요약본

디지털헬스케어 보안모델

2020. 12.

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

배경 및 목적

2016년 세계경제포럼에서 처음 사용된 용어인 디지털헬스케어(Digital Healthcare)는 인공지능(AI, Artificial Intelligence), 사물인터넷(IoT, Internet of Things), 빅데이터, 클라우드, 블록체인 등의 정보통신기술(ICT, Information and Communications Technologies) 기술과 헬스케어를 연결하여 언제 어디서나 개인 건강 및 질환을 관리하는 산업영역으로 정의할 수 있다. 질병, 부상, 신체적·정신적 장애의 예방, 진단, 치료, 사후 관리를 통한 건강 유지 또는 개선을 의미하는 헬스케어(Healthcare)는 전통적인 병원 운영 시스템에 기반한 원내 치료 중심에서 개인 건강기록(PHR, Personal Health Record)에 기반한 맞춤형 서비스를 제공하는 건강 생활 관리 영역으로 빠르게 진화하고 있다.

최근 디지털헬스케어 기기·서비스는 소프트웨어 및 네트워크 연결성이 강화되면서 네트워크 프로토콜 기반의 보안사고가 증가하고 있다.

[표] 디지털헬스케어 기기·서비스 보안사고 사례

년도	월	보안사고 사례
2020	1	FDA에서 GE Healthcare 사의 일부 의료기기가 원격으로 제어되어 환자에게 위험을 초래할 수 있음을 발표
	3	FDA에서 SweynTooth 사이버보안 취약점은 특정 의료기기에 영향을 미칠 수 있음을 발표
2019	3	미 국토안보부에서 Medtronic 사의 체내 이식형 세동 제거기가 안전이 보장되지 않은 프로토콜을 사용하여 수집된 민감 정보에 공격받을 가능성이 있음을 발표
	6	FDA에서 Medtronic 사의 인슐린 펌프에 무선으로 연결된 다른 기기를 통해 펌프를 제어할 수 있음을 발표
	11	미 UC San diego Cybermed Conference에서 의료장비에 가상 랜섬웨어로 공격하는 시뮬레이션 시연
2018	10	FDA에서 Medtronic 사의 이식형 심장 장치와 관련된 사이버보안 취약점에 대해 환자 및 의료 서비스 제공자에게 통신 발표
		Zingbox에서 방사선학, X-Ray 및 기타 영상 시스템을 포함한 연결된 의료기기의 오류 메시지를 활용하여 민감한 정보를 얻을 수 있음을 발표

년도	월	보안사고 사례
2017	1	FDA에서 St. Jude Medical 사의 몸속에 이식된 심장박동기와 가정에 설치된 심장박동기 게이트웨이에 심각한 사이버보안 취약점이 있음을 발표
	7	DEFCON에서 정맥 펌프의 해킹을 시연하고, 환자에게 약물 투여량 조절, 개인정보 탈취에 따른 2차 위협 등이 발생할 수 있음을 발표
2016	10	Johnson&Johnson에서 최초로 인슐린 펌프에 대한 사이버보안 취약점이 있음을 발표
2015	5	FDA에서 Hospira LifeCare PCA3와 PCA4 Infusion Pump System에 대한 취약점을 이용하여 소프트웨어 코드가 조작될 경우 비인가 사용자가 해당 펌프를 조정할 수 있음을 발표
2015	6	TrapX Lab 보고서에서 구버전 Windows를 사용하는 혈액 가스 분석기에 백도어를 설치하여 보건의료기관에 대한 공격을 할 수 있음을 발표
2014	11	POC Conference 2014에서 생명과 직결된 의료장비에 침투하여 환자 상태를 마음대로 조작하고 다른 화면으로 변경할 수 있음을 발표
2013	1	FDA에서 생화학 자동 분석 장치 COBAS INTEGRA 400 분석기의 ORACLE SW 취약점을 이용하여 기기 DB에 원격으로 접근할 수 있음을 발표
	6	ICS-CERT에서 의료기기 내부에 하드 코딩된 암호에 대한 취약점을 이용하여 인공호흡기, 약물 주입 펌프 등의 수술 장비를 원격으로 조작할 수 있음을 발표
2012	10	BreakPoint 2012 Security Conference에서 맥박 조정기에 대한 사이버 보안 취약점이 있음을 발표
2011	10	인슐린 펌프에 탑재된 무선기능의 취약점을 이용하여 투여되는 인슐린양을 외부에서 조작할 수 있음을 발표

이에 따라, 디지털헬스케어 기기 · 서비스 개발단계부터 보안을 고려하여 안전하게 개발하는 것이 필요하며, 서비스 제공시에도 보안을 고려하여 안전하게 관리 및 서비스를 제공할 수 있도록 하는 것이 필요하다.

따라서, 본 가이드에서는 디지털헬스케어 서비스 제공을 위한 구성요소를 기반으로 대표적인 서비스 사례를 제시하고, 디지털헬스케어 기기 · 서비스 개발단계부터 운영단계까지 전체 수명주기에 대한 보안요구사항을 제시하고자 한다. 본 가이드를 통해 디지털헬스케어 기기 · 서비스의 안전성을 제고하고, 식품의약품안전처의 의료기기 사이버보안 허가 · 심사에 도움을 줄 수 있을 것으로 기대한다.

디지털헬스케어 서비스 모델

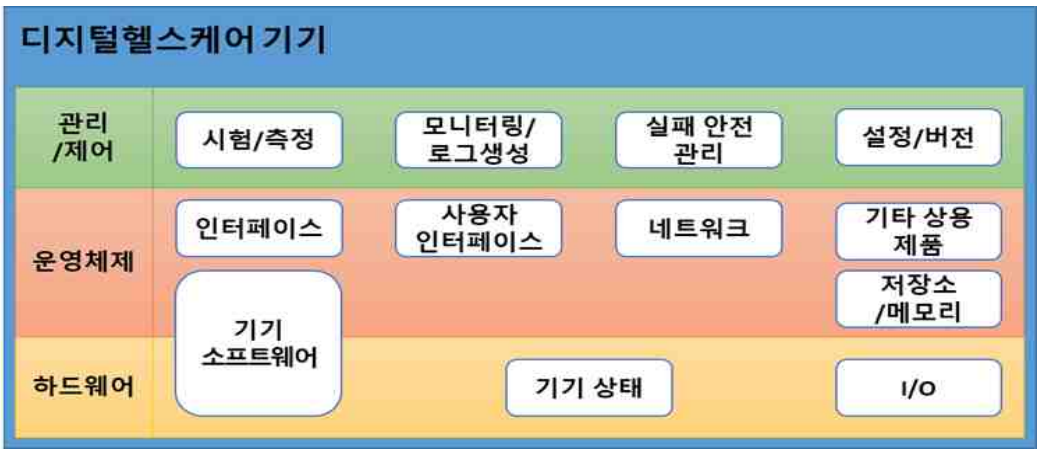
디지털헬스케어 서비스는 개인의 질병에 대한 예방, 개인 맞춤, 관리 중심의 의료서비스 형태로서 의료 기술과 ICT 기술이 융합된 기술을 활용하여 시간과 장소가 갖는 한계를 극복하고 언제 어디서나 개인의 건강 상태를 실시간으로 측정하여 환자 또는 사용자에게 최적화된 맞춤형 의료서비스를 통칭한다.

미래 의료는 4P 의료, 즉 예측의료(Predictive Medicine), 맞춤의료(Personalized Medicine), 예방의료(Prventive Medicine), 참여의료(Participatory Medicine)로 질병의 사전 예방 및 예측, 환자 개인에 대한 맞춤형 그리고 환자의 역할 확대로 변할 것이라고 예측하고 있으며, 디지털헬스케어 서비스는 이를 구현할 수 있는 개념이라고도 할 수 있다.

디지털헬스케어 서비스는 디지털헬스케어 기기들이 디지털헬스케어 기기 또는 진료정보시스템 또는 IT시스템 등과의 연계를 통해 제공되기 때문에 디지털헬스케어 기기의 역할이 매주 중요하다. 미국의 의료분야 비영리기관인 IHE(Integrating the Healthcare Enterprise)는 디지털헬스케어 기기의 기본 구조를 다음 그림과 같이 하드웨어, 상용 운영체제, 기기 관리 및 제어 영역으로 구분하여 제시하였다.

하드웨어 영역은 일반적으로 성능, 기능, 실시간이 중요하며, 입출력(I/O), 기기 상태, 기기 소프트웨어 구성요소를 포함한다. 상용 운영체제 영역에는 인터페이스, 사용자 인터페이스, 네트워크, 저장소 및 메모리, 기타 상용 소프트웨어, 기기 소프트웨어 구성요소를 포함한다. 기기의 운영체제 환경(및 실행되는 관련 상용 아키텍처 하드웨어 플랫폼)은 일반적으로 기기의 상위 기능을 수행하지만 성능 및 실시간 중요도가 낮다. 운영체제는 상용 하드웨어 구성요소 (마더보드 또는 컴퓨터)나 맞춤형 설계 플랫폼에서 실행될 수 있다. 마지막으로 기기 관리 및 제어 영역은 기능 오류에도 안전하게 동작할 수 있도록 하는 역할을 담당하며, 시험 · 측정, 모니터링 · 로그생성, 실패 안전 관리, 설정(형상) · 버전 구성요소를 포함한다.

그림 디지털헬스케어 기기 구조 (출처: IHE Medical Device Cybersecurity)



■ 하드웨어 영역

▶ 입 · 출력(I/O) : 전용 입 · 출력 연산으로, 실제 기기 기능으로 여길 수 있음 (예, 입력 : 전극, 센서, 다이얼, 스위치으로부터의 입력, 출력: 모터, 자극기, 신호 발생기로의 출력)

▶ 기기 상태 : 설정을 저장하고 이벤트를 기록하거나 기타 상태 또는 제어 데이터를 유지하는 데 사용되는 레지스터 또는 메모리

▶ 기기 소프트웨어 : 일반적으로 기기 하드웨어나 펌웨어에 가까움. 상위 소프트웨어(예, 운영체제)와 하위 소프트웨어(예, 기기 펌웨어)간 통합 및 인터페이싱 뿐만 아니라, 기기 기능, 신호 입 · 출력, 기기 상태 제어 및 레지스터를 제어하고 관리하며, 시간이 중요함

■ 상용 운영체제 영역

▶ 인터페이스(I/F) : 일반적인 입 · 출력 기능에 대한 표준 기반 인터페이스(예, USB, 블루투스)

▶ 사용자 인터페이스(U/I) : 일반적으로 키보드, 마우스, 디스플레이, 터치 스크린과 같은 사용자 인터페이스

▶ 네트워크 : 표준 기반 유 · 무선 네트워크 연결

▶ 저장소 및 메모리 : 기기의 휘발성(예, RAM) 및 비휘발성(예, 하드디스크) 저장소와 메모리 구성요소

▶ 기타 상용 소프트웨어(비-운영체제) : 운영체제 외에 상용 소프트웨어 구성요소(예, 데이터베이스, 자바 가상신 등)

▶ 기기 소프트웨어 : 일반적으로 상용 프로그래밍 언어로 작성되고 정보 전송, 기기 관리 등과 같은 기기의 상위 기능을 처리하는 어플리케이션 소프트웨어

■ 관리 · 제어 영역

▶ 시험 및 측정 : 기기의 정상작동 여부 시험 및 교정 필요 여부 측정

▶ 모니터링 및 로그 생성 : 에러에 대한 모니터링 및 로그 생성

▶ 실패 안전 관리 : 기기 실패시에도 안전하게 기기가 동작할 수 있도록 관리

▶ 설정 및 버전 : 기기 설정(형상) 및 버전 관리

디지털헬스케어 기기는 개인의료정보 및 생체정보를 측정 및 수집하고, 의료기관 등에 전송 및 저장하여 의사가 진단가능하게 도와주는 진단 및 예방관리의 목적으로 사용할 수 있으며, 환자를 수술 및 치료하기 위한 목적으로 사용할 수 있다. 또한, 환자의 생명유지를 위한 목적이나 사용자의 건강 관리를 위한 목적으로 사용할 수도 있다.

디지털헬스케어 기기의 역할에 따라 수술 및 치료, 감시, 분석, 진단, 건강관리 등으로 분류할 수 있으며, 다음과 같이 기기 역할에 따라 사용자 및 사용 장소 등을 구분할 수 있다.

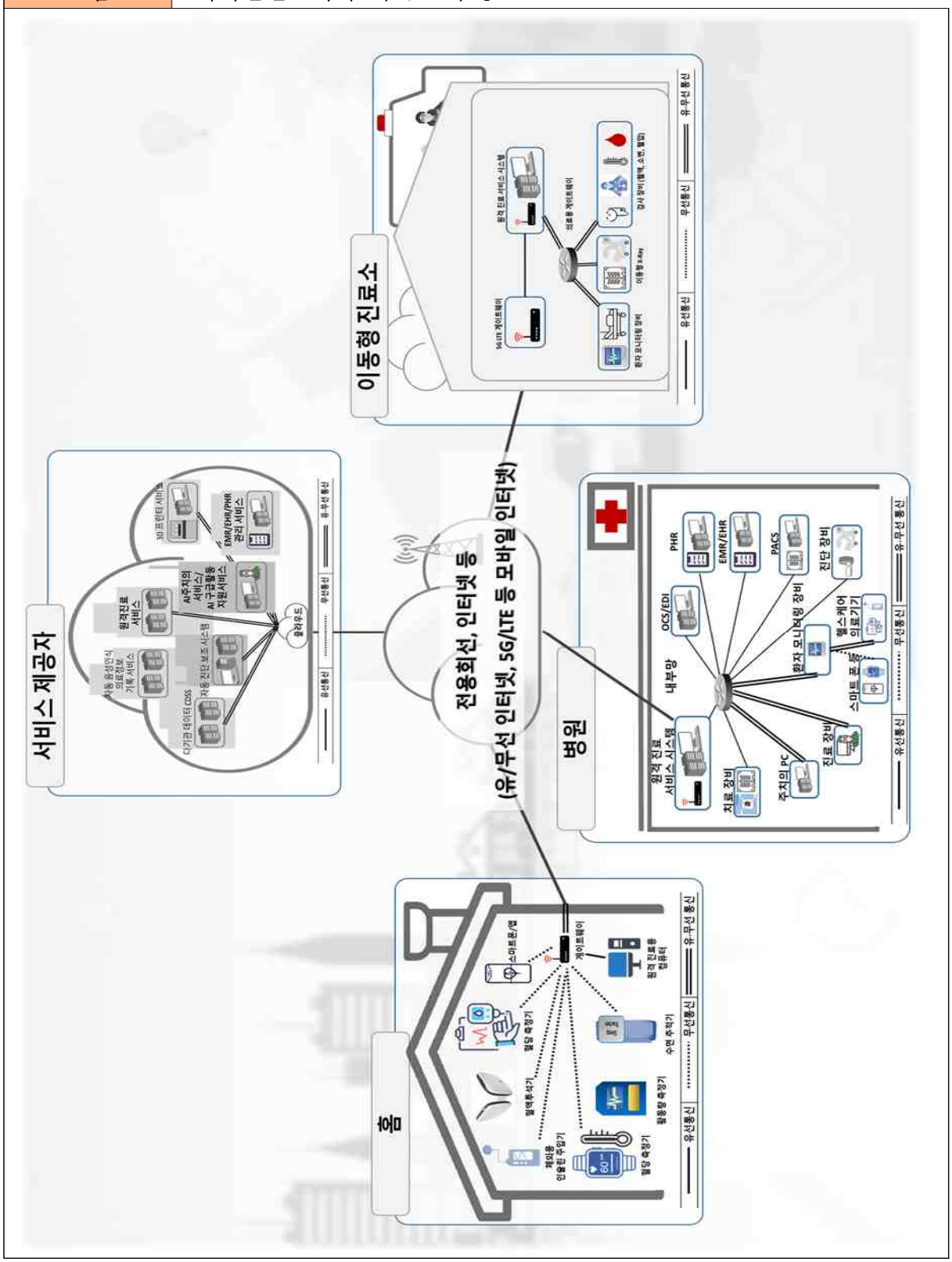
[표] 디지털헬스케어 기기의 역할에 따른 분류

구분	수술 · 치료	감시 · 측정	분석	진단	건강관리
대상	• 환자	• 환자	• 환자 • 일반인	• 환자 • 일반인	• 일반인
조작	• 의사	• 의사 등 의료인	• 의사 등 의료인	• 의사	• 일반인
관련 기기	• 로봇수술기 • 레이저수술기 • 치료용X선조사장치 • 고출력심장충격기 등	• 환자감시장치 • 인공호흡기 등	• 의료영상진단보조장치 • 의료영상검출보조장치 • 혈구세척원심분리기 등	• 자기공명전산화단층촬영장치 • X선 촬영장치 • 초음파영상진단장치 • 진단지원시스템 등	• 자동혈압계 • 전자체온계 등
사용 장소	• 병원	• 병원 • 이동형 진료소	• 병원 • 서비스 제공자	• 병원 • 이동형 진료소	• 가정(홈)

디지털헬스케어 서비스 제공을 위한 구성요소는 ‘ICT 융합 표준 프레임워크 – 스마트헬스(2019.12, ETRI)’, ‘유헬스 서비스 참조모델(2014.4.10., TTAK.KO-10.0463/R1)’, ‘스마트의료 서비스 참조 모델의 보안위협(2017.11.9., TTAR-12.0026)’ 등에서 사용자, 서비스 공급자, 병원 등으로 제시하고 있으며, 최근 발간된 ETRI 자료에서는 병원 도메인에 이동 진료소를 포함시키고 있다.

이를 기반으로 다양한 목적의 디지털헬스케어 기기 및 의료정보시스템 등을 기반으로 디지털헬스케어 서비스를 제공하기 위한 구성요소를 다음 그림과 같이 홈, 이동형 진료소, 병원, 서비스 제공자와 같이 재구성할 수 있다.

그림 **디지털헬스케어 서비스 구성요소**



[표] 디지털헬스케어 기기의 역할에 따른 분류

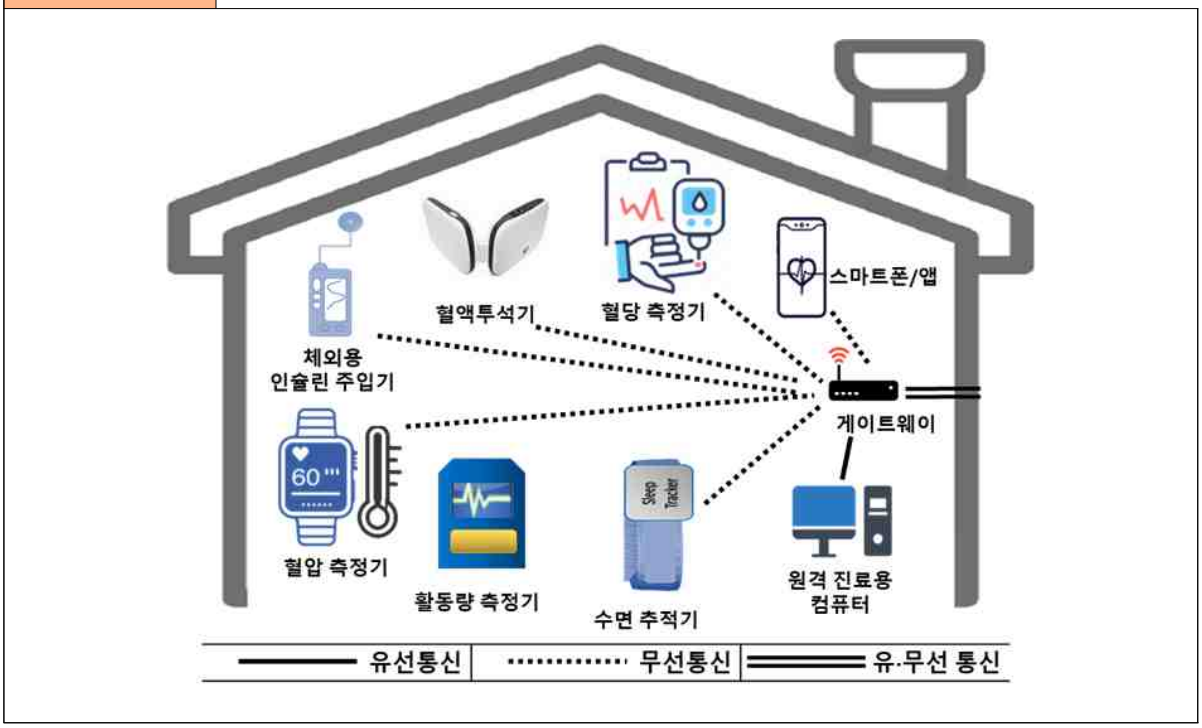
구성요소	설명	서비스 및 기기 예시
홈	• 기능: 개인 의료 정보 수집 및 전송 • 역할: 사용자와 사용자가 사용하는 단말을 구성하는 사용자 애플리케이션, 진료정보I/F, 통신 모듈, 그리고 사용자의 건강 상태 측정을 위한 PHD 등으로 구성됨. 사용자는 PHD를 통해 건강 상태를 측정하여, 사용자 단말을 통해 외부와 연동하며, 또한 사용자 단말의 애플리케이션을 이용하여 원격 서비스를 제공받음 ※ PHD: Personal Health Data	• 스마트 기기, PHD, 헬스케어 IoT, 웨어러블 기기, Home IoT 기기 등
이동형 진료소 (구급차 포함)	• 기능: 원격 의료서비스 • 역할: 비대면으로 환자를 진단 및 치료 수행하고, 이동 중인 환자의 상태를 감시할 수 있음	• 원격진료 서비스 시스템, 생명 유지용 의료기기, AI 이동 진료소, 구급차, 보건소 등
병원	• 기능: 의료서비스 • 역할: 환자를 진료하며, 원격진료 시스템을 이용하여 외부 사용자들과 연동하며 환자의 개인정보 보호를 위해 시스템들은 내부망을 이용하며 통신 G/W를 통해서 외부 도메인에 위치한 시스템들과 연결됨. 의료인, 진료 장비, 검사장비, 원격진료 서비스 시스템, 원격진료 서비스 클라이언트, PACS, CDSS, EMR, 진료정보 I/F, 통신 G/W 등으로 구성됨 ※ OCS: Order communication system ※ EMR: Electronic Medical Record ※ EHR: Electronic Health Records ※ EDI: Electronic data interchange ※ CAD/FMS: 3D 파일관리시스템 ※ PACS: 의료영상저장전송시스템 ※ CDSS: Clinical Decision Support System	• 진료 장비, 진단 장비, 뷰어(3D모델 뷰어 포함), 원격진료 서비스 시스템, PACS, CAD/FMS, EMR/EHR, EDI, OCS
서비스 제공자	• 기능: 서비스 공급 • 역할: 건강관리와 관련 정보 서비스를 제공하는 것으로, 병원 외부 서비스는 시험기관 시험시스템, 의료 빅데이터, PGHD 및 PHR, MyData 시스템, 3D 프린팅 출력소, 3D 프린팅 보철 제작소, 공공 데이터 시스템 등으로 구성되고 내부 서비스는 자동진단 보조 시스템, 다기관 데이터 CDSS, 자동 음성인식 의료 정보 기록 시스템, 인공지능 주치의, 만성질환 케어 에이전트, 3D 임플란트 프린팅, 비삽입형 3D 프린팅, 3D 프린팅 클라우드 중계, 개인맞춤형 보철 3D 프린팅, 치과 교정 및 CAD 자동화 등으로 구성됨 ※ PHR: Patient Health Record ※ PGHD: Patient-Generated Health Data ※ CDSS: Clinical Decision Support System	• 자동 진단보조 시스템, 다기관 데이터 CDSS, 자동음성인식 의료정보기록 시스템, 인공지능주치의 시스템, 3D 프린팅 임플란트, 비삽입형 3D 프린팅, 만성질환 케어 에이전트시스템, MyData, PGHD, 3D프린팅 출력소, 3D 프린팅 보철 제작, 공공데이터, 의료빅데이터

가. 홈(Home)

디지털헬스케어 서비스를 제공하기 위한 구성요소 중 홈은 개인이 디지털헬스케어 기기를 기반으로 디지털헬스케어 서비스를 제공받는 도메인이다. 홈은 개인의료정보 및 개인건강정보를 수집(센싱), 전송, 분석 요청, 검색 기능을 수행하고 서비스를 제공한다. 사용자는 디지털헬스케어 기기를 통해 자신의 건강 상태를 측정하고, 측정된 정보를 서비스 제공자에게 전송하여 분석된 정보를 제공받을 수 있다. 또한 디지털헬스케어 기기의 애플리케이션을 이용하여 원격의료 서비스를 제공받을 수 있다.

홈 도메인에서 사용될 수 있는 디지털헬스케어 기기는 다음 그림과 같이 혈당측정기, 체외용 인슐린 주입기, 혈압 측정기 등이 있으며, 스마트폰(앱)을 통해 디지털헬스케어 기기를 연동하거나 정보를 조회할 수 있다. 디지털헬스케어 기기가 직접 또는 게이트웨이를 통해 외부로 데이터를 전송할 수 있다.

그림 **디지털헬스케어 서비스 구성요소 : 홈**



■ 홈 관련 기기

사용자 또는 환자가 착용하거나 근거리 통신이 가능한 거리에서 사용되며, 주로 사용되는 통신 방식은 댁내에 구성된 무선 네트워크로 Wi-Fi, Bluetooth, ZigBee, NFC 등의 통신 방식이 일반적이다. 원격 서비스 또는 클라우드에 접속하는 경우 광대역 네트워크인 5G, LTE, 3G망을 이용할 수 있으며, 소규모 네트워크를 구성하고 있는 Wi-Fi, Bluetooth, ZigBee, NFC 등은 게이트웨이 또는 스마트 기기를 이용하여 개인의료정보 또는 개인건강정보를 전송한다. 스마트 기기(스마트폰, 태블릿 PC 등), 게이트웨이 등 연동(전송) 목적의 기기를 제외한 의료 및 웰니스 목적의 기기는 대부분 저사양의 MCU로 구성되어 운영체제가 없는 펌웨어 또는 RTOS(Real-Time Operating System)로 구현되어 있다.

[표] 홈과 관련된 디지털헬스케어 기기 유형

분류	관련 기기	운영체제	통신인터페이스	비고
의료	인슐린 펌프, 혈당측정기, 심박계, 혈압측정기	펌웨어, RTOS,	Bluetooth, Wi-Fi, IRDA, Sub-Giga RF, USB, RS232, Ethernet	의료기기 (측정 등)
웰니스	활동량계, 체온계, 혈당계, 혈압계, 체지방 측정계	펌웨어, RTOS	5G, LTE, 3G, Bluetooth, Wi-Fi, IRDA, Sub-Giga RF, USB, RS232, Ethernet	개인건강을 위한 기기
연계 (전송)	이동형 스마트 기기(스마트폰), 홈게이트웨이, 스마트와치 등	윈도우즈, 안드로이드, 리눅스, 펌웨어 등	5G, LTE, 3G, Bluetooth, Wi-Fi, IRDA, USB, RS232, Ethernet	기기와 연계을 위한 일반 스마트 기기

■ 홈 관련 서비스

홈 관련 디지털헬스케어 기기는 개인의료정보 및 개인건강정보를 수집(센싱), 전송, 분석 요청, 검색 기능을 수행을 수행하기 때문에 주로 병원 데이터베이스, 원격진료를 위한 의료서비스 제공자와의 연계 서비스를 제공한다.

홈 관련 기기 기반의 대표적인 디지털헬스케어 서비스는 다음 같다.

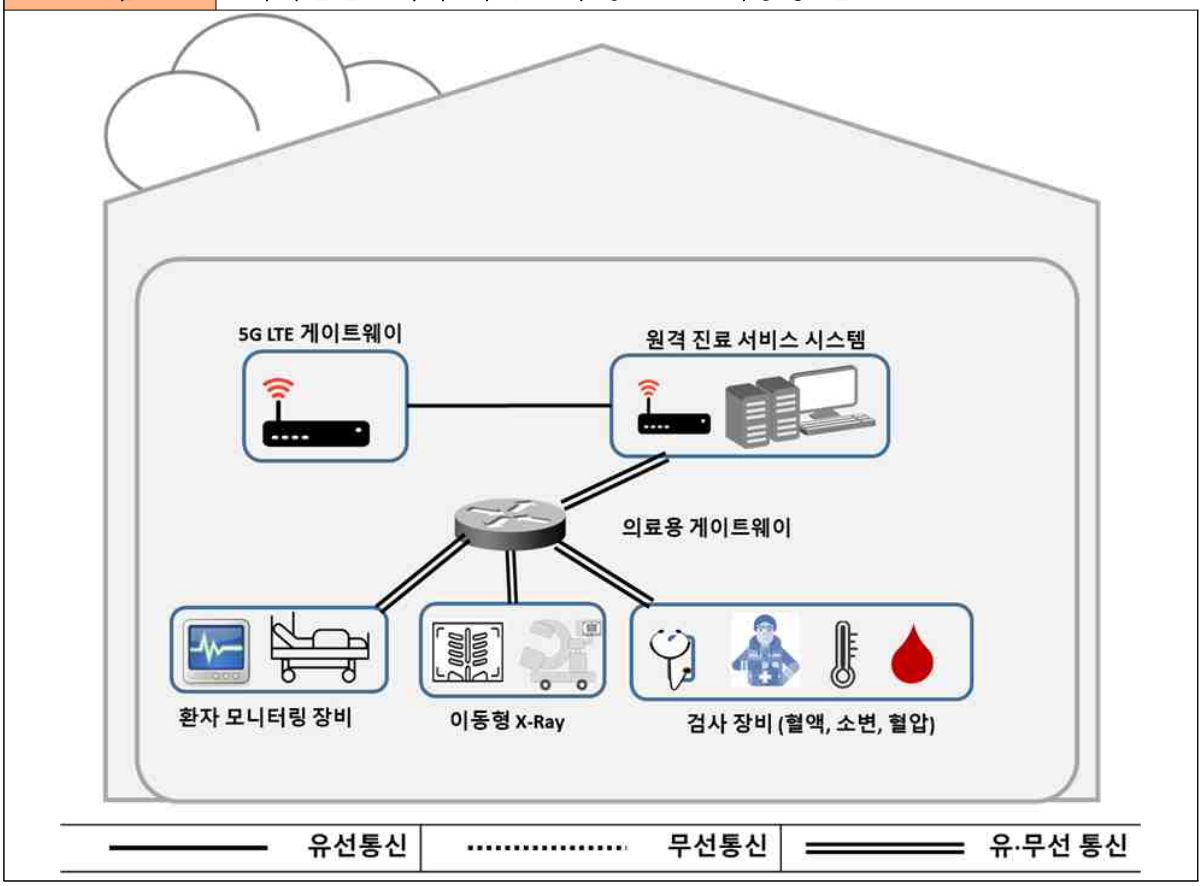
- ✓ 주치의 및 인공지능 주치의와의 **원격진료 서비스**
- ✓ 환자 모니터링에 따른 병원 또는 서비스 제공자로부터 제공받는 **응급의료 서비스**
- ✓ 병원 및 서비스 제공자 데이터베이스를 이용한 혈당, 혈압, 간수치 모니터링을 위한 데이터 전송이 수반되는 **만성질환 모니터링 서비스**
- ✓ 피트니스 등 개인건강관리를 위한 **건강정보 모니터링 및 개인 트레이닝 서비스**

나. 이동형 진료소

디지털헬스케어 서비스를 제공하기 위한 구성요소 중 이동형 진료소는 이동성이 고려된 디지털헬스케어 기기를 기반으로 간소화되거나 응급 형태의 디지털헬스케어 서비스를 제공하는 도메인이다. 이동형 진료소는 도서지역의 비대면 진단 및 치료와 이동(이송) 중인 환자의 상태를 모니터링하며 치료 서비스를 제공할 수 있다. 대표적 서비스 모델로는 구급차 내 설치된 디지털헬스케어 기기와 운영 시스템을 볼 수 있다.

이동형 진료소 도메인에서 사용될 수 있는 디지털헬스케어 기기는 다음 그림과 같이 심전도, 맥박 등과 같은 환자 모니터링 장비와 이동형 X-ray, 혈액 등 검사 장비 등이 있다. 또한, 이동형 원격진료 서비스 시스템을 통해 병원의 전문의로부터 응급처지 방법, 화상 진료 등 의료서비스를 제공받을 수 있다. 홈 도메인과 같이 디지털헬스케어 기기가 직접 또는 게이트웨이를 통해 외부로 데이터를 전송할 수 있다.

그림 디지털헬스케어 서비스 구성요소 : 이동형 진료소



■ 이동형 진료소 관련 기기

이동형 진료소 관련 디지털헬스케어 기기는 이동형 진료 장비, 이동형 환자 모니터링 장비, 원격진료 서비스 시스템(병원과 실시간 응급환자(구급차 이송)의 진료를 연결해 주는 시스템), 게이트웨이 · 스마트 기기가 있을 수 있다. 이동성이 고려되어야 하는 이동형 진료소 관련 디지털헬스케어 기기 특성상 다양한 무선 통신 방식이 제공되어야 한다. 구급차 등 이동(이송) 중 환경에서는 이동(이송) 중 진단 및 치료의 실시간 서비스가 제공되어야 하기 때문에 광대역 이동통신망인 5G, LTE, 3G 네트워크를 이용하며, 구급차 내부에서는 Wi-Fi, Bluetooth 등의 무선 통신과 Ethernet, USB, RS485 등의 근거리 통신 방식을 복합적으로 이용할 수 있다. 이동형 진료 기기에 근거리 통신 방식의 기능만 보유한 기기들의 경우는 차량용 광대역망 게이트웨이인 이동형 모뎀 등을 이용하여 네트워크를 구성할 수 있다.

[표] 이동형 진료소 관련 디지털헬스케어 기기 유형

분류	관련 기기	운영체제	통신인터페이스	비고
이동형 진료 장비	휴대용 간이 인공호흡장치, 자동심장충격기, 실시간 영상 전송 장치	윈도우즈, 안드로이드, 리눅스, 유닉스, RTOS, 펌웨어 등	5G, LTE, 3G, Bluetooth, Wi-Fi, IRDA, GPS, USB, RS232, Ethernet	수술, 치료를 위해 사용되는 장비 및 시스템
이동형환자 모니터링 장비	산소포화/ 심전도 측정기, 수액 주입기 등	윈도우즈, 안드로이드, 리눅스, 유닉스, RTOS, 펌웨어 등	5G, LTE, 3G, Bluetooth, Wi-Fi, IRDA, GPS, USB, RS232, Ethernet	이동 중 환자 상태 파악을 위한 시스템
이동형 원격진료 서비스 시스템	응급구조 원격진료 프로그램 등 (서버 · PC, 스마트 기기)	윈도우즈, 안드로이드, 리눅스, 유닉스 등	5G, 4G, 3G, Ethernet	실시간 응급환자(구급차 연계 포함) 진료 등
연계 (전송)	이동형 스마트 기기(스마트폰), 게이트웨이 등	윈도우즈, 안드로이드, 리눅스, 펌웨어 등	5G, LTE, 3G, Bluetooth, Wi-Fi, IRDA, USB, RS232, Ethernet	외부 서비스와의 연계를 위한 스마트 기기

■ 이동형 진료소 관련 서비스

이동형 진료소 관련 디지털헬스케어 기기는 환자 이동(이송) 시 진료와 치료를 수행하거나 환자 상태를 확인하며 원격에서 의사의 도움을 받아 현장에서 의료

행위가 수행되기 때문에 주로 병원 원격 시스템과 연계되거나 서비스 제공자의 데이터베이스와 연계된 서비스를 제공한다.

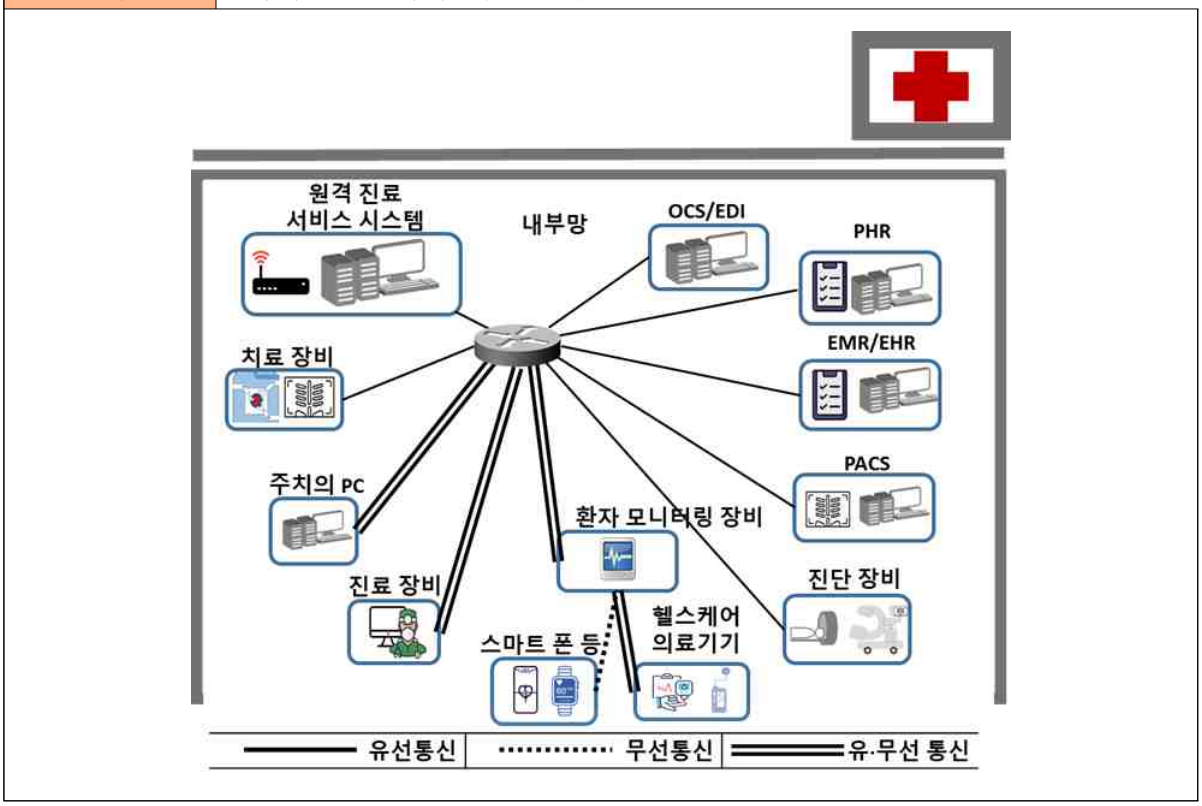
이동형 진료소 관련 기기 기반의 대표적인 디지털헬스케어 서비스는 다음 같다.

- ✓ 응급환자 이송 중 5G 네트워크 등을 이용한 실시간 환자 진료 및 이동식 수술 로봇을 이용한 응급 수술 등의 **원격의료 서비스**
- ✓ 병원 또는 서비스 제공자의 환자 상태 모니터링을 통해 현장 인원(예, 구급대원)에게 응급처치 매뉴얼 제공 등의 **응급의료 서비스**

다. 병원

디지털헬스케어 서비스를 제공하기 위한 구성요소 중 병원은 디지털헬스케어 서비스 제공에 있어 중추적인 역할을 담당하고 있다. 디지털헬스케어 서비스 구성요소에 속한 모든 디지털헬스케어 기기와 연계하여 개인의료정보가 처리되고 다양한 디지털헬스케어 서비스를 제공한다. 병원에서는 기본적으로 대면 진료를 기반의 서비스가 제공되고, 환자의 상태를 진단하기 위하여 MRI, CT, 엑스레이 등의 다양한 디지털헬스케어 기기를 사용한다. 현재, 우리나라의 원격의료 서비스는 초기 단계에 머물러 있으나, 국외 디지털헬스케어 서비스는 초고속 정보통신기술을 기반으로 비대면 및 원격의료 서비스로 진화하고 있다.

그림 디지털헬스케어 서비스 구성요소 : 병원



■ 병원 관련 기기

병원에 구축된 디지털헬스케어 기기는 의료정보시스템, 진료장비, 수술 · 치료장비, 모니터링 장비, 기기 관리 시스템, 원격진료 서비스 시스템, 네트워크 인프라 등이 있다. 관련 디지털헬스케어 기기는 대면 또는 비대면(원격진료) 등 진단, 치

료 등의 기능을 수행하거나 지원하는 역할을 하며, EMR, HER, PHR, PACS 등 의료 정보 저장 및 분석을 지원하는 기능도 수행한다. 최근에는 고도화된 수술 장비인 다빈치 로봇을 이용한 수술도 진행되고 있다.

디지털헬스케어 관련 시스템이 도입되기 전에는 의료 서비스는 병원 내부에서만 이루어졌고, 의료정보는 종이 문서 기반으로 처리되었다. 그러나, 디지털헬스케어 기기 및 의료정보시스템 등 정보통신기술이 의료분야에 도입되면서 의료서비스의 디지털화가 진행되었다. 병원 내에서 운영되는 진료 기기, 치료 기기, 모니터링 기기는 고사양의 윈도우즈 운영체제 기반의 제품에서부터 8-비트 MCU로 구성된 펌웨어 기반의 다양한 기기들로 구성되어 있으며, 네트워크 통신은 RS485 시리얼 통신부터 광대역 통신망인 5G 통신에 이르기까지 다양한 통신방식을 제공하고 있다.

[표] 병원 관련 디지털헬스케어 기기 유형

분류	관련 기기	운영체제	통신인터페이스	비고
원격진료 서비스	주치의 PC 프로그램, 응급구조 원격진료 프로그램 등 (서버, 스마트 기기기반)	Windows, 안드로이드, 리눅스, 유닉스 등	5G, 4G, 3G, Ethernet	주치의 온라인 문진 진료, 개인 의료기기 정보기반 원격진료, 실시간 응급환자(앰뷸런스 연계 포함) 진료 정보 등
EMR/HER/PHR/ PACS	PC, 서버, 웹서버	Windows, 안드로이드, 리눅스, 유닉스 등	5G, 4G, 3G, Ethernet	전자의료기록, 임상의사결정 지원 정보
진료 장비	골밀도 촬영기, MRI, CT,엑스레이, 초음파 진단기, 안압 측정기심혈관 촬영기 등	Windows, 안드로이드, 리눅스, 유닉스, RTOS, 펌웨어 등	5G, LTE, 3G, Bluetooth, Wi-Fi, IRDA, USB, RS232, Ethernet	환자 진료 정보
환자 모니터링장비	산소/심박 측정기, 수액 주입기등	Windows, 안드로이드, 리눅스, 유닉스, RTOS, 펌웨어 등	5G, LTE, 3G, Bluetooth, Wi-Fi, IRDA, USB, RS232, Ethernet	환자 입원 후 상태 정보
환자 치료 장비	다빈치 로봇, 레이저 주사기, 충격파 치료기, 수술모니터링 시스템, 방사선 치료기, 심박쇄동기 등	Windows, 안드로이드, 리눅스, 유닉스, RTOS, 펌웨어 등	5G, LTE, 3G, Bluetooth, Wi-Fi, IRDA, USB, RS232, Ethernet	수술, 치료 필요 정보 및 치료 결과 정보
스마트기기	이동형 스마트기기(스마트 폰	Windows, 안드로이드, 리눅스,	5G, LTE, 3G, Bluetooth, Wi-Fi,	개인 건강상태 정보, 운동량 및

분류	관련 기기	운영체제	통신인터페이스	비고
	류), 홈게이트웨이	펌웨어 등	IRDA, USB, RS232, Ethernet	활동량 정보
환자 웨어러블 기기	인슐린 펌프, 혈당측정기, 심박계, 혈압 측정기	펌웨어, RTOS,	Bluetooth, Wi-Fi, IRDA, Sub-Giga RF, USB, RS232, Ethernet	병원내 환자 상태 및 의료 정보

■ 병원 관련 서비스

병원은 디지털헬스케어 서비스 제공을 위한 중추적인 역할을 담당하고 있으며, 서비스 구성요소에 속한 디지털헬스케어 기기들이 매우 복잡하게 연계되어 다양한 서비스 제공하고 있다. 병원은 일반적으로 별도 내부망으로 구성되어 폐쇄망 구조가 기본이지만 디지털헬스케어 기기에 대한 원격지원 및 업데이트를 위해 제한적으로 외부망 연결이 제공된다. 최근에는 비대면진료에 대한 요구가 증가하면서 병원의 원격진료 시스템이 홈 및 이동형 진료소와 연계된 서비스가 제공될 수 있으며, 의료정보에 대한 분석을 위한 서비스 제공자와 AI 기반의 빅데이터 분석 시스템과의 연계된 서비스가 제공될 수 있다.

병원 관련 기기 기반의 대표적인 디지털헬스케어 서비스는 다음 같다.

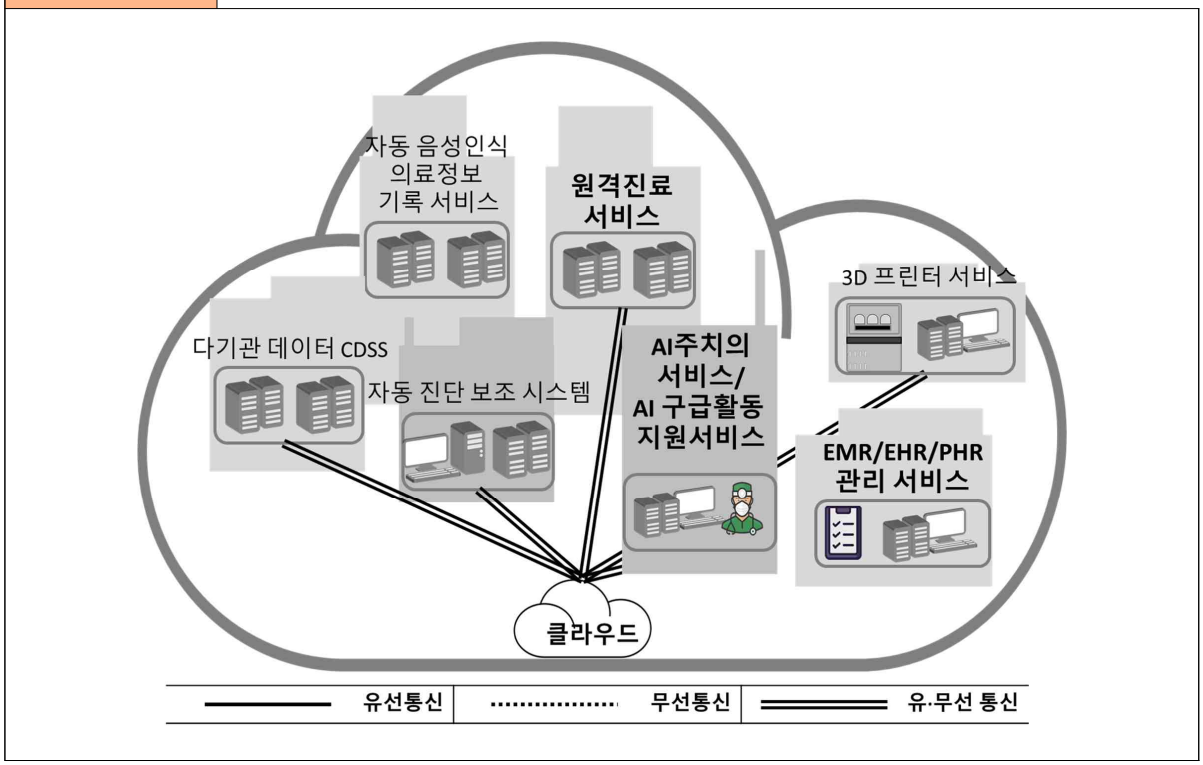
- ✓ 주치의 **원격진료 서비스** 및 다빈치 로봇 등을 이용한 **원격수술 서비스**
- ✓ 원격에서 만성질환 환자의 상태를 모니터링하는 **만성질환 관리 서비스**
- ✓ 병원 내부 또는 서비스 제공자와 연계한 **AI 기반의 의료정보 분석 서비스**
- ✓ 이송 중인 응급환자에 대한 실시간 모니터링을 통한 응급처치 매뉴얼 전송 등 **응급의료 서비스**

라. 서비스 제공자

디지털헬스케어 서비스를 제공하기 위한 구성요소 중 서비스 제공자는 홈, 이동형 진료소, 병원 도메인으로부터 전송된 개인의료정보, 개인건강정보, 환자 정보 등에 대한 저장 및 분석 서비스를 제공하는 도메인이다. 서비스 제공자는 의료정보기록 서비스, 다기관 데이터 CDSS, 인공지능 주치의 서비스, 자동진단 보조 시스템, 3D 프린트 서비스 등 개인의료정보 또는 개인건강정보에 대한 다양한 분석 서비스를 제공한다. 향후, 디지털헬스케어 영역의 확대와 기술의 고도화로 더 많은 양질의 서비스가 제공될 것으로 전망된다.

서비스 제공자 도메인에서 제공되는 대부분의 서비스는 다음 그림과 같이 데이터 기록 및 저장, 분석, 정보제공 등으로 구성되기 때문에 고성능 서버 및 웹서버, 데이터베이스 등의 장비로 구성된다. 또한 대용량의 데이터 처리 및 사용자 접속을 고려하여 클라우드 기반의 서비스를 제공할 수 있다.

그림 디지털헬스케어 서비스 구성요소 : 서비스 제공자



■ 서비스 제공자 관련 기기

서비스 제공자의 서비스 특성상 주로 웹서버 또는 데이터베이스 서버 등을 기반으로 개인의료정보 및 개인건강정보를 저장하고 관련 AI 알고리즘을 통해 분석한 정보를 제공(예, AI 주치의 등)하기 때문에 별도의 의료기기 보다는 고사양의 서버와 데이터베이스 시스템이 주축이 되고 있다. 네트워크 기술은 원격에서 접속 및 서비스가 가능해야 하기 때문에 광대역 통신망인 5G, LTE, 3G 망을 비롯하여 유선 Ethernet이 사용된다.

[표] 서비스 제공자 관련 디지털헬스케어 기기 유형

분류	관련 기기	운영체제	통신인터페이스	비고
의료정보 기록 서비스	PC, 서버, 웹서버	윈도우즈, 안드로이드, 리눅스, 유닉스 등	5G, 4G, 3G, Ethernet	의료정보제공, 다기관 데이터, AI 주치의 서비스는 물리적으로 병원, 댁내 시스템에 필수적으로 통합되지 않는 유동적 시스템으로 대개 서비스 제공 기업 서버를 통해 서비스가 제공됨
다기관 데이터 CDSS	PC, 서버, 웹서버	윈도우즈, 안드로이드, 리눅스, 유닉스 등	5G, 4G, 3G, Ethernet	
EMR/EHR/PHR 관리 서비스	PC, 서버, 웹서버	윈도우즈, 안드로이드, 리눅스, 유닉스 등	5G, 4G, 3G, Ethernet	
인공지능 주치의 서비스	PC, 서버, 웹서버	윈도우즈, 안드로이드, 리눅스, 유닉스 등	5G, 4G, 3G, Ethernet	
자동진단 보조 시스템	PC, 서버, 웹서버	윈도우즈, 안드로이드, 리눅스, 유닉스 등	5G, 4G, 3G, Ethernet	
3D 프린터 서비스	3D 프린터, PC, 서버 등	윈도우즈, 안드로이드, 리눅스, 펌웨어, RTOS	5G, 4G, 3G, Ethernet	의료용 3D 프린터는 단독 또는 PC와 연동하는 구조 (치과, 정형외과, 성형외과 등)

■ 서비스 제공자 관련 서비스

서비스 제공자 관련 서비스는 개인의료정보 및 개인건강정보 등 데이터 처리 기반의 서비스가 제공된다.

서비스 제공자 관련 기기 기반의 대표적인 디지털헬스케어 서비스는 다음 같다.

- ✓ 개인의료정보에 대한 빅데이터 분석 등을 통한 **AI 주치의 서비스 또는 진단 지원 서비스**
- ✓ 병원 등 진단 데이터를 기반으로 3D 프린팅 디자인, 의료기기 제작 등 **3D 프린팅 서비스**
- ✓ 개인건강정보 수집 및 분석을 통한 **개인 맞춤형 건강관리 서비스**

디지털헬스케어 보안위협

디지털헬스케어 기기는 홈, 이동형 진료소, 병원, 서비스 제공자 등 디지털헬스케어 서비스 구성요소별로 사용될 수 있으며, 수술 및 치료, 감시, 분석, 진단, 건강관리 등의 기능을 수행한다. 디지털헬스케어 기기 및 서비스 관련 보안위협을 인증 및 허가 유형, 암호 유형, 데이터 보안 및 안전한 통신 유형, 안전한 기기 관리 및 물리적 보호 유형으로 분류하고, 해당 보안위협에 대한 보안대책을 설명한다.

인증 및 허가 유형의 보안위협은 다음 표와 같다.

[표] 인증 및 허가 유형의 보안위협

보안위협	설명	관련 보안대책
인증우회	인가되지 않은 사용자가 디지털헬스케어 기기나 서비스에 접근할 수 있으며, 기기에 저장된 개인의료정보, 기기 설정파일 등 중요 데이터에 임의로 접근할 수 있음	사용자 인증, 접근통제
비인가된 기기 연결	디지털헬스케어 기기로의 비인가된 기기가 접근하거나, 비인가된 기기 또는 서버로의 개인의료정보 등을 전송할 수 있음	기기 인증, 접근통제,
과도한 권한 부여	과도하거나 불필요한 권한 부여로 공격자는 디지털헬스케어 기기가 허용하는 모든 기능과 접근이 제한된 개인의료정보 등에 접근할 수 있음	접근통제
연속된 인증시도	인가되지 않은 사용자가 연속적으로 인증을 시도하여 인가된 사용자 권한을 획득할 수 있음	접근통제
응급상황 대응 제한	응급상황 발생시 디지털헬스케어 기기 사용의 어려움으로 인해 적절한 응급처치를 하지 못할 수 있음	접근통제
동시접속에 따른 정책 일관성 오류	관리자 계정으로 동시 접속시 중요 기능 설정이 임의로 변경될 수 있음	접근통제
인증정보 노출 및 유추	비밀번호 등 인증정보가 하드코딩 또는 평문으로 저장되거나, 로그인을 위해 인증정보(예: 비밀번호) 입력 시 평문으로 출력되거나, 구체적인 인증 실패 사유에 대한 피드백으로 되어 인	안전한 비밀번호 메커니즘

보안위협	설명	관련 보안대책
	증정보가 노출되거나 유추될 수 있음	
취약한 비밀번호	비밀번호의 디폴트값 이용 등 관리가 미흡한 비밀번호를 획득하거나, 낮은 수준의 비밀번호 조합규칙이 적용된 경우 인가된 사용자로 위장할 수 있음	안전한 비밀번호 메커니즘
인증 결과 변조	인증 결과(예, 성공, 실패) 변조로 인증 기능이 우회될 수 있음	안전한 비밀번호 메커니즘

암호 유형의 보안위협은 다음 표와 같다.

[표] 암호 유형의 보안위협

보안위협	설명	관련 보안대책
취약한 암호화	취약한 암호 알고리즘, 불충분한 암호키, 유추 가능한 난수 사용으로 중요데이터를 적절하게 보호하지 못 할 수 있음	안전한 암호 알고리즘 사용, 안전한 암호키 관리, 안전한 난수 생성
취약한 암호 알고리즘	취약한 암호 알고리즘을 사용하는 트래픽을 분석하여 키 정보를 유추하거나 통신암호문의 내용을 알아낼 수 있음	안전한 암호 알고리즘 사용

데이터 보안 및 안전한 통신 유형의 보안위협은 다음 표와 같다.

[표] 데이터 보안 및 안전한 통신 유형의 보안위협

보안위협	설명	관련 보안대책
입력값 검증 부재	입력값에 대한 검증 부재로 디지털헬스케어 기기가 오작동할 수 있음	인터페이스 입력값 검증
신뢰할 수 없는 데이터 송수신	신뢰할 수 없는 데이터 송수신으로 디지털헬스케어 기기가 오작동을 유발하거나 악성코드를 전파할 수 있음	정보흐름통제
데이터 노출 및 변조	디지털헬스케어 기기에서 전송되거나 저장되는 개인의료정보, 기기 설정, 암호키 등 중요 데이터가 외부에 노출되어 악용되거나, 변조될 수 있음	저장데이터 보호, 전송데이터 보호, 개인정보보호, 보안통신
사용자 세션	정상적으로 세션 종료되지 않은 인가된 사용자 세션을 이용하	세션관리

보안위협	설명	관련 보안대책
탈취	여 권한을 탈취하거나, 기기별로 동일한 암호키 사용에 따라 세션을 탈취할 수 있음	

안전한 기기 관리 및 물리적 보호 유형의 보안위협은 다음 표와 같다.

[표] 안전한 기기 관리 및 물리적 보호 유형의 보안위협

보안위협	설명	관련 보안대책
안전하지 않은 업데이트	원하는 업데이트 파일이 다운로드 되지 않거나 출처를 알 수 없는 변조된 업데이트 파일이 실행될 수 있음	안전한 업데이트
업데이트 실패	업데이트 진행 중 오류발생으로 디지털헬스케어 기기가 정상적으로 동작하지 않을 수 있음	안전한 업데이트
무결성 오류	디지털헬스케어 기기의 주요 실행코드 및/또는 설정값의 임의 변조에 따라 오작동할 수 있음	안전한 서비스 제공, 인터페이스에 대한 물리적 보호
서비스 거부	디지털헬스케어 기기 기능의 오작동으로 디지털헬스케어 기기의 가용성이 제한될 수 있음	안전한 서비스 제공
악성행위	디지털헬스케거 기기 · 서비스의 목적에 맞지 않은 기능이 존재하여 악성 행위를 할 수 있음	안전한 서비스 제공, 보안취약점 탐지 및 대응
잔여정보 악용	암호연산, 인증, 데이터 전송을 위해 사용된 암호키, 비밀번호, 민감 데이터 등이 메모리에 남아 있어 악용될 수 있음	안전한 서비스 제공
중요 설정 임의 변경	디지털헬스케어 기기 및 서버에 대한 보안관리 부재로 중요 설정이 임의로 변경되어 안전하지 않은 서비스를 제공할 수 있음	기기 설정 관리
오류 대응	디지털헬스케어 기기 · 서비스에서 발생하는 오류, 악성행위 등에 대한 적절한 탐지 및 대응 부재로 안전하지 않은 서비스를 제공할 수 있음	감사기록, 보안취약점 탐지 및 대응
안전하지 않은 개발	디지털헬스케어 기기 · 서비스 설계 및 구현과정에서 잠재적인 보안취약점이 포함될 수 있으며, 시험과정에서 이에 대한 검증 및 대응이 부재하거나 적절하지 않을 수 있음	소프트웨어 개발보안, 보안취약점 탐지

보안위협	설명	관련 보안대책
		및 대응
취약한 운영체제	모바일 디바이스가 루팅/탈옥되었거나 취약한 운영체제 환경에서 앱 동작 시 앱의 보안 기능이 무력화되거나 우회될 수 있음	소프트웨어 개발보안
취약한 3rd party 모듈/라이브러리 사용	취약한 3rd party 모듈/라이브러리 사용으로 공격자가 해당 모듈/라이브러리를 호출할 수 있음	소프트웨어 개발보안
시스템 로그에 민감한 정보 기록	시스템 로그에 민감한 정보가 기록되어 공격자에 의해 해당 정보가 노출되어 악용될 수 있음	소프트웨어 개발보안
디버깅을 통한 중요정보 노출	디지털헬스케어 기기 · 서비스 릴리즈 및 배포 시 로그생성 및 디버깅 기능을 통해 중요정보가 유출되어 악용될 수 있음	소프트웨어 개발보안, 터페이스에 대한 물리적 보호
비인가된 물리적 접근	디지털헬스케어 기기에 비인가된 물리적 접속으로 기기를 임의로 변경할 수 있음	인터페이스에 대한 물리적 보호

디지털헬스케어 기기 보안요구사항

디지털헬스케어 관련 보안위협에 대응할 수 있는 디지털헬스케어 기기에 대한 보안요구사항은 다음과 같다.

(1) ‘인증 및 허가‘ 유형

보안항목	보안요구사항	
사용자 인증	1.1.1	디지털헬스케어 기기 운영 및 관리 기능 접근 시 사용자 인증을 해야 한다.
	1.1.2	민감 데이터에 접근 시 사용자 인증을 해야 한다.
	1.1.3	필요 시 암호학적으로 강력한 인증 기술이나 다중인증 방법 등을 사용해야 한다.
	1.1.4	디지털헬스케어 기기는 원격/무선 접근 시 사용자 인증 후 접근을 허용해야 한다.
기기 인증	1.2.1	디지털헬스케어 기기에 대한 기기인증을 통해 비인가된 접근을 통제해야 한다.
	1.2.2	디지털헬스케어 기기는 다른 기기나 서버와 중요정보 전송/수신 시 혹은 기기 제어를 위한 상호연결 수행 시 인증이 선행되어야 한다.
	1.2.3	디지털헬스케어 기기는 기본적으로 외부 통신이 “거부(deny)“되도록 설정되어 있어야 한다.
	1.2.4	디지털헬스케어 기기에 접속하는 다른 기기의 MAC 주소, IP 주소 등을 제한하여야 한다.
	1.2.5	디지털헬스케어 기기별로 고유 ID가 할당되어야 한다.
접근통제	1.3.1	디지털헬스케어 기기에 대한 비 인가된 접근을 제한해야 한다.
	1.3.2	디지털헬스케어 기기는 비밀번호, 암호키 등 중요데이터에 비인가된 접근을 제한해야 한다.
	1.3.3	디지털헬스케어 기기의 모든 사용자 계정에 대해 최소 권한의 원칙을 적용해야 한다.
	1.3.4	역할 기반 접근제어 시, 사용자 역할 및 기기 기능에 따른 권한을 부여할 수 있어야 한다.
	1.3.5	디지털헬스케어 기기는 반복된 인증시도에 대하여 인증 제한 등의 방법으로 대응해야 한다.
	1.3.6	비상시 디지털헬스케어 기기 접근을 허용하는 방법을 마련해야 한다.
	1.3.7	사용자 계정의 유효기간 만료 시 접근을 제한해야 한다.
	1.3.8	관리자 계정에 대해서는 동시 접속을 제한해야 한다.
	1.3.9	디지털헬스케어 기기는 비인가된 네트워크 접속을 제한 할 수 있어야 한다.
안전한 비밀번호 메커니즘	1.4.1	비밀번호는 하드코딩되지 않아야 한다.
	1.4.2	디지털헬스케어 기기는 비밀번호 입력 등 화면에 표시하는 경우 마스킹 처리를 해야 한다.
	1.4.3	비밀번호에 대한 안전한 저장 방법을 제공해야 한다.

보안항목	보안요구사항	
	1.4.4	비밀번호는 길이, 복잡도, 업데이트 주기를 고려하여 설정되어야 한다.
	1.4.5	디지털헬스케어 기기는 인증 실패메시지로 인증 실패 사유와 비밀번호를 유추할 수 있는 정보를 제공하지 않아야 한다.
	1.4.6	디지털헬스케어 기기는 제품 사용 초기에 인증정보를 설정하도록 요구하거나, 초기 인증정보를 변경하도록 요구해야 한다.
	1.4.7	디지털헬스케어 기기가 서버/클라이언트 형태로 구성된 경우, 비밀번호는 서버에서 검증해야 한다.

(2) ‘암호‘ 유형

보안항목	보안요구사항	
안전한 암호 알고리즘 사용	2.1.1	디지털헬스케어 기기에 적용되는 암호 알고리즘은 안전성이 검증된 알고리즘을 사용하여야 한다.
안전한 암호키 관리	2.2.1	암호키의 생명주기를 고려하여 안전하게 관리되어야 한다.
	2.2.2	암호 연산 목적에 따라 별도의 암호키를 사용하여야 한다.
안전한 난수 생성	2.3.1	난수 생성 시 난수성이 검증된 알고리즘을 이용해야 한다.

(3) ‘데이터 보안‘ 유형

보안항목	보안요구사항	
인터페이스 입력값 검증	3.1.1	디지털헬스케어 기기는 기능 동작에 사용되는 모든 입력값을 검증해야 한다.
	3.1.2	디지털헬스케어 기기는 통신인터페이스를 통해 유입되는 민감 데이터에 대해 무결성을 확인해야 한다.
	3.1.3	디지털헬스케어 기기가 서버/클라이언트 형태로 구성된 경우, 기기 동작을 위해 서버에서 유입되어 사용되는 모든 매개변수는 서버에서 검증해야 한다.
정보흐름통제	3.2.1	디지털헬스케어 기기의 구성 요소가 2개 이상인 경우, 구성요소로/에서 송·수신되는 정보 흐름을 통제할 수 있어야 한다.
저장데이터 보호	3.3.1	디지털헬스케어 기기에 의해 저장되는 모든 민감 데이터와 개인식별정보에 대한 기밀성과 무결성을 보장해야 한다.
	3.3.2	디지털헬스케어 기기에 저장되는 민감데이터에 대한 비인가된 접근을 차단해야 한다.
	3.3.3	디지털헬스케어 기기에 저장되는 암호키 등 안전 관련 데이터를 보호를 제공해야 한다.
전송데이터 보호	3.4.1	디지털헬스케어 기기에 의해 전송되는 모든 민감 데이터와 개인식별정보에 대한 기밀성과 무결성을 보장해야 한다.
	3.4.2	환자의 부상이나 사망을 초래할 수 있는 디지털헬스케어 기기 조작 명령어 등에 대한 전송데이터에 대한 기밀성 및 무결성을 보장해야 한다.
개인정보보호	3.5.1	디지털헬스케어 기기는 개인의료정보를 저장하지 않아야 한다.

(4) ‘안전한 통신‘ 유형

보안항목	보안요구사항	
세션 관리	4.1.1	디지털 헬스케어 기기에 동일 사용자가 다중 접속이 되지 않도록 제한해야 한다.
	4.1.2	디지털 헬스케어 기기는 세션 연결 후 일정 시간동안 미사용 또는 설정한 시간 경과 시 세션을 잠그거나 종료시켜야 한다.
	4.1.3	세션 종료 후 재접속하기 위해서는 재인증을 통해 접속을 허용해야 한다.
	4.1.4	디지털헬스케어 기기는 기기별로 유일한 암호화 통신키를 사용해야 한다.
보안 통신	4.2.1	디지털헬스케어 기기는 통신 대상 기기 및/또는 서버와 통신방식을 고려하여 안전한 통신을 제공해야 한다.

(5) ‘안전한 기기 관리‘ 유형

보안항목	보안요구사항	
안전한 업데이트	5.1.1	디지털헬스케어 기기는 업데이트 기능을 제공하여야 한다.
	5.1.2	업데이트 파일에 대한 버전, 배포자, 무결성을 검증할 수 있어야 한다.
	5.1.3	인가된 사용자에 의해 업데이트가 수행될 수 있도록 해야 한다.
	5.1.4	디지털헬스케어 기기는 롤백 기능을 제공하여야 한다.
안전한 서비스 제공	5.2.1	디지털헬스케어 기기의 안전 및 필수 성능을 보장하기 위해 실행코드 및 설정값 등에 대한 무결성을 보장해야 한다.
	5.2.2	디지털헬스케어 기기의 펌웨어 및 소프트웨어를 검증할 수 있어야 한다.
	5.2.3	디지털헬스케어 기기 서비스에 대한 가용성을 보장해야 한다.
	5.2.4	디지털헬스케어 기기의 불필요한 서비스는 제거되거나 비활성화 되어야 한다.
	5.2.5	디지털헬스케어 기기 파기 시 등 기기에 있는 모든 데이터를 완전 삭제할 수 있어야 한다.
기기 설정 관리	5.3.1	디지털헬스케어 기기의 설정을 위해서는 안전한 관리 수단을 제공해야 한다.
	5.3.2	디지털헬스케어 기기의 서버에 사용자 접근 차단을 설정할 수 있어야 한다.
감사기록	5.4.1	디지털헬스케어 기기는 중요 시스템 이벤트나 상태가 발생할 경우 자동으로 알람을 발생시켜야 한다.
	5.4.2	디지털헬스케어 기기는 주요 이벤트를 탐지하여 감시기록을 생성 및 검토 할 수 있는 기능을 제공해야 한다.
	5.4.3	감사기록을 안전하게 보호할 수 있어야 한다.
소프트웨어 개발 보안	5.5.1	디지털헬스케어 기기 개발과정에서 소스코드 보안 취약점이 존재하지 않도록 개발하여야 한다.
보안취약점 탐지 및 대응	5.6.1	악성코드로부터 보호할 수 있어야 한다.
	5.6.2	보안취약점 존재 여부를 확인하고 제거하여야 한다.

(6) ‘물리적 보호‘ 유형

보안항목	보안요구사항	
인터페이스에 대한 물리적 보호	6.1.1	디지털헬스케어 기기의 불필요한 인터페이스는 물리적으로 접근을 제한해야 한다.
	6.1.2	디지털헬스케어 기기에 대한 비인가된 물리적 접근을 탐지하고, 대응기능을 제공해야 한다.

디지털헬스케어 서비스 보안요구사항

디지털헬스케어 서비스를 제공하는 모바일 앱, 웹 서비스, 디지털헬스케어 서비스 인프라를 대상으로 준수해야 할 보안요구사항은 다음과 같다.

가. 디지털헬스케어 서비스 모바일 앱 보안요구사항

(1) ‘인증‘ 유형

보안항목	보안요구사항	
사용자 인증	01	처음 제품을 사용할 때 인증정보를 설정하도록 요구하거나, 초기 인증정보를 변경하도록 요구해야 한다.
	02	관리서비스 및 중요정보 접근 시 사용자 신원을 검증하기 위해 식별 및 인증이 선행되어야 한다.
	03	잘못된 인증정보를 통한 반복된 인증 시도를 제한해야 한다.
	04	제품에서 사용되는 사용자 계정 및 권한에 대한 관리 기능을 제공해야 한다.
	05	길이, 주기, 복잡성을 고려하여 안전한 비밀번호로 설정되도록 해야 한다.
인증 정보의 안전한 사용	01	인증정보는 하드코딩 되거나 평문으로 저장되지 않아야 한다.
	02	인증을 위한 비밀번호 입력 시 화면에 노출되지 않도록 마스킹 처리해야 한다.
	03	인증 실패 시 실패 사유에 대한 피드백 정보를 제공하지 않아야 한다.
제품 인증	01	제품 간 중요정보 전송 시 혹은 제품 제어를 위한 상호연결 수행 시 상호인증이 선행되어야 한다.

(2) ‘암호‘ 유형

보안항목	보안요구사항	
안전한 암호 알고리즘 사용	01	중요정보 전송 또는 저장 시 안전한 암호 알고리즘을 사용해야 한다.

(3) ‘데이터 보호‘ 유형

보안항목	보안요구사항	
전송데이터 보호	01	제품 간 전송되는 중요정보는 암호화해야 한다.
	02	알려진 프로토콜 기반으로 통신채널 생성 시 안전한 보안 모드를 사용해야 한다.

보안항목	보안요구사항	
저장데이터 보호	01	제품에 저장되는 중요정보는 암호화해야 한다.
정보흐름 통제	01	허가되지 않은 네트워크 트래픽 차단 기능을 제공해야 한다.
안전한 세션관리	01	세션 연결 후 일정 시간동안 미사용 시, 세션을 잠그거나 종료시켜야 한다.
개인정보 보호	01	제품에서 처리하는 개인정보는 비식별화 조치되어야 한다.

(4) ‘플랫폼 보호‘ 유형

보안항목	시험 기준	
소프트웨어 보안	01	보안약점이 존재하지 않도록 시큐어코딩을 적용해야 한다.
	02	알려진 보안취약점 존재여부를 확인하고 제거하여야 한다.
소프트웨어 보안	01	소스코드 분석 방지를 위해 난독화를 적용해야 한다.
	02	주요 설정 값 및 실행코드에 대한 무결성 검증 기능을 지원해야 한다.
안전한 업데이트	01	업데이트 수행 전 인가된 사용자 여부를 확인해야 한다.
	02	업데이트 수행 전 무결성을 검사해야 한다.
보안 관리	01	불필요한 서비스는 제거하거나 비활성화해야 한다.
	02	원격관리는 신뢰할 수 있는 환경에서 수행되어야 한다.
	03	3rd party 라이브러리 사용 시 최신 보안패치가 적용된 버전을 사용해야 한다.
감사기록	01	보안과 관련된 이벤트는 감사기록을 생성해야 한다.
	02	감사기록에 대한 보호 기능을 제공해야 한다.

나. 디지털헬스케어 서비스 웹 서비스 보안요구사항

(1) '입력값 검증' 유형

보안항목	보안요구사항	
SQL 인젝션	01	입력값 검증을 통해 DB 정보 유출 및 타 사용자 권한이 유출되지 않도록 해야 한다.
크로스사이트 스크립팅	02	특수문자 필터링 등을 통해 악의적인 스크립트가 실행되어 타인 계정 탈취 등이 발생하지 않도록 차단해야 한다.
파일 업로드	03	파일 업로드 구간에서 악성코드가 삽입된 실행파일이 업로드 되지 않도록 차단해야 한다.
경로 추적 및 파일 다운로드	04	권한이 없는 사용자가 중요파일 및 시스템 파일을 열람할 수 없도록 해야 한다.

(2) '인증관리' 유형

보안항목	보안요구사항	
불충분한 인증 및 인가	01	관리 또는 개별 메뉴 접근 시 사용자 신원을 검증하기 위해 식별 및 인증이 선행되어야 한다.
계정 최소화의 원칙	02	모든 사용자 계정에 대해 최소 권한의 원칙을 적용해야 한다.
관리자 페이지 접근 차단	03	관리자 계정에 대해서는 동시 접속 제한 및 접근 기록을 남겨두어야 한다.

(3) '암호관리' 유형

보안항목	시험 기준	
데이터 평문전송	01	제품 및 서비스 간 전송되는 중요정보는 암호화해야 한다.
취약한 패스워드 복구	02	길이, 주기, 복잡성을 고려하여 안전한 비밀번호를 설정되도록 해야 한다

(4) '보안관리' 유형

보안항목	시험 기준	
디렉터리 인덱싱	01	웹 어플리케이션의 파일 위치 및 정보가 노출되지 않도록 설정해야 한다.
정보누출	02	서버 정보, 디폴트로 설정된 에러 페이지 등 웹 페이지의 민감 정보가 노출되지 않도록 설정해야 한다.

다. 디지털헬스케어 서비스 인프라 보안요구사항

(1) ‘서버 보안‘ 유형

보안항목	보안요구사항	
계정관리	01	패스워드 정책 - 패스워드 복잡성 설정 - 패스워드 최소 길이 설정 - 패스워드 최대 사용기간 설정 - 패스워드 최소 사용기간 설정
	02	불필요한 계정 관리
	03	Session Timeout 설정
파일 및 디렉터리 관리	01	Root 홈, 패스 디렉터리 권한 및 패스 설정
	02	파일 소유자 및 권한 설정 - /etc/passwd - /etc/shadow - /etc/hosts - /etc/syslog.conf
	03	사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정
	04	접속 IP 및 포트 제한
서비스 관리	01	Anonymous FTP 비활성화
	02	Dos 공격에 취약한 서비스 비활성화
	03	DNS Zone Transfer 설정
	04	디렉터리 리스팅 제거
	05	불필요한 파일 제거
	06	파일 업로드 및 다운로드 제한
패치 관리	01	최신 보안패치 및 벤더 권고사항 적용
	02	백신 프로그램 업데이트
로그 관리	01	로그의 정기적 검토 및 보고
	02	정책에 따른 시스템 로깅 설정

(2) ‘WEB 서버 보안‘ 유형

보안항목	보안요구사항	
접근제어	01	프로세스 권한 제한
	02	디렉터리 쓰기 권한 설정
보안 설정	01	불필요한 파일 제거
	02	응답 메시지 헤더 정보 숨기기
	03	MultiViews 옵션 비활성화
	04	HTTP Method 제한
	05	파일 업로드 및 다운로드 제한
	06	로그 설정 관리
보안 패치	01	최신 패치 적용

(3) ‘DBMS 보안‘ 유형

보안항목	보안요구사항	
계정 관리	01	기본 계정의 패스워드, 정책 등을 변경하여 사용
	02	패스워드의 사용기간 및 복잡도 기관 정책에 맞도록 설정
	03	데이터베이스 관리자 권한을 꼭 필요한 계정 및 그룹에 허용
접근 관리	01	원격에서 DB서버로의 접속 제한
	02	DBA이외의 인가되지 않은 사용자 시스템 테이블 접근 제한 설정
	03	일정 횟수의 로그인 실패 시 잠금 정책 설정
옵션 관리	01	응용 프로그램 또는 DBA 계정의 Role이 Public으로 설정되지 않도록 조정
패치 관리	01	최신 패치 적용 점검
	02	데이터베이스의 접근, 변경, 삭제 등의, 감사기록이 감사기록 정책에 적합하도록 설정
로그 관리	01	Audit Table은 데이터베이스 관리자 계정에 속해 있도록 설정