

2025년 MPIS

개인정보관리 특수 전문기관 지정 소개 및 의료기관 대응 방안

(2025년 5월 13일)

디지털헬스보안협회장 한기태

강사 소개 : 한기태



사)디지털헬스보안협회 회장

삼육보건대학 겸임교수

병원정보보안협회 고문

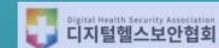
前)대한병원정보협회 회장

前)건국대학병원 의료정보팀장

사)디지털헬스보안협회 소개



안전하고 신뢰할 수 있는
디지털의료 환경 조성
디지털의료 정보보안 강화 및
국제 표준 선점
Since 2015



디지털헬스보안협회

설립 목적 및 연혁

디지털 헬스보안 강화 및 국제표준 선점

2024

- 11.29 의료기기 사이버보안 특화교육 총 9회 수행
- 10.04 정기총회 (사명변경 : 디지털헬스보안협회)
- 10.04 제13회 스마트의료 정보보호 컨퍼런스 2024
- 04.18~20 제12회 스마트의료 정보보호 컨퍼런스 2024

2023

- 12.08~12.09 스마트의료보안포럼&강원 의료정보보호 세미나
- 12.08 정기총회
- 09.23 사무국 이전 (서울 송파구 문정동)
- 08.24 한기태 의장 취임
- 08.23~08.25 스마트의료 정보보호 컨퍼런스 2023
- 01.11 사무국 이전

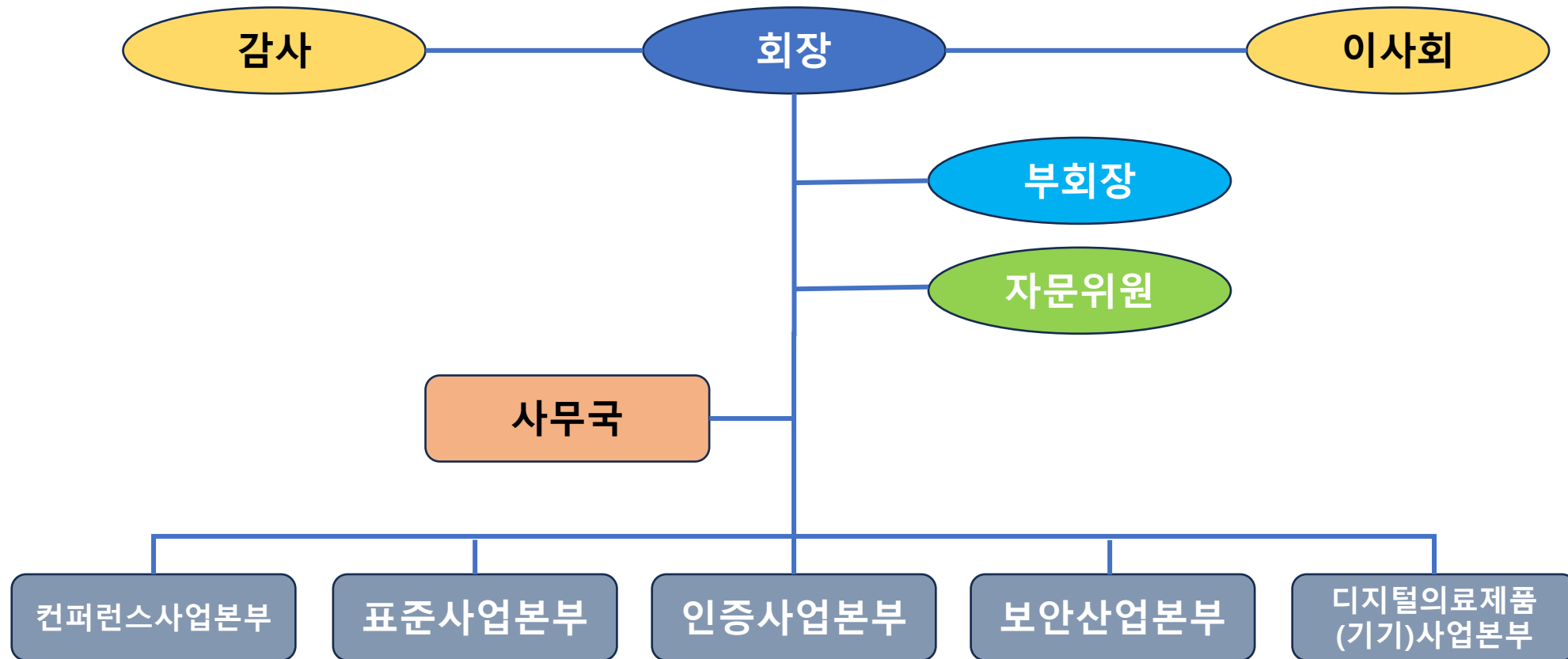
2017

- 12.01~02 정기 총회 및 워크숍
- 10.27 사무국 이전 (성남시 수정구 대왕판교로 815 기업지원허브 정보보호클러스터 460호)
- 06.27~28 스마트의료 정보보호 컨퍼런스 2017

2015

- 12.07~08 정기 총회 및 워크숍
- 12. 01 스마트의료보안포럼 설립허가 (과학기술정보통신부, 정보보호산업과)
- 11.19~20 스마트의료 정보보호 컨퍼런스 2015

[협회 조직도]



개인정보관리 특수 전문기관 지정 소개 및 의료기관 대응 방안

본 발표자료는

개인정보보호위원회 홈페이지 와

“전 분야 마이데이터 제도 시행 설명회” 자료를 인용했습니다.

1. 특수전문기관의 개념

[개인정보보호법 시행령]

제42조의9(개인정보관리 전문기관의 업무 등)


특수전문기관 : 통합조회, 맞춤형 서비스, 연구, 교육 등을 위하여 정보전송자로부터 전송 받은 **보건의료전송정보**를 관리·분석하는 업무를 수행하는 자

1. 특수전문기관의 개념

[개인정보보호법 시행령]

제42조의9(개인정보관리 전문기관의 업무 등)

특수전문기관 · 통한조회, 맞춤형 서비스, 연구, 교육 등을 위하여 **정보전송자로부터** 전송 받은 **보건의료전송정보**를 관리 · 분석하는 업무를 수행하는 자



개인정보보호법 시행령

제42조의2(정보전송자 기준) 다음 각 호에 해당 하는 자를 “정보전송자”라 한다.

“**보건의료 정보전송자**”-

질병관리청, 국민건강보험공단, 건강보험심사평가원, 상급종합병원(47개),

그 밖에 「보건의료기본법」 제3조제4호에 따른 보건의료기관 중 개인정보를 전송할 수 있는 기술적 · 재정적 능력과 그 개인정보가 저장 · 관리되고 있는 정보주체의 수 등을 고려하여 보호위원회가 보건복지부장관과 협의하여 고시하는 자

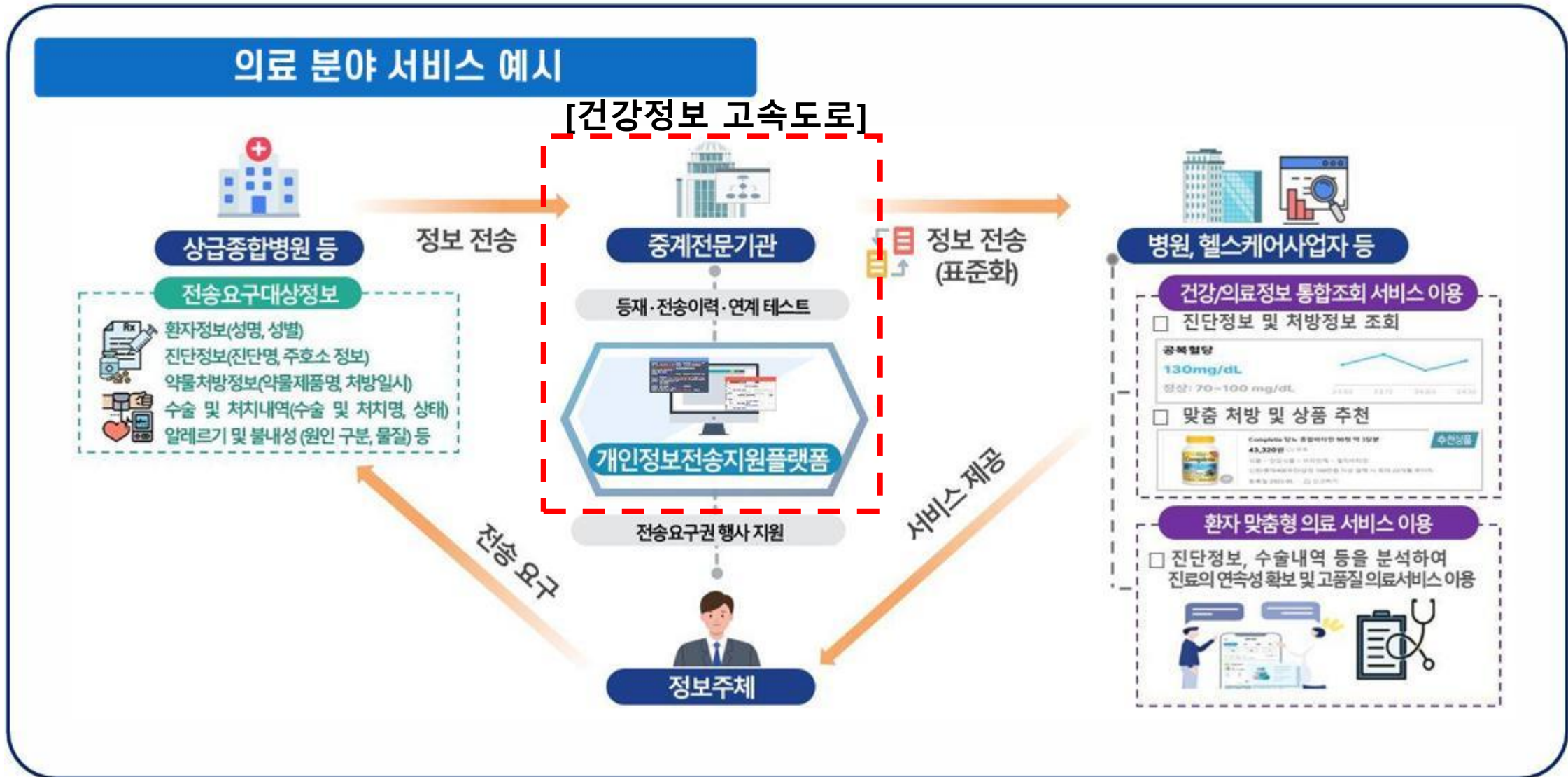
2. 마이데이터 전송 체계도

특수전문기관

상급종합병원
(47개)



3. 특수전문기관 업무흐름도



4. 보건의료 전송 정보

[개인정보보호법 시행령]

제42조의4(전송 요구 대상 정보의 범위)

「의료법」 제22조 및 제23조에 따른 진료기록 등 진료와 관련하여 생성된 정보

「약사법」 제30조에 따른 조제기록 등 조제와 관련하여 생성된 정보

「의료기기법」 제2조제1항에 따른 의료기기를 통하여 생성·수집된 정보

그 밖에 가목부터 다목까지와 유사한 보건의료 관련 정보

4. 보건의료 전송 정보

- ❖ 본인 대상 전송정보와 제3자 대상 전송정보를 일치하도록 규정
- ❖ 본인 대상 전송정보의 경우 사업자가 자율적으로 정보를 추가적으로 정보주체에게 전송할 수 있도록 규정

보건의료전송정보

- ❖ 해당 보건의료정보전송자가 보유하고, 고시된 정보 중 아래 어느 하나에 해당하는 정보
 - ① 「의료법」 제22조 및 제23조에 따른 진료기록 등 진료와 관련하여 생성된 정보
 - ② 「약사법」 제30조에 따른 조제기록 등 조제와 관련하여 생성된 정보
 - ③ 「의료기기법」 제2조 제1항에 따른 의료기기를 통하여 생성·수집된 정보
 - ④ 이와 유사한 보건의료 관련 정보

정보전송자	정보항목	세부항목	대상 범위
질병관리청	예방접종정보	접종자 현황(성명, 성별, 생년월일), 접종일자, 접종기관명, 접종차수, 예방접종명	전체기간
국민건강보험공단	건강검진정보	건강검진정보, 영유아건강검진정보, 암건강검진정보	전송 요구 시점으로부터 10년
	진료내용정보	대상자 현황, 병의원/약국 명칭, 진료개시일, 진료형태, 방문입원일수, 처방횟수, 본인부담금, 병의원 소재지	전송 요구 시점으로부터 1년
건강보험심사평가원	투약이력정보	조제일자,약품코드,약품명(제품명),성분코드,함량,투약량,투여횟수,총투약일수	전송 요구 시점으로부터 1년
「의료법」 제3조의4에 따른 상급종합병원	환자정보	성명, 성별, 생년월일	전송 요구 시점으로부터 3년
	내원정보	내원 상태, 진료 구분, 내원 기간	
	진단정보	진단 임상적 상태, 진단명, 진단 및 주호소 정보, 진단 일자	
	약물처방정보	약물 처방상태, 약물 처방 의도, 지참약 여부,약품 제품명, 약물 처방 일시, 약물 투여 방법	
	수술 및 처치내역	수술 및 처치 상태, 수술 및 처치명, 수술 및 처치 일자	
	진단검사, 기타검사	진단검사상태, 검사구분(진단, 기타), 검사항목명, 검사 일시, 검사결과, 참고구간	
	알레르기 및 불내성	알레르기 및 불내성 원인 구분,알레르기 및 불내성 원인 물질, 알레르기 및 불내성 기록 일시,알레르기 및 불내성 반응, 추가정보	
	영상검사, 병리검사	검사 상태, 검사구분(영상, 병리), 검사명, 검사 의뢰일, 검사 결과	

5. 개인정보 전송권 : 마이데이터 관련 법률 개정

[개인정보보호법]

제6조(다른 법률과의 관계) ① 개인정보의 처리 및 보호에 관하여 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따른다.

제35조의2(개인정보의 전송 요구) ① 정보주체는 개인정보 처리 능력 등을 고려하여 대통령령으로 정하는 기준에 해당하는 개인정보처리자에 대하여 개인정보를 자신에게로 전송할 것을 요구할 수 있다.

④ 제1항 및 제2항에 따른 전송 요구를 받은 개인정보처리자는 정보주체에 관한 개인정보를 전송하여야 한다.

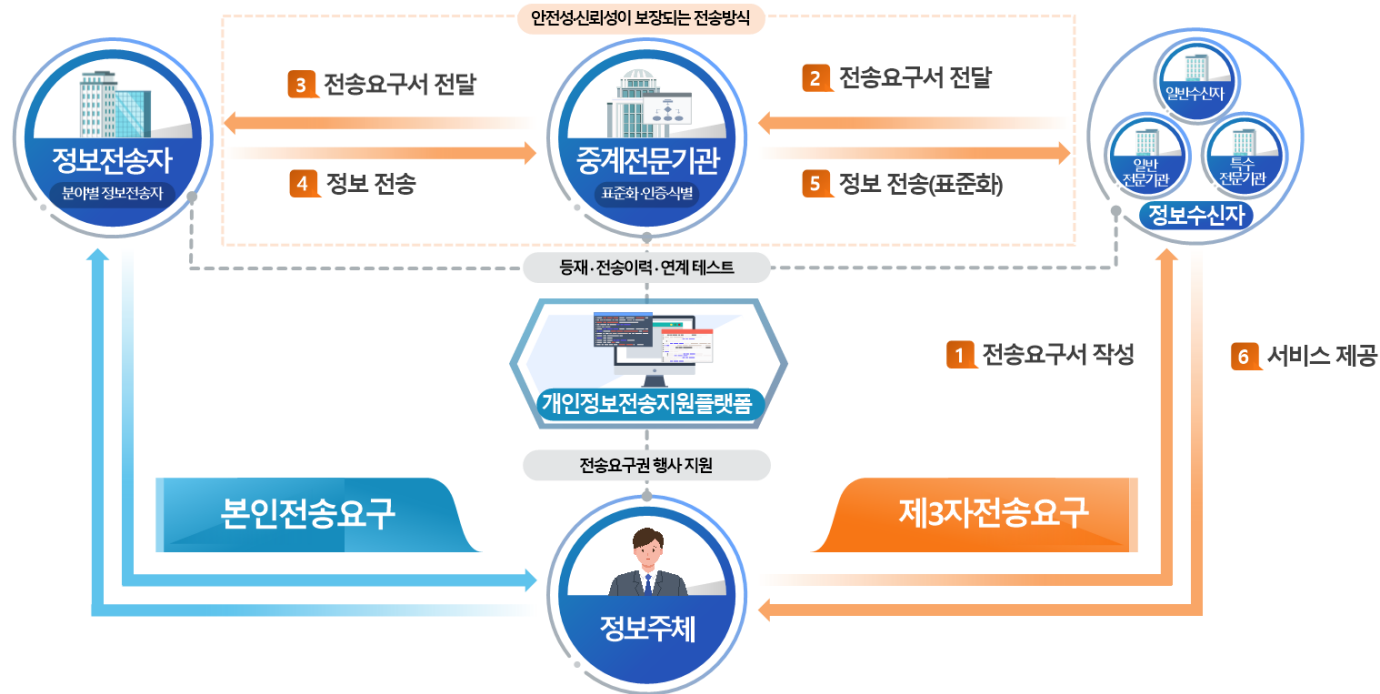
제35조의3(개인정보관리 전문기관) ① 다음 각 호의 업무를 수행하려는 자는 보호위원회 또는 관계 중앙행정기관의 장으로부터 개인정보관리 전문기관의 지정을 받아야 한다.

1. 제35조의2에 따른 개인정보의 전송 요구권 행사 지원
2. 정보주체의 권리행사를 지원하기 위한 개인정보 전송시스템의 구축 및 표준화
3. 정보주체의 권리행사를 지원하기 위한 개인정보의 관리·분석

6. 개인정보보호위원회 마이데이터 사업 추진경과



7. 마이데이터 체계도 및 주요개념



본인
전송요구

정보주체가 개인정보처리자에게 특정 요건을 충족하는 개인정보를 **‘본인에게로’** 전송할 것을 요구 할 수 있는 권리

제3자
전송요구

정보주체가 개인정보처리자에게 특정 요건을 충족하는 개인정보를 기술적으로 허용되는 범위에서 **‘제3자에게’** 전송할 것을 요구 할 수 있는 권리

7. 마이데이터 체계도 및 주요개념



정보전송자	정보주체의 요구에 따라 보유하고 있는 개인정보를 정보주체 본인 또는 제3자에게 안전하게 제공
정보수신자	제3자전송요구권에 따라 전송된 개인정보를 안전하게 전송 받아 개인 맞춤형 서비스 제공 등에 활용 (일반전문기관, 특수전문기관)
중계전문기관	개인정보 전송 중계에 필요한 시스템 운영 및 기능을 제공, 정보전송자의 전송을 지원하는 업무를 수행하는 기관
개인정보전송지원	전송이력 확인, 전송철회 요청 등 정보주체의 마이데이터 전 이용과정을 기술적으로 지원

8. 개인정보관리 (특수)전문기관 지정 심사제도

지정 심사제도

개인정보(개인 의료데이터)의 안전한 활용을 위해 사업자 업종, 개인정보보호·보안, 시스템 요건(연계환경, 보안체계 등), 서비스 계획, 데이터 활용 범위 등이 검증된 기관이 플랫폼(건강정보 고속도로)을 통해 제공되는 건강정보를 활용하여 대국민 서비스를 제공할 수 있는 제도

근거: “개인정보 전송 및 개인정보관리 전문기관 지정 등에 관한 고시” (개인정보보호위원회고시 25. 3. 5.)

개인정보관리 전문기관 지정요건

- **(기술수준 및 전문성)** ①사업계획의 타당성 및 건전성, ②개인 정보관리계획의 적정성, ③업무 수행을 위해 필요한 설비 및 기술의 적정성
- **(안전성 확보조치)** ①안전조치의무(법 § 29)를 이행하기 위한 요건을 갖출 것, ②안전한 개인정보관리 전문기관 운영을 위한 보호 체계의 적정성
- **(재정능력)** ①재무구조의 건전성 및 안전성, ②각 구분에 따른 자본금*을 보유할 것, ③손해배상책임 보험 공제 가입 또는 준비금 적립

* 중계전문기관 10억원, 일반·특수 전문기관 1억원

8. 개인정보관리 (특수)전문기관 지정 심사제도

지정 심사제도

사업계획	<ul style="list-style-type: none"> 정보주체의 권리와 이익 등을 증대하고 정보주체와의 이행상충을 방지하기 위한 사업계획이 타당하고 건전할 것
개인정보 관리계획	<ul style="list-style-type: none"> 개인정보관리 전문기관 업무를 위한 개인정보 관리 계획이 적정할 것
설비 및 기술	<ul style="list-style-type: none"> 개인정보관리 전문기관 업무를 효과적으로 수행하기 위하여 보호위원회가 정하여 고시하는 설비 및 기술을 갖추고 있을 것
보호체계	<ul style="list-style-type: none"> 개인정보관리 전문기관을 안전하게 운영하기 위하여 보호위원회가 정하여 고시하는 보호체계를 적정하게 갖출 것 법 제29조에 따른 안전조치 의무를 이행하기 위한 요건을 갖출 것
재정능력	<ul style="list-style-type: none"> 재무구조가 건전하고 안전성이 있을 것 중계전문기관은 자본금 10억원 이상, 특수전문기관은 자본금 1억원 이상을 갖출 것 (비영리법인은 기본재산, 단체의 경우 보유자산가액) 손해배상책임의 이행을 위한 보험 또는 공제에 가입하거나 준비금을 적립할 것

9. 개인정보관리 (특수)전문기관 지정 절차



10. 개인정보관리 특수전문기관 지정 업무 프로세스



[첨부 : 특수전문기관 지정 평가항목]

❖ 1. 사업계획 (점수)

심사기준	세부 심사기준
사업계획의 타당성	1.1.1 서비스 목적이 명확하며 실현 가능한가?
	1.1.2 추진 전략이 구체적이고 실현 가능한가?
	1.1.3 서비스 내용이 의료법, 건강보험법, 약사법, 생명윤리법 등 의료 관련 법령 및 관련 중앙행정기관의 소관 법령에 위배되거나 저촉될 가능성은 없는가?
	1.1.4 사업 내용이 정보주체의 권리와 이익을 증대하기 위한 내용에 해당하는가?
	1.1.5 서비스 목적을 고려할 때 전송 요구 데이터별 활용의 필요성이 있는가?
사업계획의 건전성	1.2.1 전문기관 업무 수행을 위한 조직 및 운영 인력이 마련되어 있는가? - 담당자들이 담당 업무를 수행하기에 적합한 경력을 갖추고 있는가?
	1.2.2 전문기관 업무를 수행하기 위한 비목별 세부 예산 계획이 적정하게 수립되어 있는가?
정보주체의 권리보호 방안	1.3.1 정보주체와의 이해상충 방지 방안을 적절하게 마련하고 있는가?
	1.3.2 민원 접수 방법이 적절한가?
	1.3.3 민원 대응 절차가 적절한가?
	1.3.4 서비스 가입 절차가 적절한가?
	1.3.5 서비스 가입 방법이 적절한가?
	1.3.6 서비스 탈퇴 절차가 적절한가?
	1.3.7 서비스 탈퇴 방법이 적절한가?

[첨부 : 특수전문기관 지정 평가항목]

❖ 2. 개인정보 관리 계획 [점수]

심사기준	세부 심사기준
전송요구 계획	2.1.1 개인정보 보호법 시행령 제42조의5, 제42조의6에 따라 전송요구 방법이 작성되어 있는가?
	2.1.2 개인정보 보호법 시행령 제42조의5제3항에 따라 정보주체에게 전송의 목적, 이용과 관련된 사항을 설명하고 있는가?
개인정보 처리 계획	2.2.1 개인정보 보호법 제15조, 제16조, 제23조, 제24조에 따라 개인정보 수집·이용에 관한 처리근거가 타당한가?
	2.2.2 개인정보 보호법 제22조, 제22조의2에 따라 개인정보 수집·이용 등 처리 방법이 적절한가? - 동의를 받지 않는 경우, 적절하게 고지하고 있는가? - 동의를 받는 경우, 동의항목 및 동의 방식이 적절한가? - 다크패턴 등 부당한 방법으로 수집·이용하고 있지 않는가?
	2.2.3 전송받은 정보와 타 정보가 시스템에서 분리·보관되도록 설계되어 있는가?
	2.2.4 개인정보 보유·이용기간 도과 시 개인정보를 파기하도록 설계되어 있는가?
전송요구 철회, 전송 중단 방법	2.3.1 전송요구 변경, 철회, 전송 중단 방법이 적절한가?
	2.3.2 전송요구 철회, 전송 중단 시 파기 방법이 적절한가?

[첨부 : 특수전문기관 지정 평가항목]

❖ 3. 설비 및 시설 [적/부]

심사기준	세부 심사기준
전송관리 및 연계, 전송 이력 관리기능	3.1.1 전송요구서 관리 및 정보주체 인증 기능
	3.1.2 중계전문기관의 연계 기능
	3.1.3 개인정보 전송지원 플랫폼과의 연계 기능
	3.1.4 개인정보 전송 이력의 기록·보관 기능
	3.1.5 전송받은 정보의 분리·보관 기능
	3.1.6 전송 내역, 전송받은 정보의 제3자 제공 동의내역의 중계전문기관을 통한 개인정보 전송지원 플랫폼 제출 기능
정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위한 네트워크 구성 및 보안시스템 구축	3.2.1 전송 요구 관련 시스템의 네트워크 구축
	3.2.2 전송 요구 관련 시스템에 대한 침입탐지·차단 시스템 구축

[첨부 : 특수전문기관 지정 평가항목]

❖ 4. 보호체계 (적/부)

심사기준	세부 심사기준
보호정책의 수립·시행 및 점검	4.1.1. 전문기관 업무 관련 정보의 안전성 확보를 위한 내부 관리계획
	4.1.2 개인정보 전송 이력의 기록·보관 및 점검 방안
	4.1.3 정보주체 대상 전송 내역의 통지 절차
접근권한의 관리	4.2.1 전송 요구 관련 시스템의 주요정보를 안전하게 처리하기 위한 접근권한의 관리 및 점검 체계
접근통제	4.3.1 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 중계 관련 시스템, 업무용 단말 등에 대한 접근통제 체계
	4.3.2 유출 및 해킹을 신속하게 탐지·대응할 수 있는 모니터링 체계
	4.3.3 전송 요구 관련 시스템에 접근할 수 있는 관리용 단말기를 지정·관리하고, 전송 요구 관련 시스템에 접속하려는 경우 추가적인 인증수단 등 안전한 인증수단을 적용하여 정당한 권한을 가진 자만 접속 가능하도록 조치
	4.3.4 전송 요구 관련 시스템에 접근할 수 있는 관리용 단말기에 대한 인터넷망 차단 조치
암호화	4.4.1 정보의 송·수신, 저장 등을 위한 안전한 암호화 적용
	4.4.2 암호키의 안전한 관리 체계
접속기록의 보관 및 점검	4.5.1 전송 요구 관련 시스템을 안전하게 관리하기 위한 접속기록의 보관점검 및 이상접속을 탐지하기 위한 조치
악성프로그램 등 방지	4.6.1 악성프로그램 등을 예방·탐지·대응하기 위한 조치
물리적 안전조치	4.7.1 정보를 안전하게 보관·관리하기 위한 물리적 안전조치
재해·재난 대비 안전조치	4.8.1 재해·재난 및 장애 등에 대비한 비상계획, 복구계획 및 훈련실시 방안
	4.8.2 정보의 안전한 백업 및 복구 체계
출력·복사시 안전조치	4.9.1 개인정보, 전송요구서 등을 안전하게 이용·관리하기 위한 출력·복사시 안전조치 방안
파기	4.10.1 정보의 안전한 파기를 위한 조치

[첨부 : 특수전문기관 지정 평가항목]

❖ 5. 재정능력 (점수 8 적/부)

심사기준	세부 심사기준													
자본금 규모, 재무구조 건전 및 안전성	① 최근 3년간 재무구조의 건전성 및 안전성													
	- 전문기관 지정신청자의 유동비율 ※ 평가점수: 유동비율 1.0 이상 : 50점 / 1.0 미만 : 0점													
	- 전문기관 지정신청자의 부채비율 ※ 평가점수: 환산비율(업종별 부채비율 대비 부채비율)													
	<table><tr><th>환산비율</th><th>90% 이하</th><th>100% 이하</th><th>110% 이하</th><th>110% 초과</th></tr><tr><td>배점</td><td>50점</td><td>40점</td><td>30점</td><td>20점</td></tr></table> *환산비율=(신청자 부채비율/기업경영분석 업종별 부채비율)×100 *부채비율=(유동부채+비유동부채)/자기자본×100					환산비율	90% 이하	100% 이하	110% 이하	110% 초과	배점	50점	40점	30점
환산비율	90% 이하	100% 이하	110% 이하	110% 초과										
배점	50점	40점	30점	20점										
	② 자본금 1억 이상의 재정능력													
보험 또는 공제 가입	- 최저가입금액 10억원 이상의 보험 또는 공제 가입하거나 준비금 적립 ※ 다만, 진료 목적으로 보건의료전송정보를 전송받는 경우에 해당하는 경우에는 별표 1의4에 따른 최저가입금액(최소적립금액)으로 한다. (최소금액은 매출액 10억원 이상 50억원 이하의 경우 5천만원)													