보가 저장된 하드디스크에 대해 완전 포맷(3회 이상 권고), 데이터 영역에 무작위 값(0, 1 등)으로 덮어쓰기(3회 이상 권고), 해당 드라이브를 완전한 알고리즘 및 키 길이로 암호화 저장 후 삭제하고 암호화에 사용된 키 완전 폐기 및 무작위 값 덮어쓰기 등

○ 개인정보 처리 업무 위탁 종료 후 개인정보의 추가 처리

- 위탁 종료 후라도 법률상 의무 이행, 민원 등의 목적으로 개인정보의 보관 등 추가 처리가 필요한 경우, 위탁 문서에 해당 내용을 명시

5) 개인정보 처리 업무 위탁 현황 점검

○ **(수행 주체)** 정보보호부

○ **(점검 횟수)** 연 1회 이상

○ **(점검 방법)** 서면 점검(필요 시 시스템 및 현장 점검 병행)

○ **(점검 내용)** 개인정보 처리 업무 위탁 시 위탁부가 수탁자 교육 및 관리·감독 등 법적 의무사항 준수하였는지 점검

Ⅳ 기타 유의 사항

1. 손해배상책임

○ **위탁자의 사용자 책임**

- 수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 발생한 손해배상책임에 대하여는 수탁자를 위탁자의 소속 직원으로 간주
- 손해배상 청구에서 위탁자는「민법」제756조(사용자의 배상책임)에 의한 '사용자책임(대위책임)'을 부담
  · 수탁자에 대한 선정 및 교육, 관리·감독 등에 상당한 주의를 다한 경우, 위탁자는 사용자 책임을 면함
  ※ 선정 및 교육, 관리·감독 이행 여부에 대한 입증 책임은 위탁자가 부담
  · 수탁자에 대한 선정 등 법적 유의 사항은 [첨부9] 참고

○ **수탁자의 사용자 책임**

- 수탁자의 고의 또는 과실로「개인정보 보호법」등을 위반하여 정보주체에게 손해가 발생하였을 시, 그 불법행위에 대해 손해배상 책임을 부담
  ·「민법」제750조(불법행위의 내용)에 따라 불법행위로 인한 손해를 배상할 책임을 부담

2. 개인정보 처리 업무 재위탁 시 준수 사항

○ **원칙**

- 개인정보 처리 업무 재위탁은 개인정보 유출 등의 위험성을 높이므로 최소한의 범위로 한정

○ **위탁부 조치 사항**

- 위탁부는 재수탁자를 교육하고 관리·감독할 의무가 있음
- 위탁부는 재위탁하는 업무의 내용과 재수탁자를 정보주체가 언제든지 쉽게 확인할 수 있도록 공개*하여야 함

* 공개 방법은 '개인정보 처리 업무 위탁 내용 통보(7~8p)' 참고

○ **수탁자 조치 사항**

- 「개인정보 보호법」 제26조제6항에 따라 개인정보 처리를 제3자에게 재위탁하려는 수탁자는 재위탁 사실을 위탁부에 미리 알리고 '개인정보 처리 업무 재위탁 동의서[첨부10]'에 따라 동의를 받아야 함
- 수탁자는 재수탁자의 관계에서는 「민법」 제756조(사용자의 배상책임)에 의한 '사용자책임(대위책임)'을 부담하게 되므로 재수탁자에 대한 관리·감독 의무가 있음

○ **재수탁자 조치 사항**

- 재수탁자는 수탁자와 동일하게 개인정보 보호를 위한 모든 조치*를 수행해야 함

* 조치 사항은 '개인정보 처리 업무 위탁 절차(5p)' 참고

첨부1

수탁자 개인정보 보호 역량 분석 평가표

수탁자 개인정보 보호 역량 분석 평가표

구분	평가지표	결과	비고
관리적 보호 수준	개인정보 보호계획을 수립 여부		
	개인정보 처리 방법 및 시스템 저장 여부		
	개인정보취급자 교육 프로그램 마련·운영 여부		
기술적 보호 수준	개인정보 물리적·기술적 보호조치 마련 여부		
	개인정보에 대한 방어벽 등 보호 장치 운영 여부		
	개인정보취급자에 대한 접근로그 및 관리 방안 여부		
물리적 보호 수준	개인정보 처리 장소에 대한 보안 관리 여부		
	개인정보 처리 장소에 대한 출입통제, 보안, 저장매체 등 관리 여부		
	개인정보취급자에 대한 점검 방법 등 운영 여부		
기타	(해당 시) 개인정보보호 및 정보보호 인증 획득 여부		

※ 점검 결과는 '양호', '미흡', 또는 '해당 없음' 표기

점검 일자: 0000년 00월 00일

점검 수행자: (서 명)

첨부2

개인정보 처리 업무 위탁 계약서

개인정보 처리 업무 위탁 계약서(안)

OOO(이하 “위탁자”이라 한다)과 △△△(이하 “수탁자”이라 한다)는 “위탁자”의 개인정보 처리업무를 “수탁자”에게 위탁함에 있어 다음과 같은 내용으로 본 업무위탁계약을 체결한다.

제1조 (목적) 이 계약은 “위탁자”가 개인정보 처리업무를 “수탁자”에게 위탁하고, “수탁자”는 이를 승낙하여 “수탁자”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」및「표준 개인정보 보호지침」에서 정의된 바에 따른다.

제3조 (위탁업무의 목적 및 범위) “수탁자”는 계약이 정하는 바에 따라 (_____) 목적으로 다음과 같은 개인정보 처리 업무를 수행한다.[1)]

1.
2.
3.

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 제3자와 재위탁 계약을 할 경우에는 “수탁자”는 해당 사실을 계약 체결 7일 이전에 “위탁자”에게 재위탁의 필요성 및 “재수탁자”의 적격성을 포함하여 통보하고 재위탁에 대한 동의를 받아야 한다.

제6조 (개인정보의 안전성 확보조치) “수탁자”는「개인정보 보호법」제23조제2항 및 제24조제3항 및 제29조, 같은 법 시행령 제21조 및 제30조,「개인정보의 안전성 확보조치 기준」에 따라 개인정보의 안전성 확보에 필요한 관리적·기술적 조치를 취하여야 한다.

---

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

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」에 따라 즉시 파기하거나 “위탁자”에게 반납하여야 한다.

③ 제2항에 따라 “수탁자”가 개인정보를 파기한 경우 지체 없이 “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 계약기간 내에 1회 이상 “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.

제11조 (손해배상) ① “수탁자” 또는 “수탁자”의 임직원, “재수탁자”가 이 계약에 의하여 위탁 또는 재위탁 받은 업무를 수행함에 있어 이 계약에 따른 의무를 위반하거나 “수탁자” 또는 “수탁자”의 임직원, “재수탁자”의 귀책사유로 인하여 이 계약이 해지

---

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

되어 “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.

제12조 (가명정보 처리 위탁 시) ① “수탁자”는 가명정보를 위탁받은 범위 외로 처리하여서는 안 된다.

② “수탁자”가 가명정보를 처리할 때에는「개인정보 보호법」제28조의4(가명정보에 대한 안전조치의무 등)에 따라 안전조치를 하여야 한다.

③ “수탁자”는 특정 개인을 알아보기 위한 목적으로 가명정보를 처리해서는 아니 된다.

④ “수탁자”는 가명정보를 처리하는 과정에서 특정 개인을 알아볼 수 있는 정보가 생성된 경우 즉시 해당 정보의 처리를 중지하고, 지체 없이 회수·파기하여야 한다.

⑤ “수탁자”는 가명정보가 재식별 되었거나, 재식별 가능성이 높아지는 상황이 발생한 경우에는 가명정보 처리를 중지하고, 지체 없이 “위탁자”에게 통지하여야 한다.

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

20 . . .

위탁자	수탁자
주 소 :	주 소 :
기관(회사)명 :	기관(회사)명 :
(위탁부가 속한 부서의 장) 성명 : (인)	대표자 성명 : (인)

첨부3

수탁자 개인정보 보호 서약서

수탁자 개인정보 보호 서약서

(*수탁 직원 성명*)은 건강보험심사평가원(이하 “심사평가원”)의 개인정보 처리 업무 위탁 수행에 따른 개인정보, 데이터베이스 및 개인정보처리시스템의 안전한 보호를 위해 아래 각 호의 사항을 준수한다.

1. 심사평가원의 개인정보 보호 규정을 준수하며 심사평가원이 위탁한 개인정보(데이터베이스 및 개인정보 처리시스템)를 안전하게 사용, 관리하며 개인정보의 보호를 위해 다음의 사항을 준수한다.
   1) 심사평가원의 개인정보 보호 규정 및 개인정보보호 관련 법규의 준수
   2) 업무상 알게 된 개인정보에 관한 비밀 유지
   3) 제공받은 목적 외 제공 금지
   4) 제공받거나 허가받은 개인정보 취급 업무 및 취급 권한의 제3자 공유 금지
   5) 개인정보 처리 업무 종료 시 파기 등 의무 사항 이행
   6) 심사평가원의 규정 및 관련 법규의 미준수 또는 관리 소홀로 인해 발생한 개인정보 사고에 대한 법적 책임 부담
2. 심사평가원의 사전 승인을 받지 않은 프로그램 및 정보기기는 심사평가원의 업무 위탁과 관련하여 사용하지 않는다.
3. 심사평가원의 정보보안 및 개인정보보호 정책에 반하는 행위로 야기되는 문제에 대해 민 · 형사상 책임을 진다.
4. 본인은 위의 사항을 숙지하여 이를 성실히 준수할 것이며 만일 이를 위반하였을 경우「개인정보 보호법」및「부정경쟁방지 및 영업비밀에 관한 법률」등 관련 법령에 따른 민 · 형사상의 책임을 감수함은 물론, 심사평가원에 끼친 손해에 대해 지체 없이 변상 · 복구할 것을 서약합니다.

년 월 일

소 속:

직 위:

서약자: (서명 또는 인)

첨부4

개인정보 처리 업무 위탁 사전 점검

개인정보 처리 업무 위탁 사전 체크리스트

점검 사항	결과	비고
① 위탁자(심사평가원)는 업무 위탁의 개인정보 위험성을 확인하였는가?		・개인정보 유・노출 위험성 등을 고려하여 위탁 여부 결정 ・개인정보 위험성이 높다고 판단된 경우, 위탁 여부 재검토・수탁자 감독 강화・사고 발생 시 책임소재 명확화 등의 대책 마련 필요
② 위탁자(심사평가원)는 수탁자의 개인정보 보호 역량을 확인하였는가?		・수탁자 개인정보 보호 역량 분석 평가 지표 참고
③ 위탁자(심사평가원)는 위탁하여 처리할 개인정보의 범위를 명확히 하고 수탁자와 사전 협의하였는가?		・필요 최소한의 범위 설정
④ 위탁자(심사평가원) 및 수탁자는 다음 6가지 내용이 포함된 위·수탁 문서를 작성하였는가? - 위탁 업무의 목적 및 범위 - 위탁 업무 수행 목적 외 개인정보 처리 금지 사항 - 위탁 업무 관련 보유하고 있는 개인정보 처리 현황 점검 등 감독에 관한 사항 - 개인정보의 기술적·관리적 보호조치 사항 ※ 개인정보에 대한 접근 제한 등 안전성 확보 조치 사항 - 재위탁 제한 사항 - 수탁자 준수 의무 위반한 경우 손해배상 등 책임에 관한 사항		
⑤ 위·수탁 업무 종료 후에도 수탁자가 개인정보를 보관하는 등 추가 처리를 해야하는 사유가 있다면, 사전에 위·수탁 문서에 이를 포함하였는가?		
⑥ 법령상 수탁자에게 개인정보를 보관해야 하는 의무가 발생하는 경우 위탁자에게 이를 미리 알리고 위·수탁 문서 내 법률상 근거와 개인정보 보관 기간·목적 등을 명시하였는가?		

※ 상기 점검항목은 관련 법령의 변경 등에 따라 변경·적용할 수 있음

※ 점검 결과는 '양호', '미흡', 또는 '해당 없음' 표기

점검 일자: 년 월 일

점검 수행자: (서 명)

첨부5

개인정보 인수증

개인정보 인수증

○ 제공 내역

제공자	**기관명**	건강보험심사평가원	**소속 부서**	
	직위		**성명**	
제공받는 자	**기관명**			
	직위		**성명**	
제공 일자	*0000년 00월 00일*			
제공 목적	*00업무*			
제공 항목	*성명, 연락처, 주소 등*			
제공 형태	*보안USB*			
제공 건수	*00건*			

당사는 상기 자료를 제공받았음을 확인하며, 제공받은 자료는 업무 위탁 목적으로만 사용하고, 타 기관에 재제공 금지 및 사용 후 즉시 반환·파기하는 등 개인정보 보호 관련 법규를 준수하여 제공받은 자료의 안전성을 확보하기 위해 최선을 다할 것을 서약합니다.

년 월 일

소 속:

직 위:

서약자: (서명)

첨부6

개인정보 처리 업무 위탁 내용 통보 서식

업 무 연 락

수신자 : ICT전략실장(정보보호부)

(경유)

제 목 : 0000년도 0000 사업 관련 개인정보 처리 업무 위탁 내용 통보

개인정보 처리 업무 위탁을 위해「개인정보 처리 업무 위탁 계약서」를 작성하였으며, 이에 따라 개인정보 처리 업무 위탁 내용을 아래와 같이 통보합니다.

1. 위탁명: 0000년도 0000 사업
2. 위탁 **'개인정보'** 항목: (예) 이름, 주소, 연락처
   ※작성 방법: 위탁하는 '개인정보' 항목 작성(회신 시 해당 문구 삭제)
3. 위탁 기간: 0000.00.00.~0000.00.00.
   ※작성 방법: 계약 시작일 ~ 계약 완료일(회신 시 해당 문구 삭제)
4. 수탁 업체명: ㈜0000
5. 수탁 담당자명 및 (사무실)연락처: 홍길동(000-000-000)
   ※작성 방법: 수탁 업체의 담당자 및 사무실 연락처 작성(회신 시 해당 문구 삭제)

* 간이문서(담당 전결) 정보보호부 송부(회신 시 해당 문구 삭제)

I C T 전 략 실 장

결재 담당 전결

협조

시행 정보보호부 접수 ()

우 26465 강원도 원주시 혁신로 60(반곡동) / www.hira.or.kr

/ 비공개

첨부7

개인정보 처리 업무 위탁 현황 점검표

개인정보 처리 업무 위탁 현황 점검표

○ 위탁 개요

위탁부	위탁명	위탁 기간	수탁자

○ 점검표

점검 내용	결과	비고
1. 개인정보 보호 관리 체계 기반 마련		
· 수탁 직원에 대한 개인정보 보호 서약서가 징구되었는가? ※ 수탁 인원 변경 시에도 개인정보 보호 서약서가 즉시 작성되었는가?		
2. 개인정보 보호 교육 추진		
· 수탁 직원에 대한 개인정보 보호 교육 계획을 수립하고, 이를 수행하고 있는가?		
3. 재위탁 제한		
· 재위탁 필요 시 위탁자의 동의를 받았는가?		
4. 목적 외 이용 및 제3자 제공 절차 운영		
· 위탁자가 제공한 개인정보를 목적 외로 이용하거나 제3자 제공하는 것을 제한하고 있는가?		
5. 개인정보 노출 방지		
· 개인정보처리시스템을 통하여 자료 업로드, 다운로드 시 PC나 모바일 기기 내 중요 개인정보(고유식별정보*, 민감정보 등)가 마스킹 처리 되어 있는가? * 고유식별정보: 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호		
· 개인정보 노출 방지를 위해 보안시스템 및 백신 소프트웨어를 설치하고 운영(모니터링, 정기 점검, 업데이트 등) 하고 있는가?		
6. 접근 통제 시스템		
· 침입차단시스템 또는 침입탐지시스템의 설치 및 운영을 하고 있는가?		
· 비인가된 P2P, 웹하드, 공유설정에 대한 차단을 하고 있는가?		

7. 개인정보처리시스템 접근 권한		
· 개인정보처리시스템 접근 권한에 대하여 개인정보취급자 별로 사용자 계정을 차등 부여하여 발급받고, 다른 개인정보취급자와 공유되지 않도록 하는가?		
8. 개인정보 파기 및 관리		
· 제공받은 개인정보 처리 목적이 달성되거나 보유 기간이 경과한 경우 지체 없이(5일 이내) 해당 개인정보를 복원이 불가능한 방법으로 파기하는가?		
· 개인정보 취급 과정에서 발생한 출력물 및 임시 파일을 즉시 삭제하는가?		
9. 물리적 접근 방지		
· 전산실, 자료보관실, CCTV상황실 등 개인정보를 보관하고 있는 물리적 보관 장소에 출입 통제 절차를 수립 및 운영하고 있는가?		

점검 일자: 0000년 00월 00일

(수탁자)
점검 수행자: (서 명)

(위탁자)
점검 확인자: (서 명)

참고 사항

- 점검 결과는 '양호', '미흡', '해당없음' 으로 표기
- 각 점검 항목별 증빙 자료 구비 가능한 경우 첨부
- 위탁 성격에 따라 점검 항목 추가 가능
- 수탁자 자체 개인정보 처리 업무 위탁 점검표, 개인정보 보관 장소 출입 대장, 데이터 송수신 및 삭제 관리대장, 전산자료 폐기 확인 자료(전산 화면, 물리적 파기, 업체 내부 결재 등) 등 관리 실태를 증빙할 수 있는 자료 추가 첨부

첨부8

개인정보 반환 · 파기 확인서

개인정보 반환 · 파기 확인서

○ **위탁 개요**

위탁부	위탁명	위탁 기간	수탁자

○ **반환 · 파기 내역**

제공받은 일자	*0000년 00월 00일*
제공받은 자료	*제공 · 수집된 개인정보 등 항목 및 건수 기재*
파기 일자	*0000년 00월 00일*
파기 방법	*구체적인 파기 방법 기술* *※ 예시: 소각, 파쇄, 전용 소자 장비 이용, 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행 등*

당사는 (*위탁명*) 수행을 위해 제공받은 개인정보 등을 다음과 같이 반환 · 파기하였으며, 이 정보로 인해 발생된 문제에 대해 모든 책임을 부담할 것을 서약합니다.

년 월 일

소 속:

직 위:

서약자: (서명)

첨부9

수탁자에 대한 선정 등 법적 유의 사항

수탁자에 대한 선정 등 법적 유의 사항

「민법」제756조 (사용자의 배상책임) 제1항	- 타인을 사용하여 어느 사무에 종사하게 한 자는 피용자가 그 사무 집행에 관하여 제3자에게 가한 손해를 배상할 책임이 있다. 그러나 사용자가 피용자*의 선임 및 사무감독에 상당한 주의를 한 때 또는 상당한 주의를 하여도 손해가 있을 경우는 그러지 아니한다. * 피용자는 수탁자를 의미함 - 위탁부서가 수탁자 선정 및 사무감독 등에 상당한 주의를 할 경우, 피해자에 대한 손해배상책임을 감면받을 수 있음 – 판례(대판 1998.5.15., 97다58538) · 사용자나 그에 갈음하여 사무를 감독하는 자는 그 피용자의 선임과 사무감독에 상당한 주의를 하였거나 상당한 주의를 하여도 손해가 있을 경우는 손해배상의 책임이 없으나, 이러한 사정은 사용자 등이 주장 및 증명하여야 한다.
대위책임	- 사용자 책임의 목적은 피용자(수탁자)에 대한 피해자의 손해배상청구권을 보장해주는 데 있으며, 사용자(심사평가원)의 배상의무는 단지 피용자(수탁자)가 불법행위 책임을 부담하는 경우에만 발생한다. 즉, 피용자(수탁자)가 부담하여야 할 배상의무를 사용자(심사평가원)가 마치 연대보증인처럼 대신 변제(배상)해주는 기능을 한다. 따라서 피해자에게 배상해준 사용자는 언제나 피용자에게 전액 구상할 수 있다.
주의 사항	- 판례(대판 1983.5.24., 83다카208) · 공사의 하도급계약에서 하수급인이 모든 손해배상책임을 단독으로 지겠다고 약정한 경우라도 하수급인과 도급인 사이에 지시·감독 관계가 존재하는 한 도급인의 사용자 책임은 면제되지 않는다.

첨부10

개인정보 처리 업무 재위탁 동의서

개인정보 처리 업무 재위탁 동의서

1. “ *위탁명* ”과 관련하여 건강보험심사평가원(이하 “위탁자”라 한다)과 (*수탁자명*)(이하 “수탁자”라 한다)가 체결한 “개인정보 처리 업무 위탁 계약서”를 바탕으로, “수탁자”는 위탁받은 개인정보 처리 업무를 재수탁자에 다시 위탁하려는 경우 아래 사항을 준수하여야 한다.

가. “수탁자”는 재위탁 시 개인정보 위험 증가 요소, 정보주체의 권리 불이익 영향 등 개인정보 보호 역량을 종합적으로 검토하여 개인정보 위험을 최소화할 수 있는 기관을 “재수탁자”로 선정하여야 한다.

나. “수탁자”는 재위탁 시 위탁받은 개인정보 처리 업무 수행을 위한 필요한 최소한의 개인정보가 처리될 수 있도록 처리 범위를 명확히 하여야 한다.

다. “수탁자”는 재위탁 시 「개인정보 보호법」에서 부여된 일반적인 의무 및 관계 법령 등에서 요구하는 사항을 반드시 준수하여야 하며, “재수탁자”와 개인정보 처리 업무 위탁 계약서를 체결하여야 한다.

라. “수탁자”는 재위탁 시 “위탁자”의 개인정보를 안전하게 보호할 수 있도록 “재수탁자”를 교육하고, 「개인정보 보호법」 제29조에 따른 관리적·기술적·물리적 안전조치를 이행하는지 관리·감독하여야 한다.

마. “수탁자”는 기존에 동의 받은 재위탁에 관한 내용이 변경되는 경우, “위탁자”에 이를 알리고 다시 동의를 구하여야 한다.

재수탁자(사업자번호)	업무 목적 및 범위	비고

2. 위 동의 내용을 증명하기 위하여 동의서 2부를 작성하고 서명 또는 날인하여, 동의서는 “위탁자”와 “수탁자”가 각각 1부씩 보관한다.

년 월 일

위탁자 **수탁자**

강원특별자치도 원주시 혁신로 60
건강보험심사평가원
(위탁부가 속한 부서의 장) (서명 또는 인) 대표자 (서명 또는 인)