병원정보시스템
보안가이드라인

국가정보원 NSR 국가보안기술연구소

병원정보시스템
보안가이드라인

{ 문서이력 }

개정일	버전	내역	비고
2025.04.03.	1.0	신규 제정	

목 차

제1장 개요

병원정보시스템(Hospital Information System, HIS)은 병원의 진료와 운영 전반에 필요한 정보를 체계적으로 관리하고 지원하는 통합 시스템으로, 다양한 구성 요소를 포함하고 있다. 의료진은 의료정보시스템을 통해 환자의 상태를 파악하고 진단과 치료 계획을 세우는 데 필요한 정보를 관리하며, 의료기기를 활용하여 환자 진료와 치료를 수행한다. 경영진은 경영정보시스템을 통해 운영 데이터를 분석해 병원 운영의 효율성을 극대화한다. 원무(행정) 직원은 원무(행정)시스템을 통해 환자 등록, 수납, 입·퇴원 관리, 병상 관리, 행정 문서 발급 등의 업무를 수행한다. 환자와 보호자는 환자포털을 통해 진료 예약 및 병원으로부터 필요한 정보를 주고받을 수 있다. 또한, 병원 구성원은 기타 외부 연계 시스템을 통해 의료기관, 연구소, 국민건강보험공단, 건강보험심사평가원 등과 정보를 공유하여 병원 내외부의 협력을 지원한다. 이러한 구성 요소들은 통합적으로 작동하며 병원의 진료와 운영을 최적화하는 데 이바지한다.

최근 병원정보시스템에 IT 기술이 다수 도입되어 의료 데이터 관리의 효율성과 서비스의 질이 크게 향상되고 있다. 그러나 이러한 기술 도입으로 인해 병원정보시스템 운영 환경이 복잡해지면서 보안 위협 또한 증가하고 있다. 병원정보시스템은 민감한 정보를 다루고 있어 침해 사고 발생 시 개인정보 유출뿐만 아니라 시스템 마비로 인한 생명 위협까지 초래할 수 있으므로, 철저한 보안이 필요하다.

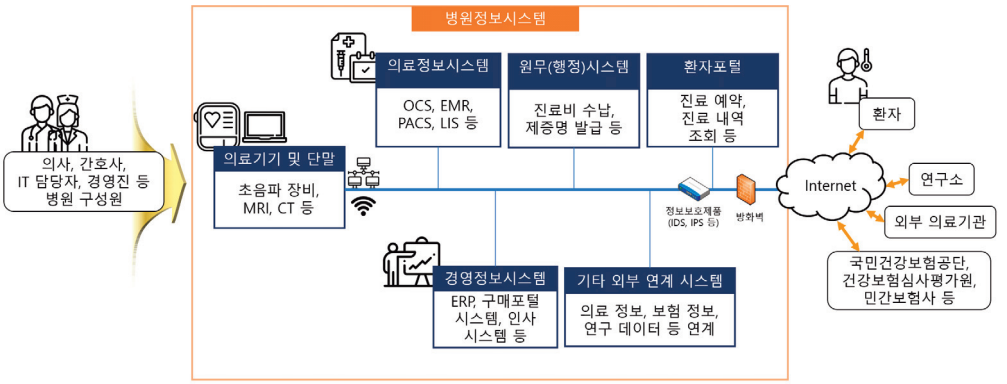
따라서 본 가이드라인은 병원정보시스템 도입 및 운영 시 보안 위협을 효과적으로 관리하고, 데이터와 시스템의 안전성을 보장하기 위한 보안대책을 제시한다. 이를 통해 병원정보시스템의 안전한 운영과 보안 위협 대응을 위한 기반을 마련하고자 한다.

※ 「병원정보시스템 보안가이드라인」은 주요정보통신기반시설(병원정보시스템)을 보유 중인 기관(병원)에서 준수해야 하는 기본 보안 수칙을 명시하였으며, 해당 기관은 가이드라인을 참고하여 보안 업무를 수행하시기 바랍니다.

※ 주요정보통신기반시설을 보유하고 있지 않은 병원 등 의료기관도 필요시 해당 가이드라인을 참고하여 보안 업무를 수행하시기 바랍니다.

제1절 병원정보시스템 개요 및 보안 필요성

가. 병원정보시스템



[그림 1-1] 병원정보시스템 개요

병원정보시스템은 실제 현장에서 다양한 형태로 운영되지만, 일반적으로 위의 그림과 같은 구조로 도식화할 수 있다. 병원에 따라 “의료정보시스템”을 “진료지원시스템”, “경영정보시스템”을 “경영지원시스템” 등으로 표현하기도 한다. 의사, 간호사, 경영진, IT 담당자, 원무(행정) 직원, 환자 등 각 사용자는 아래와 같은 업무를 수행하며, 병원정보시스템은 이를 지원한다.

○ 의사

- 의료정보시스템의 OCS[1](Order Communication System)를 통해 간호사, 약국, 영상검사실, 기능검사실 등에 오더를 전달하고 그 결과를 확인하며, EMR[2](Electronic Medical Record)을 활용해 초·재진 기록, 입원기록 등의 진료내역을 기록

1) OCS : 처방 전달 시스템
2) EMR : 전자 의무 기록

- 의료정보시스템의 PACS[3](Picture Archiving and Communication System)를 통해 초음파 장비, MRI[4], CT[5] 등의 영상 검사 결과를 통합하여 활용하며, LIS[6](Laboratory Information System)를 통해 검사실에서 나온 결과를 확인하여 진단 및 치료 방향 결정

- 기타 외부 연계 시스템을 통해 외부 의료기관이나 연구소와의 협업을 위해 데이터 공유

○ 간호사

- EMR[7]에 환자의 투약 현황, 상태 변화 등을 기록하며, 의료기기 데이터를 확인하여 업무 수행
- 환자 모니터링 장치 등의 의료기기에서 수집된 데이터를 확인하여 의사와 협력
- 환자 및 보호자에게 검사 일정, 결과 등 관련 정보 전달
- 환자 기록을 기반으로 병동 내 다른 팀 또는 기타 외부 연계 시스템에 필요한 데이터 공유

○ 경영진

- 경영정보시스템의 ERP[8](Enterprise Resource Planning), 인사 시스템을 통해 병원의 운영 상태(재정, 인사)를 관리하고 병원 서비스 수준 개선을 위한 데이터 분석
- 경영정보시스템의 구매포털 시스템을 통해 의료기기의 사용 빈도 및 상태를 확인하고 업그레이드나 유지보수 계획 수립

3) PACS : 의료 영상 저장·전송 시스템
4) MRI : 자기 공명 영상
5) CT : 컴퓨터 단층 촬영
6) LIS : 임상병리 정보시스템
7) EMR : 전자 의무 기록
8) ERP : 전사적 자원관리

- 병원의 운영 데이터를 기반으로 외부 보험사, 정부 기관 등과 협력

○ IT 담당자

- 의료기기, 의료정보시스템, 경영정보시스템, 원무(행정)시스템, 환자포털, 기타 외부 연계 시스템 간의 데이터 통합 및 안정적 운영 보장
- 환자포털, 기타 외부 연계 시스템 운영 시 안전한 통신을 사용하도록 권한 관리 수행
- 의료기기와 의료정보시스템 간의 네트워크 연결 상태를 점검하고, 장애 발생 시 신속히 복구
- 환자포털 및 내부 시스템의 이상 활동을 탐지하고, 데이터를 보호하기 위한 모니터링 수행

○ 원무(행정) 직원

- 원무(행정)시스템을 통해 환자 등록 및 접수, 입·퇴원 및 병상 관리
- 원무(행정)시스템을 통해 진료비 청구 및 수납, 행정 문서 및 증명서 발급
- 원무(행정)시스템을 통해 PACS 등의 검사 결과 환자에게 제공

○ 환자

- 환자포털을 통해 진료 예약, 변경, 취소가 가능하며, 진료 일정과 과거 기록을 확인
- 환자포털을 통해 상담 요청 및 병원 서비스 관련 정보 활용

나. 병원정보시스템 대상 보안 위협 사례 및 보안가이드라인 필요성

[표 1-1]과 같이 병원정보시스템을 대상으로 한 보안 위협이 최근 급격히 증가하고 있다. 병원정보시스템은 환자의 민감한 개인정보와 의료 데이터를 처리하는 핵심 시스템으로, 보안 사고가 발생할 경우 개인정보 유출뿐만 아니라 환자의 생명과 직결되는 치명적인 결과를 초래할 수 있다. 이러한 위협의 증가는 병원 운영의 안정성과 신뢰성에 영향을 끼칠 수 있으며, 이에 대한 적절한 보안대책이 마련되지 않으면 효과적으로 대응하기 어렵다.

[표 1-1] 병원정보시스템 대상 보안 위협 사례

위협 요인	관련 사례
악성코드 감염	• 프랑스 대형병원(CHSF) 랜섬웨어 사고(`22.08) – 랜섬웨어 감염에 따른 전산시스템 마비 – 환자 개인정보 및 의료정보 공개 유출
사이버 공격	• 미국 세인트 마가렛 헬스 사이버 공격으로 폐업 (`21.02) – 사이버 공격으로 인한 병원 시스템 중지 – 결제 시스템 문제 발생으로 인한 의료비 청구 오류로 경영 타격 발생
데이터 및 개인정보 유출	• 국내 상급종합병원 계정정보 및 의료종사자 정보 다크웹 노출 (`23.05) – 종합병원 41곳의 계정정보(관리자 계정 포함)의 다크웹 노출 확인 – 의료종사자의 근로계약서 등 민감정보를 포함한 자료까지 유출됨을 확인
	• 국내 상급종합병원 북한 해킹 공격으로 83만 명 개인정보 유출 (`21.05) – 국내 상급종합병원 서버의 취약점을 악용하여 내부망에 해커 침입 – 환자 개인정보 및 전·현직 직원 정보 유출

따라서 본 가이드라인에서는 모든 환자 및 병원 구성원이 안심하고 신뢰할 수 있는 병원정보시스템을 구축하고 운영하기 위한 보안대책을 제시한다. 보안대책을 통해 위협으로부터 환자 데이터를 보호하고 병원 서비스의 연속성을 확보함으로써 사용자가 신뢰할 수 있는 환경이 조성될 것이라 기대한다.

제2절 보안대책 구성 및 활용

본 가이드라인은 병원정보시스템 운영 시 발생할 수 있는 정보보안 사고를 방지하기 위하여 보안대책을 제시하고 있다. 보안대책 구성은 아래와 같다.

[표 1-2] 병원정보시스템 보안대책 구성

보안대책	세부 보안대책
제2장 네트워크 보안대책	
제1절 네트워크 공통 보안대책	가. 네트워크 분리 및 접근제어
제2절 연계 구간별 네트워크 보안대책	가. 시스템 내 연계 구간
	나. 시스템 간 연계 구간
	다. 인터넷 연계 구간
	라. 의료기기 및 단말기 연계 구간
제3절 상세 네트워크 보안대책	가. DMZ 구간 구성
	나. 망연계 솔루션
	다. 네트워크 장비에 대한 안전한 설정
제3장 시스템 및 애플리케이션 보안대책	
제1절 시스템 보안대책	가. 권한 관리
	나. 접근통제
	다. 계정 관리
	라. 사용자 인증
	마. 불필요 포트 및 서비스 제거
	바. 시스템 업데이트 및 보안패치
	사. 악성코드 통제
	아. 정보 유출 통제
	자. 노트북 및 모바일 기기 관리
	차. 이동식 저장매체 보안
제2절 애플리케이션 보안대책	가. SDLC 및 SPDL 적용
	나. 웹·애플리케이션 취약점 점검
	다. 암호화 정책

보안대책	세부 보안대책
제3절 의료기기 및 의료정보 보안대책	가. 의료기기 보안성 검토
	나. 의료기기 보안대책
	다. 의료기기 통신 보안
	라. 의료정보의 저장·연계
	마. 제3자 서비스 수준 계약
제4장 관리적 보안대책	
제1절 정보보안 정책 및 조직	가. 정보보안 정책 수립
	나. 경영진의 책임
	다. 정보보안 조직의 역할 및 책임
	라. 인적 보안
제2절 자산 관리	가. 정보자산 관리
	나. 취약점 점검 및 위험평가
	다. 보안대책 수립
제3절 운영 관리	가. 원격 접속 통제
	나. 외부 유지보수 관리
	다. 외주 개발 관리 감독
	라. 로깅과 모니터링
	마. 백업·복구 및 연속성 관리
제4절 물리 보안	가. 보호구역 지정
	나. 재난·재해 대비 물리적 보호대책 수립
	다. 출입 통제
	라. 작업 통제
제5절 환자 개인정보보호	가. 개인정보 개요
	나. 개인정보의 수집·이용
	다. 개인정보의 제3자 제공
	라. 개인정보 처리 업무위탁
	마. 영업의 양도
	바. 개인정보파일의 등록(공공의료기관)

보안대책	세부 보안대책
	사. 개인정보의 파기
	아. 개인정보 처리방침의 수립 및 공개
	자. 개인정보 보호 책임자 지정
	차. 정보주체의 권익보호
	카. 피해 구제 방법

먼저 제2장은 네트워크 보안대책을 제시한다. 병원정보시스템은 진료 및 운영을 위하여 다양한 시스템이 연계되어 있다. 각 연계 구간별 특징을 고려하여 적용해야 할 보안대책을 제시한다.

제3장은 시스템 및 애플리케이션 보안대책을 제시한다. 환자의 개인정보 및 의료 기록과 같은 민감한 데이터를 다루는 병원정보시스템을 대상으로 데이터 무결성과 시스템 안정성을 유지하기 위한 보안대책을 제시한다.

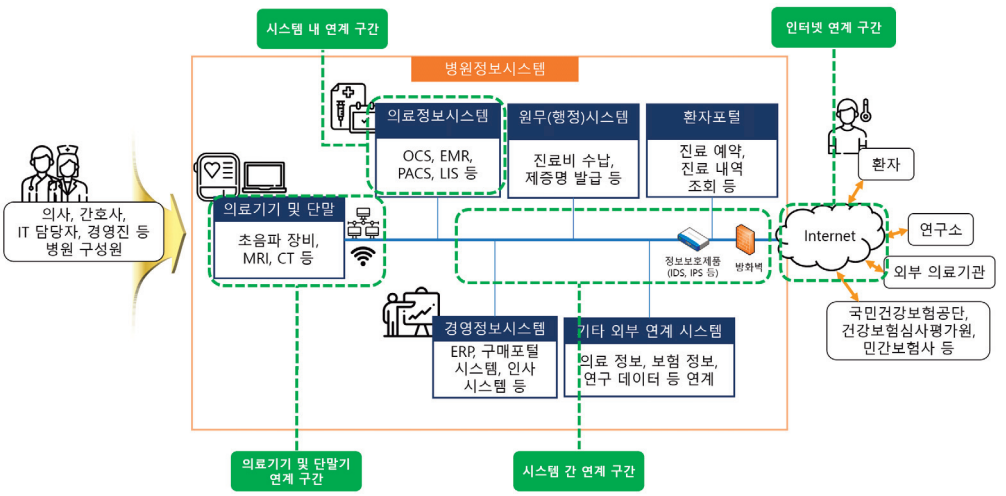
제4장은 관리적 보안대책을 제시한다. 의료 서비스는 중단 없이 제공되어야 하며, 보안 위협으로 인해 운영이 중단되면 환자의 생명과 직결될 수 있다. 따라서 정보보안 정책 및 조직, 자산 관리, 운영 관리, 물리 보안, 개인정보 보호 등의 관리적 보안대책을 제시하여 병원정보시스템의 안전성과 연속성을 보장한다.

병원정보시스템은 복잡하고 병원 규모와 제공하는 서비스가 다양하여 개별 의료기관에서 보안대책 수립에 어려움이 있다. 이를 해결하기 위해 본 가이드라인은 병원정보시스템 운영 및 구축 기관에 실질적인 보안대책 마련과 적용을 지원하고자 한다.

※ 본 문서는 병원정보시스템에 필요한 사이버보안과 관련한 중요 사항들에 대해서 다루고 있다. 본 문서와 관련된 세부 보안대책들은 관련 지침 가이드를 따라야 한다.

제2장 네트워크 보안대책

병원정보시스템은 의료정보시스템, 경영정보시스템, 원무(행정)시스템, 환자포털, 기타 외부 연계 시스템, 의료기기, 단말 등이 네트워크로 연결되어 통합적으로 운영된다. 본 장에서는 일반적인 병원정보시스템의 네트워크 구성 및 연계 유형을 정리하고 이를 기준으로 네트워크 보안대책을 제시한다. 병원정보시스템 운영기관마다 네트워크 구성이 다를 수 있으므로 각 병원의 운영 현황에 맞게 네트워크 보안대책을 적용하여야 한다.



[그림 2-1] 병원정보시스템 네트워크 구성 및 연계 유형 예시

병원마다 병원정보시스템에 연계된 시스템과 외부 기관은 다를 수 있지만, 일반적으로는 [그림 2-1]과 같은 네트워크 구성 및 연계 구간을 가진다. 병원정보시스템 내에는 의료정보시스템, 경영정보시스템, 원무(행정)시스템, 환자포털, 기타 외부 연계 시스템 등이 있으며, 각 시스템 내부에는 해당 시스템을 구성하는 하위 시스템이 존재한다. 예를 들어, 의료정보시스템 내에는 OCS, EMR, PACS, LIS 등의 시스템이 포함되어 있으며, 이들은 시스템 내에서 상호 연계되어 동작한다. 또한 의료정보시스템, 경영정보시스템, 원무(행정)시스템, 환자포털, 기타 외부 연계 시스템은 시스템 간 상호 연계되어

있으며, 환자포털과 기타 외부 연계 시스템은 외부 환자 및 다른 기관에 서비스를 제공하기 위해 인터넷에도 연결된다. 병원 구성원이 사용하는 의료기기와 단말기는 유무선 네트워크를 통해 타 시스템과 연결된다. 이를 바탕으로 연계 구간을 정리하면 아래와 같다.

- 시스템 내 연계 구간
- 시스템 간 연계 구간
- 인터넷 연계 구간
- 의료기기 및 단말기 연계 구간

이러한 특징을 바탕으로 본 장에서는 병원정보시스템의 네트워크 보안대책을 제시한다. 먼저 제1절에서는 병원정보시스템 통합망에 적용 가능한 네트워크 공통 보안대책에 대해 설명한다.

제2절에서는 연계 구간별 네트워크 보안대책에 대해 설명한다. 시스템 내, 시스템 간, 인터넷, 의료기기 및 단말기 연계 구간별로 필요한 보안대책을 제시한다.

마지막으로 제3절에서는 제2절에서 제시한 보안대책에 대한 세부 사항을 기술한다. DMZ 구간 구성, 망연계 솔루션, 네트워크 장비 보안정책 설정 등이 포함된다.

제1절 네트워크 공통 보안대책

본 절에서는 연계 구간 모두에 공통으로 적용 가능한 네트워크 보안대책을 제시한다.

가. 네트워크 분리 및 접근제어

○ 네트워크 분리

- 병원정보시스템의 네트워크를 하나의 네트워크로 구성하게 되면 접근제어와 통제가 어려우므로 사용 목적, 업무, 관리 범위 등을 고려하여 분리하여 구성
  - 구축 예산, 운영 효율성 등의 이유로 단일 네트워크로 구성한 경우에는 VLAN과 IP 대역 분리를 통한 네트워크 세분화 적용
- 운영하는 시스템·서비스·DB 등이 대규모인 경우 별도의 IP 대역을 할당하여 계층적으로 구성하고 각 계층별로 서브넷 클래스를 할당하여 IP 주소를 그룹화

○ 네트워크 접근제어

- 네트워크 간 데이터 전달이 반드시 필요한 경우에 한해서만 통신을 허용
- 라우터, 스위치 등의 네트워크 장비에서 필요한 통신만 가능하도록 ACL(Access Control List)을 설정하고, 진료 및 업무상 필요한 네트워크 간 통신을 제외하고는 원칙적으로 통신을 제한
- 각 네트워크 연결 접점에는 침입차단시스템(방화벽) 등의 정보보호 시스템을 구성하고, 제한된 시스템 및 서비스에 한정하여 통신을 허용
- 중요한 시스템들의 경우, 지정된 IP와 포트로 특정한 시스템과 서비스에 대해서만 통신을 허용

제2절 연계 구간별 네트워크 보안대책

가. 시스템 내 연계 구간

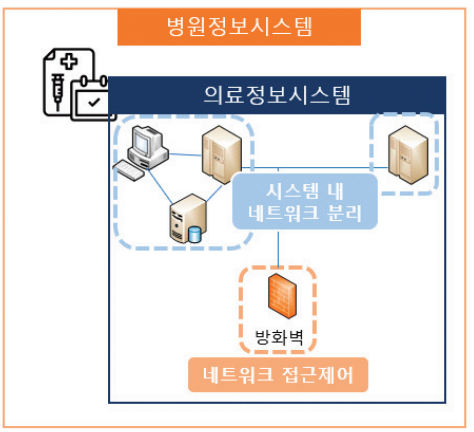
○ 의료정보시스템, 경영정보시스템 등 각 시스템 내 네트워크 연계

※ 예를 들어 의료정보시스템 내에서 PACS를 통해 CT, MRI와 같은 영상 데이터를 OCS/EMR로 연계

○ 적용 가능한 네트워크 보안대책

- 네트워크 분리를 통해 관리적 효율성 및 보안성 향상
- 접근제어 적용으로 인가된 사용자만 접근 허용
- 침입차단시스템(방화벽) 등의 정보보호시스템 도입

※ 안전하고 적합한 네트워크 보안 정책 설정



[그림 2-2] 시스템 내 연계 구간 보안대책

나. 시스템 간 연계 구간

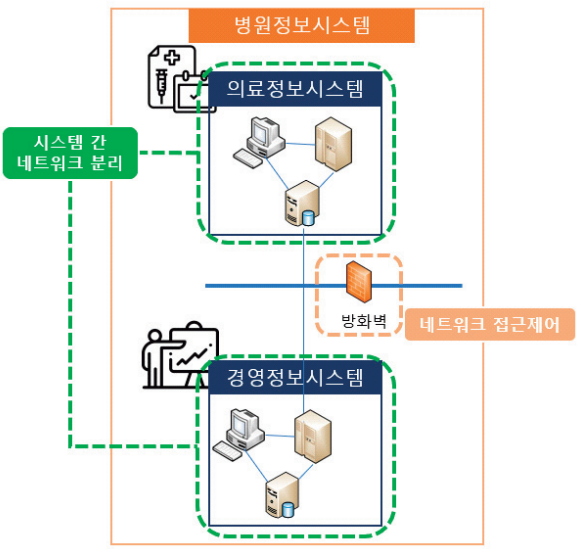
○ 의료정보시스템, 경영정보시스템 등 각 시스템 간 네트워크 연계

※ 예를 들어 의료정보시스템에 입력된 정보를 경영정보시스템으로 전송하여 병원 운영을 위한 데이터로 활용

○ 적용 가능한 네트워크 보안대책

- 네트워크 분리를 통해 관리적 효율성 및 보안성 향상
- 접근제어 적용으로 인가된 사용자만 접근 허용
- 침입차단시스템(방화벽) 등의 정보보호시스템 도입

※안전하고 적합한 네트워크 보안 정책 설정



[그림 2-3] 시스템 간 연계 구간 보안대책

다. 인터넷 연계 구간

○ 병원정보시스템을 통해 환자 및 외부 유관기관에 서비스를 제공할 목적으로 인터넷으로 통신

※ 예를 들어 환자가 병원정보시스템의 환자포털을 통해 진료 예약을 수행하고 진료 내역 조회 등을 수행

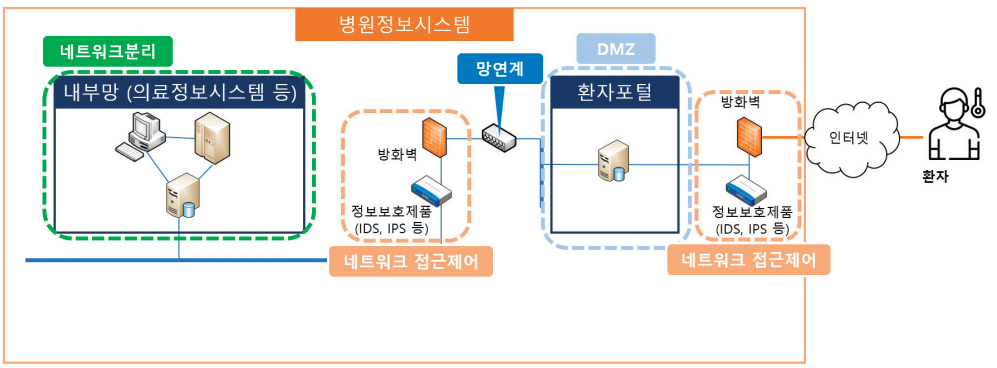
○ 적용 가능한 네트워크 보안대책

- 네트워크 분리를 통해 관리적 효율성 및 보안성 향상
- 접근제어 적용으로 인가된 사용자만 접근 허용

- 침입차단시스템(방화벽), IDS/IPS 등의 정보보호시스템 도입

※ 안전하고 적합한 네트워크 보안 정책 설정

- 전체 네트워크를 직접 연계하지 않고 별도 시스템(환자포털 등)을 DMZ 내에 두도록 구성
- 보안성 유지를 위해 DB는 DMZ 구간에 구성하지 않음
- 검증된 망연계 솔루션을 적용하여 데이터의 보안성 및 기밀성을 향상



[그림 2-4] 인터넷 연계 구간 보안대책

라. 의료기기 및 단말기 연계 구간

○ 의료기기 및 단말기를 의료정보시스템과 연결하여 데이터를 송·수신하기 위해 시리얼 통신, 유/무선 통신, 블루투스 등을 이용

※ MRI, CT, X-ray 등에서 생성된 이미지를 의료정보시스템의 PACS로 전송하여 의료진이 해당 데이터를 활용

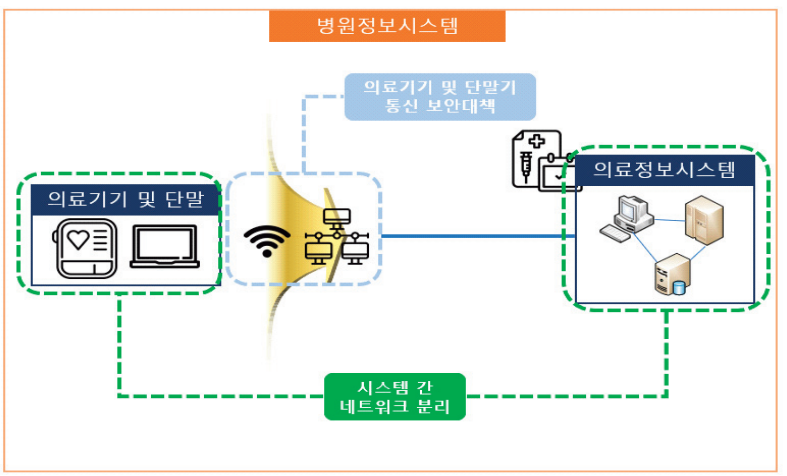
○ 적용 가능한 네트워크 보안대책

- 의료기기 데이터 전송 시 암호화 방안을 마련
- TLS[9](Transport Layer Security) 기반으로 암호화를 지원하는 DICOM-TLS[10](Digital Imaging and Communications in

9) TLS : 전송 계층 보안
10) DICOM-TLS : 의료-전송 계층 보안의 디지털 이미징 및 통신

Medicine-Transport Layer Security) 프로토콜을 지원하는 의료기기의 경우, 해당 기능을 활성화하여 데이터 전송 시 암호화 적용

- DICOM을 지원하지 않는 의료기기의 경우
  - 다수의 의료 보안 게이트웨이가 채택하고 있는 윈도우 운영체제에서 기본적으로 지원하는 VPN[11](Virtual Private Network) 기능 등 활용
- Wi-Fi 사용 시
  - SSID를 숨기고 관리자 비밀번호를 길고 복잡하게 설정
  - WPA3 프로토콜 사용
  - 주기적인 펌웨어 업데이트를 통해 보안 취약점 패치
- 블루투스 사용 시
  - 인증된 장치만 연결할 수 있도록 설정 및 강력한 PIN 코드 사용
  - 블루투스를 사용하지 않는 경우 블루투스 기능 비활성화 및 페어링 기록 삭제
  - 주기적인 펌웨어 업데이트를 통해 보안 취약점 패치



[그림 2-5] 의료기기 및 단말기 연계 구간 보안대책

11) VPN : 가상 사설망

제3절 상세 네트워크 보안대책

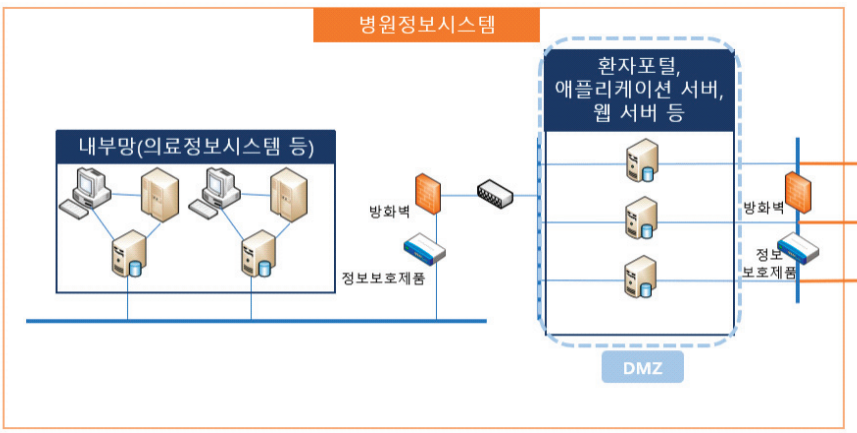
가. DMZ[12] 구간 구성

○ 환자 및 유관기관에 서비스를 제공하기 위해 인터넷 연계를 위한 시스템을 분리하여 DMZ 구성

- 외부 서비스를 위한 시스템들은 병원정보시스템이 구성된 네트워크에서 분리하여 별도의 DMZ를 구성하여 운영
- 서로 다른 기관과 연계하거나, 보안 중요도에 따라 물리적·관리적으로 다른 네트워크로 구성해야 하는 경우, DMZ 내에서도 분리하여 운영

○ DMZ 구간과 병원정보시스템 사이는 접근통제 및 정보 콘텐츠 제한

- DMZ 구간과 병원정보시스템 사이 제한된 IP, 서비스에 대해서만 연결을 허용하고, 업무상 불필요한 모든 연결을 제한



[그림 2-6] 인터넷 연계 구간 DMZ 구성 예

나. 망연계 솔루션

○ 서로 다른 수준의 보안정책이 적용된 분리된 망 환경에서 높은 보안성을 유지하면서 데이터 연계와 파일 전송이 가능하도록 하는 망연계 솔루션 필요

12) DMZ : 내부 네트워크와 외부 네트워크 사이에 위치한 서브넷

○ 망연계 솔루션은 인증(보안기능확인서·CC인증 등)받은 제품을 사용

다. 네트워크 장비에 대한 안전한 설정

○ 네트워크 장비에 대한 최신 펌웨어 및 보안 패치 업데이트, 불필요한 서비스 차단, 배너 변경 등을 통하여 시스템 보안 강화

- 네트워크 장비에 대한 취약점이 지속적으로 공개되고 있으므로 주기적으로 업데이트 및 제조사 권고사항 적용
- 네트워크 장비에서 기본적으로 제공하는 서비스들에 대하여 검토하여 네트워크 운용관리에 필요하지 않은 서비스 차단
- 기본 설정된 배너는 네트워크 장비에 대한 정보를 제공하지 않도록 변경하고, RAT(Router Audit Tool)와 같은 네트워크 보안설정 점검 도구를 통하여 안전하게 설정되었는지 점검
- 운영 관리상 필요한 서비스는 반드시 패스워드를 사용하도록 설정하고, 관리자 시스템에서만 접근할 수 있도록 설정
- SSH 등과 같은 암호화된 서비스 사용
- 원격 접속 시 세션 타임아웃 설정

○ 네트워크 장비 제작업체에서 제공되는 기본 패스워드는 추측 및 크랙이 어려운 패스워드로 반드시 변경

- Login password, community string, enable password 등은 반드시 안전한 패스워드로 변경하여 적용

○ SNMP[13](Simple Network Management Protocol) 보안 설정

- SNMP는 UDP 프로토콜을 사용하여 DoS 공격에 취약하고 장비 성능 저하의 위험이 있어, 서비스를 사용하지 않는 경우 중지
- 낮은 버전의 SNMP v1/v2는 평문을 통해 전송되어 보안이 취약하므로 사용 금지

13) SNMP : 간이 망 관리 프로토콜

[표 2-2] SNMP 버전별 비교

버전	인증	암호화
V1	community string	X
V2	community string	X
V3(NoAuthNoPriv)	사용자명	X
V3(AuthNoPriv)	MD5 or SHA	X
V3(AuthPriv)	MD5 or SHA	DES

- SNMP에 대한 ACL을 적용하여 접근이 가능한 IP를 제한
- SNMP의 RO(Read Only)와 RW(Read&Write) 권한 중 네트워크 설정 정보를 임의 변경할 수 있는 RW 삭제 필요

○ 로깅 설정 및 NTP(Network Time Protocol)를 이용한 시간 동기화 적용

- 네트워크 장비 장애 및 침해 사고 시 이를 분석할 수 있도록 로깅을 설정
- 각 네트워크 장비의 시간이 다른 경우 정확한 사고분석을 수행할 수 없으므로, 각 네트워크 장비의 시간은 NTP를 사용하여 동기화

○ 불필요한 프로토콜 및 서비스 차단, ACL 적용, MAC 주소 필터링 등을 통해 안전한 네트워크 운영

- 병원정보시스템 운영에 필요하지 않은 프로토콜과 서비스는 네트워크에서 사용되지 못하도록 차단
- 비인가 접근 및 침해 전이로부터 안전성 강화를 위해 네트워크 및 서브넷 간의 통신에 대하여 ACL 설정
- 네트워크 내의 시스템이 소수인 경우 MAC 주소 필터링을 사용하여 제한된 시스템의 네트워크 접근만 허용

○ DDoS 공격 방어 설정

- DDoS 공격을 방어하기 위해 관리기관의 네트워크 구성·환경에 적합한 ACL 적용

○ ARP Spoofing 등의 비인가된 네트워크 사용과 침해에 대해 안전하도록 Port Security, ARP Inspection, 사설 VLAN 등의 기능 사용

- ARP Spoofing 등 각종 네트워크 공격에 대해서 안전한 장비를 도입하여 운영하는 것이 바람직함
- Port Security[14] 기능, ARP Inspection[15] 기능 등을 사용하여 ARP Spoofing에 대한 방지 대책 강구
- 병원정보시스템의 각 시스템 네트워크 규모가 크지 않은 경우 MAC 주소를 정적으로 지정하여 안전하게 관리
- 네트워크 장비에서 관리할 수 있는 MAC 주소는 제한적이므로 대규모 네트워크에서는 NAC(Network Access Control) 도입

14) Port Security 기능 : 네트워크 장비의 물리적인 포트가 수용할 수 있는 MAC 주소의 개수와 사용 가능한 MAC 주소를 고정적으로 지정할 수 있는 기능으로, MAC 주소의 정적인 관리로 ARP Spoofing 공격에 의한 IP/MAC 주소 테이블 불법 변조의 효과적인 차단 가능(네트워크 장비 공급사에 따라 제공하는 기능의 유무, 이름이 상이할 수 있음)

15) ARP Inspection(ARP 패킷 검사) 기능 : 침입차단시스템의 동작과 유사하게 네트워크 장비에서 ARP 패킷을 검사하여 지정된 경로로만 ARP 패킷이 전송되도록 하는 기능으로, ARP Spoofing 공격에 대한 효과적인 대응 가능 (네트워크 장비 공급사에 따라 제공하는 기능의 유무, 이름이 상이할 수 있음)

제3장 시스템 및 애플리케이션 보안대책

의료기관의 병원정보시스템은 상용 OS 기반의 서버, PC, 노트북 등의 자산 외에도 진료 및 진단을 위한 의료기기와 다수의 모바일 기기를 통하여 운영되고 있다. 환자의 의료정보를 다루는 병원정보시스템 특성상 내부 시스템 및 애플리케이션에 취약점이 존재하는 경우 사이버 공격으로 인해 개인정보 유출뿐만 아니라 의료시스템 마비로 이어질 수 있다.

본 장에서는 병원정보시스템을 구성하는 정보자산에 공통으로 적용할 수 있는 시스템 및 애플리케이션의 보안대책에 대해 제시하고, 의료기기 도입 시 검토해야 하는 보안대책에 대해 설명한다.

제1절 시스템 보안대책

가. 권한 관리

○ 사전 정의된 역할에 따라 시스템·메뉴·데이터의 접근이 차등적으로 관리되도록 적용 및 구현

- 의료기기 및 정보시스템의 특성과 사용자의 역할을 식별하여 역할별로 권한을 부여하고 관리

○ 권한 적정성 검토를 통해 부적합한 권한의 회수 조치

- 직무별 권한을 분리하고, 담당 업무별 최소 인원에게 최소권한 부여
- 업무와 무관한 사용자 존재 여부 확인
- 퇴직/휴직, 장기 시스템 미사용자 존재 여부 확인
- 계약이 종료된 협력사 직원 존재 여부 확인
- 업무시간 외 사용에 대한 사용 현황 확인

○ 의료기관 내 정보자산의 시스템 관리자 권한에 대해 관리·검토

※ 관리자 권한 : root, administrator 등 최상위 권한, 모니터링 및 배치작업 등의 권한, 정보보호시스템의 관리자 계정 등

- 필요시 책임자의 승인을 통해 최소한의 인원에게 권한을 부여하고 목록을 주기적으로 검토하여 재승인
- 유지보수 등을 위한 협력사 직원에게 특수 권한 계정 부여 시 작업 완료 후 계정 즉시 삭제 또는 정지

나. 접근통제

○ 의료기관의 정보자산을 보호하기 위해 직무 분류와 사용자 역할에 따른 접근통제 수행

- 정보자산의 등급과 사용자 역할·특성에 따라 접근 권한 정의
  - 의료기관 특성상 환자의 개인정보 관련 시스템 접근 권한과 이와 무관한 정보 및 애플리케이션 접근 권한 분리
- 시스템 접근 사용자, 접속 기기, 접속 장소 등의 종합적인 상황을 고려하여 시스템, 메뉴, 데이터에 대한 차등적인 접근통제 정책 적용
- 정의한 접근 권한에 따라 사용자 계정 및 권한 관리

○ 비인가자의 접근 차단을 위한 대책 수립

- 의료기관의 중요시스템에 대해서는 비인가자 접근 차단을 위한 정보보호시스템 설치
- 매체 제어, 백신 및 패치 관리, P2P나 메신저 사용 관리

다. 계정 관리

○ 계정 관리는 신청·승인·등록·잠금·회수 절차에 따라 수행

- 사용자 접속기록(ID, 접속일시, IP, 수행업무, 인증 로그, 파일 접근, 계정 권한 변경 등)에 대해 로그 기록
- 1인 1계정 원칙 하에 계정을 관리하여 사용자 추적성 확보
- 신규 계정 등록 시 신원 확인 및 승인 후 처리
- 퇴사 시 계정 즉시 삭제 또는 비활성화, 휴직 시 계정 잠금 등 처리
- 주기적 계정 유효성 및 중복성 점검

라. 사용자 인증

○ 시스템 로그인 시도 횟수 제한을 통해 비인가자의 접속 시도 차단

- 로그인 시도 제한 횟수를 설정하고, 횟수 초과 시 경고 메시지를 발송하고 로그인 시도 차단

○ 시스템 패스워드 정책 적용을 통해 취약한 비밀번호를 통한 접속 시도 차단

- 초기 또는 임시 비밀번호 변경 후 사용
- 숫자·문자·특수문자 등을 혼합하여 안전한 비밀번호 규칙을 수립하고 설정
- 추측하기 쉽거나 유출된 비밀번호 사용 제한
- 비밀번호 변경 주기 설정
- 동일한 비밀번호 재사용 제한
- 메모장, 엑셀 등을 통한 일괄적 비밀번호 관리 또는 공유 금지

○ 세션 타임아웃을 설정하여 일정 시간 동안 접속이 없으면 세션 중지

마. 불필요 포트 및 서비스 제거

○ 의료기관의 서버 및 컴퓨터, 의료기기, 단말기 등의 정보자산에 특별히 필요하지 않은 포트, 프로토콜 및 서비스 식별

- 주기적으로 정의된 규칙에 따라 불필요하고 안전하지 않은 포트, 프로토콜 및 서비스는 비활성화하거나 제거

바. 시스템 업데이트 및 보안패치

○ 주기적(최소 월 1회 이상)으로 보안 패치 공개 여부를 점검하고, 보안 패치 적용 시 적용일을 포함한 패치 정보를 기록 및 관리

- 운영체제별 보안 권고문 및 패치 사이트를 참조하여 해당 운영체제 버전으로 발표된 패치 수행
- 주요 보안 패치는 적용할 시스템에 대한 안전성 및 보안성을 검증한 후 안전한 경로를 통해 보안 패치 수행
- 시스템에 설치된 패치에 대해 관리 및 유지·보수할 수 있는 솔루션을 이용하여 패치 수행
  - OS에서 제공하는 보안패치 점검 도구 및 기타 점검 도구를 이용하여 보안 패치 수행
- 외부로부터 격리된 네트워크의 경우에는 저장매체를 사용하여 오프라인으로 업데이트 및 패치 파일 적용
- 업데이트 및 패치 절차를 수립하고, 업데이트 및 패치로 인한 시스템 오류와 장애를 최소화하기 위하여 테스트 환경을 별도 구성

사. 악성코드 통제

○ 의료기관 내 서버 및 컴퓨터 등 정보자산에 백신 프로그램 설치

- 정기적으로 악성코드 감염 여부에 대한 전수검사 실시(월 1회 이상)
- 중앙 통제를 통해 자동으로 백신 프로그램을 업데이트하고 이를 비활성화할 수 없도록 설정
- 백신 프로그램 설치·업데이트가 불가한 경우 별도 보안대책 마련
  - 정기적 점검 등을 통해 비인가 접근, 이상 프로세스 실행 여부 등 확인
  - USB·LAN포트 봉인, 비인가 기기를 차단하여 악성코드 유입 원천 차단
  - 인가된 정보통신 기기 접속 시 악성코드 감염 여부 점검 등
- 단말기의 각종 이벤트 수집을 통해 이상 징후 탐지 및 모니터링
- 악성코드 감염 시 해당 단말기의 네트워크 격리 조치

아. 정보 유출 통제

○ 의료기관 내 서버 및 컴퓨터 등 정보자산에서 발생 가능한 정보 유출 경로에 대한 통제 정책 수립

- 다음과 같은 정보 유출 경로에 대한 통제 수단 마련
  - 웹 메일, 클라우드 및 저장소를 통한 파일 등 정보 전송
  - 이동식 저장장치를 통한 파일 등 정보 저장
  - FTP/SFTP 등 외부와의 원격 접속을 통한 파일 등 정보 전송
  - LAN, Wi-Fi, 테더링 등 직접 통신을 통한 파일 등 정보 전송
- 정보 유출 이상 징후에 대한 모니터링 및 점검 수행
- 원격 접속에 대해 추적이 가능하도록 접속기록 로깅 및 주기적 분석
- 중요정보(예: 고유식별번호 등)를 저장할 때 암호화 적용

자. 노트북 및 모바일 기기 관리

○ 휴대가 가능한 노트북 및 모바일 기기에 개인정보, 의료정보 등 민감한 정보가 저장되는 경우 도난·분실·해킹으로 인한 사고가 발생할 수 있으므로 다음과 같은 관리 및 통제 적용

- 의료기관 내 사용하는 단말기에 대한 자산 리스트를 관리하고 등록된 기기만 사용할 수 있도록 설정
- 노트북 부팅 시 CMOS 비밀번호 설정
- 화면보호기 및 비밀번호 설정
- 저장 정보 암호화 적용
- 무선 네트워크 사용 시 암호화 적용 확인
- 시스템 변경 및 소프트웨어 설치·변경이 불가하도록 설정
- 도난·분실에 대비하여 원격 비활성화, 삭제 및 잠금 기능 적용

○ 기기 관리에 대해 정보보안 인식 제고, 교육·훈련 제공

차. 이동식 저장매체 보안

○ 의료기관 내 환자의 개인정보를 다루는 중요 서버 및 컴퓨터 등 정보자산의 USB 포트는 사용을 차단하고 승인된 USB 장치만 사용할 수 있도록 설정

- 의료기관 내 중요 서버 및 컴퓨터 등의 자산은 쓰기 가능한 이동식 미디어와 개인 소유의 이동식 미디어 사용 제한
- 내부 네트워크에 연결된 자산은 포트 잠금장치 등을 활용하여 승인된 USB 외 사용을 원칙적으로 금지
- USB 연결 시 자동 실행되지 않도록 자동 실행권한을 차단하고, 백신을 통해 악성코드 감염 여부 검사
- USB를 사용해야 하는 전용 PC 및 의료기기는 네트워크 격리하여 운영

제2절 애플리케이션 보안대책

가. SDLC[16](Software Development Life Cycle) 및 SPDL[17](Secure Product Development Life Cycle) 적용

○ 애플리케이션 분석·설계 시 사전 정의된 보안성 요건 적용

○ 애플리케이션 신규·변경 소스 코드에 대해 정적·동적 취약점 점검 수행 및 취약점 개선 조치

- 발견한 취약점 미조치 시 운영 환경으로 프로그램 이관이 불가하도록 통제

※ 단, 예외적인 상황으로 운영 이관 시 승인 절차 수행 후 사후 조치

○ 정기적으로 애플리케이션을 운영 중인 시스템 대상으로 취약점 점검 수행 및 취약점 개선 조치

○ SW, 의료기기 등의 제품 개발·공급업체는 전체 수명 주기 동안 보안을 고려하여 개발

나. 웹·애플리케이션 취약점 점검

○ 의료기관의 병원정보시스템에 웹·애플리케이션을 사용하는 경우 다음과 같은 취약점에 대해 점검을 수행하고 주요 보안 위협에 대한 시큐어 코딩 적용

- SQL 삽입 공격
- 경로 조작 및 자원 삽입
- XSS(크로스사이트 스크립트)
- CSRF(교차 사이트 요청 위조)
- 부적절한 오류 처리

16) SDLC : 소프트웨어 개발 생명주기
17) SPDL : 제품 개발 생명주기

- 위험한 형식 파일 업로드
- 메모리 버퍼 오버플로우
- 적절한 인증 없는 중요 기능 허용
- 반복된 인증 시도 제한
- 중요 자원에 대한 잘못된 권한 설정
- 중요 데이터 평문 저장 및 전송
- 하드 코딩된 비밀번호
- 주석에 하드 코딩된 시스템 주요 정보 등

다. 암호화 정책

○ 고도의 보안성이 요구되는 의료기관의 중요정보는 암호화를 통해 저장 및 전송

○ 법적·기관 요구사항을 고려하여 암호화 대상, 암호화 방법, 암호화 알고리즘 등의 정책 수립

- 암호화 관련 법적 요구사항 반영
- 암호화 대상 식별(개인정보, 의료정보, 비밀번호 등)
- 안전한 암호화 알고리즘(데이터 저장·통신 및 비밀번호 암호화 등)
- 암호 통제 정책
- 안전한 암호화 키 관리 정책 등

○ 정보 전송 시에도 인증 및 암호화 적용

- 비인가된 시스템의 정보 위·변조를 차단하기 위하여 서버와 시스템 간 인증을 수행하고, 암호화를 통해 무결성 검증 등의 보안대책 적용

제3절 의료기기 및 의료정보 보안대책

가. 의료기기 보안성 검토

○ 의료기관에서 의료기기를 구매할 때 최소한의 보안 요구사항을 검토한 후 도입·운영

- 의료기기 및 새로운 시스템을 수용하기 위한 요구사항과 기준을 명확히 정의, 합의, 문서화하고 테스트 수행
- 다음과 같은 조건을 고려하여 새로운 의료기기 승인
  - 모든 단계에서 영향을 받는 사람 및 그룹 대표와 협의
  - 도입 시 기존 시스템에 부정적인 영향을 끼치지 않는지 확인
  - 도입 전 의료기관 보안 영향도 분석 수행
  - 운영 절차 준비 및 테스트 방법 정의
  - 운영 또는 사용에 대한 사전 교육 제공
  - 오류 복구 및 재시작 절차, 비상조치 절차 교육 제공
- 현재 시스템의 상황 및 조건을 고려하여 새로운 시스템 설치로 인한 영향 분석 및 테스트
- 의료기기 공급담당자는 의료기관에서 정의한 보안 요구사항을 준수하고 이에 대한 테스트·평가 결과 제공
- 의료기관은 테스트·평가 결과 중 식별된 결함을 확인
- 경영진으로부터 공식 승인을 받은 후 새로운 의료기기를 사용하고 업그레이드 수행

※ 의료기기에 따라 본 가이드의 보안 요구사항을 모두 적용할 수 없는 경우 가능한 부분에 적용하고 다른 보안성 향상 방안을 고려하도록 권고

○ 다음을 고려하여 의료기기 사이버보안 요구사항 수립

- 의료기기 사이버보안은 가용성, 기밀성, 무결성을 종합적으로 고려
- 유·무선 통신 경로가 있는 의료기기는 정보의 위변조, 오작동 또는 의료기기에 승인되지 않은 접근 등을 방지하기 위한 대책 마련
- 의료기기 제조사는 의료기기의 통신 방법, 사용 환경, 잠재적 결함으로 인해 사용자에게 발생할 수 있는 위해 정보 등을 종합적으로 고려하여 보안 요구사항 적용
- 의료기기의 사이버보안 요구사항은 다음과 같음
  - 식별 및 인증
  - 사용통제
  - 시스템 무결성
  - 데이터 기밀성
  - 이벤트 적시 대응
  - 자원 가용성 등

※ 위 요구사항은 사이버보안 규제의 국제조화를 위해 IEC 62443-4-2, IEC 50501-4-5 규격의 요구사항을 적용한 것이며, 제품 특성상 적용할 수 없는 항목은 미적용 사유를 확인할 수 있는 근거자료를 제출

- 각 요구사항에 대해 보안 기능을 구현하는 경우 의료기기의 기본 안전과 필수 성능에 부정적인 영향을 주지 않아야 함
- 의료기기 자체적으로 요구사항에 대응하는 보안 기능을 제공하지 못하는 경우 상위 개체(예: IT 네트워크 수준)에서 제공하는 기능의 도움을 받도록 설계

※ 의료기기 사이버보안 요구사항 및 허가·심사에 대한 사항은 식약처『의료기기의 사이버보안 허가·심사 가이드라인, 2024』을 참고

나. 의료기기 보안대책

○ 의료기기 입고 및 설치 시 초기 비밀번호 변경을 포함한 보안 관련 설정 변경

- 취약한 관리자 ID 변경(예: administrator, admin, root 등)
- 초기 비밀번호 변경(예: 1111, 0000 등) 및 안전한 비밀번호 설정
- 특수 권한에 대해 이중 인증 설정으로 보안성 강화
- 공유폴더, 미사용 계정, 미사용 포트·서비스 삭제 및 비활성화
- 백신 설치(의료기기의 경우 충분히 검증된 버전을 사용)
- 이벤트 로깅 및 백업 설정
- 응급 모드 제공 시 위급한 경우만 사용 가능하도록 설정

※ 의료기기의 응급 모드는 응급 상황 시 정상적 환자 등록·확인 절차 없이 의료기기를 사용할 수 있는 기능을 제공

○ 의료기기 구매 계약 시 보안서약서와 비밀유지서약서를 징구하고 지속적 기술지원에 대해 협의

다. 의료기기 통신 보안

○ 의료기기 사용 및 통신 전송의 안전한 보호를 위해 인증 절차 수립

- 의료기기의 사용 및 통신에 표준 암호 알고리즘 및 프로토콜을 사용하여 인증 (예: DICOM 기기의 DICOM-TLS 기능 활성화)
- 의료기기의 메시지, 명령, 업데이트를 수행하는 통신은 강한 인증 방법(타임스탬프 사용, 일회용 번호, 디지털 서명 및 암호화 등) 사용
- 의료기기의 인증 방법 중에는 물리적 하드웨어(RFID, NFC 카드 등)를 이용한 인증 방법 고려
- 의료기기 사용 및 통신 전송의 인증 절차에 대해 정기적으로 검토

○ 다음을 고려하여 의료기기 정보 전송 정책 수립

- 의료기기 정보 전송과 관련된 기타 관련 법률, 규정, 규제 및 계약 요구사항 고려
- 정보 전송 보안 사고가 발생한 경우를 대비하여, 이해관계자 식별 및 역할과 책임 부여
- 의료기기 정보 전송 중 가로채기, 무단 접근, 복사, 수정, 파괴, 서비스 거부 등으로부터 보호하기 위한 정책(예: 암호화, 디지털 서명) 수립
- 의료기기 전송 정보 관리 연속성을 보장하기 위한 보안정책(예: 부인 방지 매커니즘) 수립
- 정보 전송 서비스 및 의료기기 사용에 대해 신뢰성 및 가용성을 고려한 정책 수립
- 의료기기 정보 전송에 관한 합의는 필요할 때마다 또는 정기적으로 정책 검토 및 수정

라. 의료정보의 저장·연계

○ 환자의 의료정보는 도난, 분실 등으로 인한 유출을 방지하고, 유출되더라도 해당 내용을 확인할 수 없도록 저장·관리되어야 하며, 전송 과정에서도 데이터 유출 방지되도록 보안대책 적용

- 개인정보보호법 상 환자를 식별할 수 있는 고유식별정보, 비밀번호, 바이오 정보 등은 저장·전송 시 개인정보 암호화 적용 기준에 따라 안전한 암호화 알고리즘을 사용하여 암호화

※ 개인정보의 암호화 조치에 대한 기준은『개인정보의 암호화 조치 안내서, 2020』를 참고

○ 환자의 의료정보가 저장된 이동식 미디어는 데이터 보호를 위해 안전한 장소 관리 및 사용 제한

- 이동식 미디어 보관 시 물리적인 안전장치가 있는 장소에 보관하고 주기적으로 모니터링

- 병원 내부에서는 쓰기 가능한 이동식 미디어와 개인 소유의 이동식 미디어 사용 제한

○ 외부 연계(예: 진료 협력, 타 기관 연계 관리 등) 시 교환 및 데이터 공유 정책 수립

- 다음을 수행 후 외부 연계(예: 진료 협력, 타 기관 연계 관리 등)
  - 정보의 분류 및 중요도 산정
  - 전송, 발송, 수령을 통제하고 통지하는 관리 책임 부여
  - 발송인에게 전송, 발송, 수령 사실 통보
  - 추적성 및 부인 방지 보장
  - 전송을 위한 최소한의 기술 수준 보장
  - 데이터 손실 등 정보보안 사고 발생 시 대응을 위한 책임과 의무 부여
  - 데이터 보호, 저작권, 소프트웨어 라이선스 준수 등에 대한 소유권 및 책임 고려 사항 정의
- 외부 연계 시 교환 및 데이터 공유 정책을 정기적으로 검토 및 업데이트 수행

○ 외부 연계 시 상호 연결된 시스템에 대한 보안 수준 및 보호조치 기준 정의

- 외부 연계 시 정보의 유출 등으로부터 보호하기 위한 기술적 보호조치 수행
- 환자 개인정보 활용을 위해 사전에 환자 개인정보 활용 목적, 범위, 세부 속성에 대해 확정하여 불필요한 정보가 활용되지 않도록 조치
- 정보의 기밀성과 무결성을 보호하기 위해 데이터 통신에 인증된 암호화 메커니즘 적용
- 상호 시스템 연계를 통해 송수신된 정보에 대한 보존 및 백업, 보안 사고 대책 준비

- 외부 연계를 위한 기준은 정기적으로 검토 및 업데이트 수행

※ 개인정보보호에 대한 항목은『분야별 개인정보 보호 안내서(2024.12) 내(內) 의료기관 편』,『개인정보보호법, 2024』,『개인정보보호법 시행령, 2024』을 참고

마. 제3자 서비스 수준 계약

○ 의료기관은 제3자 업체의 서비스를 제공받을 경우, 서비스 수준 계약(Service-Level Agreement, SLA)에 대해 적절한 수준을 관리

- 서비스 수준 계약 또는 서비스 약정이 합의된 계약은 책임, 서비스 정의, 보안 제어 및 기타 서비스 관리 측면 포함
- 개인정보 관리의 아웃소싱 계약의 경우 개인정보 처리에 필요한 정보 및 시스템을 이관하고 서비스 기간동안 보안이 유지되도록 보장
- 의료기관은 서비스 수준 계약에 대해 매년 업데이트 수행

○ 의료기관은 제3자 업체의 서비스를 제공받을 경우, 서비스 제공업체의 보안 기능 구현 여부를 확인

- 신규 및 기존 규정을 포함하여 경영진과 합의한 요구사항을 충족하는지 정기적으로 네트워크 서비스 감사 수행
- 제3자가 작성한 서비스 보고서를 검토하고 정기적인 회의 진행
- 제3자가 제공한 서비스 관련 문제, 장애 기록을 검토하고, 정보보안 사고에 대한 정보는 사고대응팀에 제공
- 의료기관은 제3자 서비스 제공업체의 보안 제어 규정 준수와 서비스 관리 및 서비스 수준을 지속적으로 모니터링하여 이상 및 위반 사항 감지

※ 의료기기 선정에 있어 환자 진료가 최우선이여야 하며, 의료기기 도입 시 자체적으로 마련한 정보보호솔루션이 있으면 사용 권고

제4장 관리적 보안대책

의료기관은 병원 진료를 위해 다수의 병원 관계자가 다양한 자산을 활용하는 복잡한 환경으로 구성되어 있다. 의료진, 행정직원, IT 개발·관리 인력 등 각기 다른 역할과 IT 지식수준을 가진 관계자들이 병원정보시스템을 운영·활용하여 각자의 업무를 수행한다. 이때 환자의 의료정보 및 개인정보를 포함한 민감한 정보를 다루는 의료기관 특성상 관리적 보안대책은 필수적으로 적용되어야 한다.

본 장에서는 의료기관의 정보보안 정책 및 조직을 수립하는 방안과, 자산 관리, 운영 관리, 물리 보안, 환자 개인정보 보호 등의 관리적 보안대책을 제시한다.

제1절 정보보안 정책 및 조직

가. 정보보안 정책 수립

○ 의료기관 차원의 사용자 역할 및 책임과 관련된 정책 또는 표준 수립

- 의료기관의 정보보안 요구사항을 도출하고 개인정보보호 관련 법과 규정, 지침에 부합하는 정책 수립
- 의료기관의 정보보안 관련 다양한 이해관계자의 역할 및 책임 정의
  - 의사, 간호사, 행정(원무) 직원, 병원정보시스템 개발자, 운영자, 의료기기 공급담당자, 정보보안 담당자, 시설·설비 담당자 등
- 비인가 접근, 정보 유출 등 보안정책 미준수 시 징계 사항 포함
- 사이버공격으로 인한 병원정보시스템 중단 등 사고 발생 시 이해관계자의 역할 및 책임에 따른 대응 및 복구 조치

○ 의료기관은 사용자 역할 및 책임에 관한 정책을 문서화하여 이를 배포하고 매년 검토 및 업데이트를 수행

나. 경영진의 책임

○ 의료기관 경영진에 대한 정보보안 정책, 절차, 보안 통제에 대한 관리 책임 정의

- 보안 위협 및 사고로 인한 병원 피해 및 영향도에 대해 이해
- 이해관계자들이 보안정책을 준수하도록 전사 공표 및 인식 제고
- 중장기 보안 로드맵 이행을 위한 예산 및 자원 확보 지원
- 보안 사고 발생 시 보고 체계, 전사 대응 및 의사결정에 참여
- 정기적인 협의체를 통한 전사 보안 관련 현안 검토 등 관리 감독

○ 의료기관 경영진은 보안 체계 구축, 점검, 교육 및 모니터링 활동 계획이 적시에 개발, 유지 및 실행되도록 보장

다. 정보보안 조직의 역할 및 책임

○ 의료기관의 정보보안 조직은 정보보호 정책, 절차, 보안 통제에 대한 관리 책임 정의

- 정보보호 최고책임자는 조직 전체의 정보보안 계획을 조정하고 개발, 구현 및 유지 관리 수행
- 보안정책의 수립, 문서화 및 배포, 지속적인 업데이트
- 보안 관리체계 개선을 위한 중장기 로드맵 수립 및 이행
- 보안 취약점 점검 및 조치
- 각종 보안 이벤트 및 이상 징후 모니터링 및 분석
- 위험평가 분석 결과에 대한 관리
- 의료기기에 대한 보안성 검토 및 정보 전송에 대한 보호조치
- 병원정보시스템의 네트워크 구획화, 단말기에 대한 망 분리
- 병원정보시스템의 사용자 계정 및 권한 관리

- 서버, DB, 네트워크, 애플리케이션, 단말기 등 보호 대상에 대한 보안정책 및 기술 적용
- 정보보안 사고 대응 및 단계별 절차 수립
- 정보보안 교육 수립 및 운영

라. 인적 보안

○ 의료기관에서 근무하는 인력에 대한 정보보안 방안을 마련하여 정보보안 사고 가능성 최소화

- 정보보안 준수 사항 수립 및 보안서약서 작성
- 정보보안 정책 및 절차 이행 여부 점검
- 정보보안 교육 이수 확인
- 정보보안 관련 상벌 규정 수립
- 고용 종료 및 직무 변경에 대한 절차 수립 및 이행
- 인사 변경에 따른 자산 및 권한 변경 등의 조치 이행 여부 확인
- 정보보안 사고 발생 시 행동 요령을 숙지하고 정보보안 담당자에게 신고

제2절 자산 관리

가. 정보자산 관리

○ 의료기관의 정보자산을 식별하여 등급화하고 이에 따른 적절한 관리와 보호를 수행

※ 정보자산: 정보시스템(서버, PC, 네트워크 장비, 애플리케이션 등), 정보보호 시스템(방화벽, 침입탐지시스템, 개인정보유출방지시스템 등), 정보(문서적·전자적 정보 등) 등

- 정보자산 도입, 변경, 폐기 관련한 관리 프로세스를 수립
  - 직원의 고용 및 계약 종료 시 반납 절차를 포함
  - 자산 폐기 또는 재사용 시 저장매체에 대한 절차를 수립 (예: 물리적 폐기, 재사용 시 완전 포맷 등)
- 정보자산별 보안등급을 식별하여 중요도가 높은 자산에 대해서는 추가적인 보안 통제가 적용될 수 있도록 관리
- 정보자산별 책임자 또는 관리자를 지정하여 관리
- 정보자산은 정기적으로 자산 실사 등을 통해 정보자산 현황을 최신화하여 관리

나. 취약점 점검 및 위험평가

○ 의료기관의 시스템 및 서비스에 대한 위험도, 발생 가능성, 영향도 등을 평가할 수 있는 위험평가 수행 기준 수립

- 정보자산 유형별 특성을 고려하여 적합한 취약점 점검 수행
- 연 1회 이상 위험평가를 수행, 해당 결과를 문서화하고 해당 내용에 대하여 경영진의 승인 획득
- 내부적으로 수용 가능한 위험으로 식별한 경우 관련 사유를 기재하여 문서화하고 경영진의 승인 획득

- 의료기관 내 신규 서비스 및 시스템이 도입되는 경우 내부 보안 검토 절차에 따라 보안 관련 위험평가 수행
- 정보시스템이나 운영 환경에 중대한 변화 발생 시 종합적인 위험평가 수행

다. 보안대책 수립

○ 보안대책 우선순위를 식별하고 위험을 개선하는 등 보안정책 수립 및 관리

- 위험평가 수행 결과를 기준으로 효과성, 경제성, 용이성, 적용 가능성 등을 평가하여 조치 우선순위에 따라 위험 조치 계획을 수립하고 경영진의 승인을 획득
- 위험 조치 계획이 이행될 수 있도록 조치 주관 부서, 담당자, 조치 기간 등을 수립 및 운영
- 위험 조치 계획 이행에 부하가 생기지 않도록 예산, 인력 등을 미리 확보
- 위험 조치 계획을 기반으로 위험의 개선 여부를 주기적으로 점검 및 모니터링 수행

제3절 운영 관리

가. 원격 접속 통제

○ 외부 네트워크에서 내부 네트워크로 직접 접속되지 않도록 원칙적으로 차단

- 불가피하게 내부 네트워크에 접속이 필요한 경우, 내부 원격 접속에 대해 소속 부서장 및 정보보안 담당자의 승인 후 다음과 같은 보안대책 마련
  - 원격 운영에 대한 정보보호 최고책임자 승인 절차
  - 접속 단말 및 사용자 인증 절차(강화된 인증 방식 적용 권고)
  - 한시적 접근 권한 부여(예: VPN 계정, 시스템 접근권한 등)
  - VPN 등의 전송 구간 암호화
  - 접속 단말 보안(예: 백신 설치, 보안패치 적용 등)
  - 원격 운영 현황 모니터링, 접속기록 로깅, 주기적 분석
  - 원격 운영 관련 보안 인식 교육 등
- 논리적 망분리 시스템에 접속 시 사용자 인증 및 다중(MFA) 인증을 적용하고, 승인받은 특정 시스템·기능만 접근할 수 있도록 통제

나. 외부 유지보수 관리

○ 외부 인력에 의한 정비와 정비 도구 반입·반출, 원격 접속 정비 등에 대한 보안대책을 마련하여 정보 유출 등 보안 사고에 대비

- 외부 인력에 의한 유지보수와 관련한 절차·주기·문서화 등에 관한 사항을 자체 규정에 포함하여 작성
- 유지보수 절차 수립 시 고려 사항
  - 공급자가 권고하는 서비스 기간 및 명세에 따라 유지보수 절차 및

항목을 수립·실시

- 유지보수 인력에 대한 인가 절차를 마련하여야 하며 인가된 인력만이 유지보수 실시
- 결함이 의심되거나 발생한 경우 이에 대한 모든 예방 및 유지보수 기록 보관
- 유지보수를 위해 시스템을 다른 장소로 이동하는 경우 적절한 통제수단 강구 및 적용

• 자체 유지보수 절차에 따라 정기적으로 정보시스템 정비를 시행하고 관련 기록 보관

• 유지보수 통제 및 기록 관리 시 고려 사항

- 유지보수는 엄격한 보안 통제하에 수행하며, 유지보수를 위한 제반 활동들을 기록하여 보관
- 시스템 변경 발생 시 정보보안 담당 부서와 협조하여 변경 사항에 대한 보안 관점 설계, 코딩, 테스팅, 구현 과정 통제
- 시스템 정비 시 일시, 담당자 인적 사항, 출입 통제 조치, 정비 내용, 시스템 폐기 또는 교체 목록 기재하여 관리

• 원격 정비 시 다음과 같은 보안관리 수행

- 외부에서의 원격 접속을 통한 정비는 원칙적으로 금지
- 원격 정비가 부득이한 경우 사전 승인 및 인증하여야 하며, 작업 내용을 모니터링 및 기록하고 사용 도구에 대한 보안점검 수행
- 원격 정비 등의 사용 종료 후에는 외부 접속 차단

다. 외주 개발 관리 감독

○ 의료기관의 정보시스템을 외주 위탁 개발하는 경우 SDLC에 따른 보안 요구사항 준수 여부 관리 감독

• SW 분석·설계·구현 및 개발 절차에 대해 보안 요구사항 명시

- 기능적, 기술적 요구사항 반영
- 개발 보안 가이드 준수(시큐어 코딩 등)
- 테스트 시 보안 요구사항 준수 여부 확인 절차 포함
- 개발한 시스템에 대한 취약점 점검, 진단 도구 사용 여부 확인
- 개발 완료 후 개발자 계정 및 권한, 테스트용 기능 제거 여부 확인

○ 개발·운영 환경은 물리적으로 구분된 별도의 네트워크로 분리

- 개발 인력 PC의 중요정보 저장 여부 점검
- 외주 개발 과정을 관리 및 통제하고 보안 활동 체크리스트 작성
- 개발 인력 대상 SW 개발 보안 관련 교육

라. 로깅과 모니터링

○ 의료기관의 네트워크 장비, 시스템, 서버, 의료기기, 애플리케이션 등에 대해 로깅과 모니터링을 수행하여 규정 준수 여부를 평가하거나 침해사고 발생 여부 및 책임 확인을 통해 사고 발생 시 대응

○ 정보시스템별 다음과 같은 로그 수집

- 보안 감사 로그 : 사용자 접속 기록(ID, 접속일시, IP, 수행업무), 인증 이벤트 로그, 파일 접근, 계정 및 권한 변경 등
- 시스템 로그 : 운영체제 구성 요소에 의해 발생하는 로그(시스템 시작/종료, 상태, 커널로그, 에러 코드 등)
- 보안시스템 정책 변경 및 이벤트 로그
- 기타 정보보안 관련 로그

○ 중요 시스템에 대해서는 접속기록 외에도 관리자 수준 권한 상승, 로그인 시도 실패, 민감한 데이터 접근, 데이터베이스 실행 실패 등에 대해 로깅 수행

○ 주기적으로 로그를 검토하여 이상 징후 확인

- 중요정보 및 정보시스템 사용자 접속 기록을 주기적으로 검토하여 오·남용 등의 이상 징후 확인
- 업무 목적 이외 중요정보의 과다 처리, 업무시간 외 접속, 비정상적인 접속 등을 검토 후 이상 징후 확인 시 책임자에게 보고

○ 로그의 위변조 및 삭제에 대비하기 위해 별도 저장장치 백업 및 보호 조치 수행

- 정보보안 침해가 의심되는 비정상적인 행위 발생 시 담당자에게 알람을 발송하도록 설정

마. 백업·복구 및 연속성 관리

○ 사람의 실수, 의도적 공격, 재해·재난 등에 의한 정보시스템 손상으로부터 시스템의 중단을 최소화하기 위해 업무 연속성 계획(Business Continuity Plan, BCP)을 수립하고 훈련

- 업무 중요도 및 영향을 분석하여 우선순위 및 복구 대상을 설정하는 등 업무 연속성 계획 전략을 수립하고 시험
- 주요 자원을 선별하고 재해 영향 및 허용·정지 시간을 분석하여 자원 복구 우선순위 결정
- 재해 복구 과정에서 혼란과 시행착오를 최소화하기 위해 비상 계획을 사전에 수립하고 모의 훈련을 통한 검증 수행
- 사이버 공격으로 인한 주 센터 마비를 대비하기 위해 재난 복구(Disaster Recovery, DR) 센터 구축 및 운영

○ 백업 데이터 범위, 빈도 및 기간을 포함하여 각 시스템에 필요한 백업 수준에 대해 정의

- 다음과 같이 백업에 대한 대상, 주기, 절차 정의
  - 백업 대상 정의(예: 전자의무기록 시스템 데이터)

- 백업 대상 정보시스템 이중화 여부
- 백업 주기 및 보존기간 정의(예: 월 1회 백업, 1년간 보존 등)
- 백업 방법 및 복구 절차
- 백업 매체 관리(예: 라벨링, 보관 장소, 접근 통제 등)
- 백업 담당자 및 책임자 지정, 백업 관리대장 관리 등
- 백업 시스템에 접근 시 통제된 단말기에 한해서 접근 허용하고, 이외 단말기는 접근 차단
- 백업 서비스가 제3자에 의해 수행되는 경우 서비스 수준 계약에는 백업 정보의 기밀성, 무결성 및 가용성을 보장하기 위한 상세 보호 조치를 포함

• 백업 정보의 완전성, 정확성 등을 점검하기 위해 정기적 복구 테스트를 수행

제4절 물리 보안

가. 보호구역 지정

○ 의료기관의 중요정보 또는 이를 처리하는 정보시스템은 비인가자 접근이 불가한 보호구역을 지정하고 해당 구역에 위치

- 지정된 보호구역을 식별하고 비인가자가 접근할 수 없도록 보호구역임을 표기

※ 접견구역: 외부인이 별다른 출입증 없이 출입이 가능한 구역

※ 제한구역: 비 인가된 접근을 방지하기 위해 별도 출입 통제 장치 및 감시 시스템을 설치한 장소(예: 부서별 사무실 등)

※ 통제구역: 조직 내부에서도 출입 인가자를 최소한으로 제한하여 비 인가된 접근 시도를 원칙적으로 차단할 수 있는 장소

- 지정된 보호구역은 외부 침입을 방지하기 위해 연결된 경계(예: 문, 창문 등)에 잠금장치 등의 보호조치 마련
  - 외부 접근 보호(예: 출입 통제 장치), 내부 자산 보호(예: 전산 랙 시건 장치 등) 등
- 보호구역 지정에 대한 현황을 주기적으로 확인 및 업데이트 수행

나. 재난·재해 대비 물리적 보호대책 수립

○ 보호구역에 대해 외부 위협(화재, 수해, 전력 이상 등)에 대한 보호조치 정의

- 정의된 정책에 따라 위협 발생 시 조치 프로세스 운영
- 다음과 같은 보호 설비를 구현
  - 화재 감지 및 소화, 누수감지기, 접지 시설, UPS, 비상 발전기, 전압 유지기, 이중전원선, 침입경보기, RACK 등 설치
  - 재해 발생 시 임직원이 대피하기 위한 절차를 마련하고, 비상벨, 비상등, 비상로 등의 안내 표지 설치

- 보호 설비 또는 보호 설비를 운영하는 시설에 대한 정기 점검을 통해 외부 위협에 대한 보호 수준을 주기적으로 검토

다. 출입 통제

○ 정보시스템, 중요 자산이 있는 보호구역은 허용된 인원만 출입할 수 있도록 출입 통제 절차 수립

- 다음의 항목을 포함한 출입 현황을 자동 혹은 수동으로 기록
  - 방문자, 조직, 서명, 신원 확인 내용, 접근 시간, 방문 목적 등
- 출입 기록 및 출입 권한을 주기적으로 모니터링하여 비인가 출입, 장기미 출입자 등에 대한 사유 확인 및 조치

라. 작업 통제

○ 보호구역 내 작업에 대한 절차, 기록 및 통제 방안 수립

- 보호구역 내 작업이 필요한 경우, 공식적인 작업 신청·승인 및 수행 절차에 따라 작업 내용 기록
  - 보호구역 출입 통제 담당자에게 사전에 신청·승인 필요
  - 작업 기록은 작업 일시, 목적, 작업 내용, 업체 및 담당자명, 검토자 승인 사항 등 포함
  - 보호구역 내 모바일 기기 사용은 원칙적으로 금지하나, 필요시 반·출입 절차, 기기 안정성 확보 절차(예: MDM 설치 등) 마련
- 보호구역 내 작업이 정의된 절차에 따라 수행되었는지 주기적 검토

○ 비인가자의 불법적인 접근을 방지하기 위해 보호구역과 분리된 외부 접점에 적재 및 하역 구역 마련

- 적재 및 하역 구역을 통해 반입되는 물품의 경우 자산 관리 절차에 따라 등록 및 승인
- 정의한 자산 관리 절차가 준수되는지 등록 및 검토 현황을 주기적 검토

제5절 환자 개인정보보호

가. 개인정보 개요

○ '개인정보'란 살아있는 개인에 관한 정보로 성명, 주민등록번호, 영상 등을 통해 개인을 알아볼 수 있거나, 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 개인을 특징지을 수 있는 정보 의미

- 개인정보를 가명 처리하여 원래 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 가명 정보도 포함

※ 의료기관에서 환자의 개인정보란 성명, 주민등록번호, 연락처, 환자등록 번호, 진료카드번호, 건강보험증번호, 유전자정보, 아이디, 비밀번호, 건강상태, 신체적 특징, 병력 등을 포함 진료과정에서 생성되는 진료정보 및 환자와 관계된 모든 정보를 말함

○ 「개인정보보호법」은 정보주체의 '개인정보 자기 결정권'을 보장

- 개인정보의 수집·이용·제공이 정당한 절차에 의해 이루어지고, 내부자의 고의나 관리 부주의 또는 외부 공격으로 인해 유출·변조·훼손되지 않도록 안전하게 관리

○ 의료기관에서 개인정보 처리를 규율하고 있는 다른 법률에 환자, 의료인, 직원의 개인정보 처리와 관련된 특별한 규정이 있으면 해당 법률이 우선적으로 적용되며 그 외에는 「개인정보 보호법」 적용

※ 법률의 위임 없이 시행령, 시행규칙, 고시 등 하위 규정으로 개인정보처리에 관해 규정하는 경우 「개인정보 보호법」 우선 적용

나. 개인정보의 수집·이용

○ 의료기관은 목적에 필요한 최소한의 개인정보를 수집하여야 하며, 필요 최소한의 개인정보 수집이라는 입증 책임을 의료기관이 지며, 또한 그 수집 목적의 범위 내에서 개인정보 이용

- 개인정보 수집·이용 동의 시 정보 주체에게 ①수집·이용 목적, 수집 항목 ②보유 및 이용 기간 ③동의 거부 권리가 있다는 사실, 동의 거부 시 불이익이 있다면 그 내용을 고지

○ 의료기관은 당초 수집 목적과 합리적으로 관련된 범위에서 정보주체에게 불이익이 발생하는지 여부, 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 정보 주체의 동의 없이 개인정보 이용 가능

○ 고유식별정보(주민등록번호 제외) 또는 민감정보를 수집·이용하는 경우 정보주체의 동의를 별도로 받거나 법령에 구체적인 근거가 있는지 확인 필요

- 법령에 따라 진료목적을 위하여 고유식별정보, 민감정보를 수집하고 이용 가능

○ 거짓이나 그 밖의 부정한 수단이나 방법으로 개인정보를 취득하거나 처리에 관한 동의를 받는 행위 금지

다. 개인정보의 제3자 제공

○ 개인정보는 환자, 의료인, 직원 등 정보주체의 동의를 받거나 법률에서 정한 개인정보 수집 목적 범위 내에서 제3자에게 제공 가능

- 개인정보를 제3자에게 제공하는 경우에는 ①제공받는 자 ②개인정보 이용목적 ③개인정보 항목 ④개인정보 보유 및 이용기간 ⑤동의거부 권리가 있다는 사실, 동의 거부 시 불이익이 있다면 그 내용을 고지

○ 의료기관은 당초 수집 목적과 합리적으로 관련된 범위에서 정보주체에게 불이익이 발생하는지 여부, 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 정보주체의 동의 없이 개인정보 제공 가능

○ 민감정보 또는 고유식별정보를 제3자에게 제공하는 경우에는 해당 정보주체의 동의를 별도로 받거나 법령에 구체적인 근거 필요

○ 업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공하는 행위 금지

라. 개인정보 처리 업무위탁

○ 의료기관에서 환자 등의 개인정보 처리 업무를 제3자에게 위탁하는 경우에는 다음 사항을 개인정보 처리 위탁 계약서에 기재

※ 환자 등의 개인정보 처리 업무는 진료 신청서, 진료비 수납사무, 연말정산 사무, 각종 증명서 발급사무 등을 의미

- 위탁업무의 목적 및 범위, 위탁 수행 목적 외 개인정보의 처리 금지에 관한 사항, 재위탁 제한에 관한 사항
- 개인정보의 기술적·관리적 보호조치, 개인정보에 대한 접근 제한 등 안전성 확보조치에 관한 사항
- 위탁업무와 관련 보유한 개인정보 관리현황 점검 등 감독에 관한 사항, 수탁자가 준수해야 할 의무를 위반한 경우 손해배상 등 책임에 관한 사항 등

○ 의료기관은 개인정보 처리 업무를 위탁받아 처리하는 수탁자를 환자 등이 언제든지 쉽게 확인할 수 있도록 홈페이지에 '개인정보 처리방침'으로 지속적으로 게재

○ 개인정보처리업무를 위탁한 의료기관은 수탁자에 대해 개인정보가 분실·도난·유출·변조·훼손되지 않도록 교육하고, 개인정보보호법과 시행령, 표준 개인정보보호 지침을 준수하는지 감독

○ 수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에 「개인정보보호법」을 위반하여 발생한 손해배상 책임에 대해서는 수탁자를 의료기관의 소속 직원으로 간주

마. 영업의 양도

○ 영업양도, 합병 등으로 개인정보를 다른 의료기관에 이전하여야 하는 때에는 개인정보를 이전하기 전 해당 정보주체에게 ①개인정보를 이전하려는 사실, ②개인정보를 이전받는 자의 성명, 주소, 연락처, ③이전을 원하지 않는 경우 조치 방법·절차를 통지

- 영업양도 등에 따라 개인정보 이전 사실을 통보하는 경우 서면, 전자우편, 팩스, 전화, 문자전송 등의 방법을 사용하거나 인터넷 홈페이지에 30일 이상 게재
- 개인정보를 이전받은 의료기관은 정보주체에게 개인정보의 이전 사실 등을 지체없이 통지
- 개인정보를 이전받은 의료기관은 본래 목적으로만 개인정보를 이용할 수 있으며, 개인정보처리자로서의 권리와 의무를 가짐

바. 개인정보파일의 등록 (공공의료기관)

○ 공공의료기관에서는 개인정보 파일을 개인정보보호위원회에 등록하여야 운용 가능

- 개인정보파일의 등록·변경등록은 개인정보취급자가 해당 공공기관의 개인정보 보호책임자에게 신청하고 개인정보 보호책임자가 개인정보보호위원회에 등록
- 개인정보 보호책임자는 등록·변경등록 사항을 검토하고, 그 적정성을 판단하여야 하며, 해당 개인정보파일을 운용하기 시작한 날부터 60일 이내에 개인정보보호위원회에 등록·변경등록 수행
- 개인정보 파일을 등록·변경등록하기 위해서는 '개인정보 파일 등록·변경등록 신청서'를 작성하여 신청하고, 등록한 개인정보 파일을 보유하는 경우 1개의 개인정보 파일에 1개의 대장을 작성하여 관리
- 개인정보파일을 등록할 때는 기관 명칭, 운영 근거 및 목적, 개인정보 항목, 정보주체 수, 처리방법, 보유기간, 제공받는 자, 처리 업무 담당 부서, 영향평가의 결과 등 개인정보파일 등록사항을 기재
- 개인정보보호위원회는 개인정보파일의 등록 현황을 누구든지 쉽게 열람할 수 있도록 공개 가능
- 개인정보보호위원회는 개인정보파일의 등록사항과 그 내용을 검토하여 개선 권고 사유에 해당하는 경우 그 개선을 권고 가능

사. 개인정보의 파기

○ 의료기관은 다음과 같은 사유로 개인정보가 불필요하게 되었을 때 그 날로부터 지체없이 파기하고, 파기할 때 복구 또는 재생되지 않도록 조치

- 개인정보의 보유기간이 경과된 경우, 개인정보의 처리목적의 달성
- 해당 의료 서비스의 폐지, 의료기관의 폐업

※ 의료기관 폐업 또는 휴업의 경우 진료기록은 관할 보건소장에게 이관

※ 공공 의료기관이 폐업한 경우 그 사무를 승계하는 기관이 없는 경우 기관의 기록물을 지체없이 소관 영구기록물 관리기관으로 이관

※ 정보주체가 의료기관의 홈페이지에서 탈퇴하는 경우 의료기관은 지체없이 파기

○ 보유기관 경과 또는 목적달성 시 지체없이 파기하는 것이 원칙이지만, 의료기관 관련 개별 법령에서 보존기관을 별도로 정하고 있는 경우 해당 법령에서 정하는 기간 동안 보존

- 의료기관의 개인정보 중 진료기록의 보존기관과 보존 방법은 「의료법 시행 규칙」 제15조에 따라 다음과 같음
  - 환자명부 5년, 진료기록부 10년, 처방전 2년, 수술기록 10년, 검사 내용 및 검사소견 기록 5년, 방사선사진 및 그 소견서 5년, 간호 기록부 5년, 조산기록부 5년, 진단서 등의 부본 3년 등

○ 보유기관 경과하여 처리 목적달성 시 지체없이 파기하는 것이 원칙이지만, 진료목적상 필요한 경우 해당 진료정보에 대해 1회에 한정하여 그 기간을 연장 가능

- 개별 진료정보 별로 연장기간, 연장 사유 등을 심의하여야 하고, 연장 기간은 과도한 기간동안 보존되지 않도록 사유에 부합된 최소 기간 동안만 연장
- 연장 보존을 결정한 경우 의료기관의 홈페이지 또는 보기 쉬운 장소에 게시하는 것을 권고

○ 의료기관의 진료정보를 포함한 기록물 파기는 제3자 위탁 시행이 가능한데, 개인정보처리 업무위탁에 따라 이를 처리

○ 공공 및 민간의료기관에서 환자 개인정보를 수집·이용·보관시 안전성 확보 조치를 한층 강화하여 시행

○ 다른 법령에 따라 보존해야 하는 경우 해당 법령을 표시하고 다른 개인정보파일과 분리하여 보존

아. 개인정보 처리방침의 수립 및 공개

○ 의료기관은 개인정보 처리방침을 수립하고 홈페이지 등을 통하여 이를 공개

- 공공의료기관은 개인정보보호위원회에 등록하여야 하는 개인정보파일에 대하여 개인정보 처리방침을 수립하고 이를 홈페이지 등을 통해 공개
- 개인정보 처리방침을 변경하는 경우 변경 및 시행의 시기, 변경 내용을 정보주체가 쉽게 확인할 수 있도록 변경 전·후를 비교하여 이를 홈페이지 등을 통해 지속적으로 공개
- 개인정보 처리방침의 내용과 의료기관과 정보주체 간에 체결한 계약의 내용이 다른 경우에는 정보주체에게 유리한 것을 적용

자. 개인정보 보호책임자 지정

○ 개인정보의 처리에 관한 업무 총괄 및 다음의 업무 수행을 위해 개인정보 보호책임자를 지정

- 개인정보 보호책임자를 지정·변경한 경우에는 해당 사실, 성명과 부서의 명칭, 전화번호 등 연락처를 개인정보 처리방침 등에 공개
- 개인정보보호 책임자를 공개하는 경우 해당 고충처리 및 상담을 실제로 처리할 수 있는 연락처를 공개해야 하며, 이 경우 개인정보보호 업무 담당자의 성명, 부서의 명칭, 전화번호 등을 함께 공개 가능

차. 정보주체의 권익보호

○ 의료기관은 요구가 있으면 개인정보를 열람·정정·삭제하여야 하고, 환자 등의 개인정보가 유출된 경우 환자 등에게 그 사실을 고지

- 환자 등 정보주체 이외로부터 수집한 개인정보를 처리하는 때에는 정보주체의 요구가 있은 날로부터 3일 이내에 수집 출처 및 처리 목적, 처리정지 요구 권리 또는 동의를 철회할 권리가 있다는 사실 고지

○ 전년도 말 기준 직전 3개월간 일일평균 5만명 이상의 정보주체에 대한 민감정보 또는 고유식별정보를 처리하거나, 100만명 이상의 정보주체에 관한 개인정보를 처리하는 의료기관은 다음과 같이 정보주체에 통지

- 정보주체 이외로부터 수집한 개인정보를 처리하는 경우 개인정보를 제공받은 날로부터 3개월 이내에 모든 사항을 정보주체에 통지
- 개인정보의 이용·제공 내역이나 이를 확인할 수 있는 시스템에 접속하는 방법을 연 1회 이상 정보주체에 통지

○ 정보주체가 개인정보에 대한 열람을 요구할 경우 의료기관은 열람 요구를 받은 날부터 10일 이내에 조치

- 환자의 기록에 대해서는「의료법」제21조에 따라 요구 처리
- 10일 이내 열람할 수 없는 정당한 사유가 있으면 그 사유를 알리고 열람을 연기할 수 있으며, 사유가 소멸시 지체없이 열람 처리
- 열람 제한·거절 사유에 해당하는 경우 그 사유를 알리고 열람을 제한·거절 가능
- 환자가 아닌 다른 사람에게 기록 열람이나 그 사본을 내주는 등 환자의 개인정보 내용을 확인할 수 있게 하는 것은 불가

○ 개인정보를 열람한 정보주체가 해당 개인정보의 정정·삭제를 요구할 경우, 10일 이내에 조치하고 그 결과를 통지

- 다른 법령에서 그 개인정보가 수집대상으로 명시된 경우 그 삭제를 요구하는 것은 불가

- 의료법 시행규칙에 근거하여 수집되는 진료기록부, 조산기록부, 간호기록부 등에 기재된 개인정보는 보관 기간에 대한 정정·삭제 요구는 불가
- 정보주체는 의료기관에 대하여 자신의 개인정보에 대한 처리에 대한 정지를 요구하거나 동의를 철회할 수 있으며, 의료기관은 10일 이내 조치 결과 통지

○ 개인정보가 분실·도난·유출된 경우 72시간 내에 정보주체에게 해당 항목, 시점과 경위, 대응조치 및 구제 절차, 담당자 연락처 등 통지

○ 진료정보 유출·침해사고가 발생한 때에는 보건복지부장관에게 즉시 그 사실을 통지(「의료법」 제23조의3)

카. 피해 구제 방법

○ 「개인정보 보호법」은 다음과 같은 피해 구제 방법을 규정

- 개인정보 분쟁조정, 개인정보 집단 분쟁조정
- 개인정보 단체소송, 침해사실 신고
- 징벌적 손해배상제도, 법정 손해배상제도 등

[표 4-1] 가명정보의 처리| 개인정보의 안전성 확보조치| 고정형 영상정보처리기기의 설치·운영

<가명정보의 처리>

- 의료기관은 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보 주체의 동의 없이 가명정보를 처리 가능
  - 가명처리 일반에 관한 사항은 「가명정보 처리 가이드라인」 참고
  - 보건의료 분야의 개인정보 가명처리에 관한 사항은 「보건의료데이터 활용 가이드라인」 참고

<개인정보의 안전성 확보조치>

- 의료기관은 처리하는 환자 등의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 안전성 확보에 필요한 기술적·관리적·물리적 조치 수행
  - 안전성 확보조치 관련 자세한 사항은 「개인정보의 안전성 확보조치 기준(개인정보보호위원회 고시)」 및 「개인정보의 안전성 확보조치 기준 안내서」 참고

<고정형 영상정보처리기기의 설치·운영>

- 의료기관이 영상정보처리기기(CCTV, 네트워크 카메라)를 설치·운영하고자 할 때에는 개인의 사생활이 침해되지 않도록 최소한의 고정형 영상정보처리기기를 설치·운영
  - 고정형 영상정보처리기기의 설치·운영에 관한 자세한 사항은 「고정형 영상정보처리기기 설치·운영 안내서」 참고

※ 의료기관의 개인정보보호에 대한 항목은 『분야별 개인정보 보호 안내서(2024.12) 내(內) 의료기관 편』을 기준으로 간략하게 정리하였으며, 상세한 내용은 해당 문서를 참고

※ 또한 관련하여 법률 및 기준은 『개인정보보호법, 2024』, 『개인정보보호법 시행령, 2024』을 확인·검토

제5장 결론

병원정보시스템은 환자의 생명을 지키고 건강을 증진시키는데 중요한 역할을 하며, 의료진과 병원 관계자가 병원을 효율적으로 운영할 수 있도록 돕는 핵심 시스템이다. 그러나 이러한 시스템에 신뢰성 있는 보안 체계와 안정적인 운영이 뒷받침되지 않는다면, 개인정보 유출이나 환자의 생명과 직결된 사고와 같은 심각한 문제를 초래할 위험이 있다.

가이드라인에서 제시한 병원정보시스템의 구조는 일반적인 운영 현황을 바탕으로 제시한 것이다. 또한, 보안대책은 병원정보시스템의 보안 강화를 위해 가장 중요하게 고려해야 할 사항들을 우선적으로 정리한 내용이다.

따라서 각 병원은 자신의 규모와 운영 환경을 고려하여, 가이드라인에서 제공하는 내용을 준수하여 보안을 강화할 수 있다.

병원정보시스템 구축 및 운영에 있어, 본 가이드라인을 참고하여 병원의 사이버 역량을 강화하고 시스템을 안전하게 운영함으로써 환자와 의료진 모두에게 신뢰할 수 있는 환경을 조성할 수 있으며, 보다 안전하고 효율적인 의료 서비스를 제공할 수 있을 것이라 기대한다.

부록

부록1 의료기관을 위한 정보보호 안내서 참고표

본 가이드라인은 병원정보시스템의 구성요소를 식별하고, 크게 네트워크, 시스템 및 애플리케이션, 운영 관리상의 보안대책으로 구분하여 상위수준에서의 보안대책을 제시하고 있다. 본 가이드라인에서는 개별 보안대책에서 준수하거나 참고해야 하는 문서 및 가이드는 본문에 표기해 두었다. 부록에서는 보안대책 항목에 대한 세부사항을 확인할 수 있도록 기존에 발간된 『의료기관을 위한 정보보호 안내서, 2016』에 대해 항목을 매핑하여 제시한다.

보안대책	세부 보안대책	정보보호 안내서
제2장 네트워크 보안대책		
제1절 네트워크 공통 보안대책	가. 네트워크 분리 및 접근제어	5. 접근통제 9. 통신보안 – 네트워크 관리 – 네트워크 분리 – 방화벽 – DMZ – 정보전송
제2절 연계 구간별 네트워크 보안대책	가. 시스템 내 연계 구간	
	나. 시스템 간 연계 구간	
	다. 인터넷 연계 구간	
	라. 의료기기 및 단말기 연계 구간	
제3절 상세 네트워크 보안대책	가. DMZ 구간 구성	
	나. 망연계 솔루션	
	다. 네트워크 장비에 대한 안전한 설정	

보안대책	세부 보안대책	정보보호 안내서
제3장 시스템 및 애플리케이션 보안대책		
제1절 시스템 보안대책	가. 권한 관리	5. 접근통제 8. 운영보안 – 접근통제
	나. 접근통제	
	다. 계정 관리	
	라. 사용자 인증	
	마. 불필요 포트 및 서비스 제거	3. 인적보안 – 종사자 유의사항 8. 운영보안 – 안티바이러스 – 노트북/모바일 기기 – 휴대용 저장장치
	바. 시스템 업데이트 및 보안패치	
	사. 악성코드 통제	
	아. 정보 유출 통제	
	자. 노트북 및 모바일 기기 관리	
	차. 이동식 저장매체 보안	
제2절 애플리케이션 보안대책	가. SDLC 및 SPDL 적용	9. 통신보안 10. 시스템 도입·개발·유지보수
	나. 웹·애플리케이션 취약점 점검	
	다. 암호화 정책	
제3절 의료기기 및 의료정보 보안대책	가. 의료기기 보안성 검토	8. 운영보안 9. 통신보안 11. 공급자 관계 – 업무위탁 시의 관리·감독 책임 『의료기기 담당자의 정보보호 안내서』
	나. 의료기기 보안대책	
	다. 의료기기 통신 보안	
	라. 의료정보의 저장·연계	
	마. 제3자 서비스 수준 계약	

보안대책	세부 보안대책	정보보호 안내서
제4장 관리적 보안대책		
제1절 정보보안 정책 및 조직	가. 정보보안 정책 수립	1. 정보보호 정책 2. 정보보호 조직 3. 인적보안 10. 정보보호 사고관리
	나. 경영진의 책임	
	다. 정보보안 조직의 역할 및 책임	
	라. 인적 보안	
제2절 자산 관리	가. 정보자산 관리	4. 자산관리 – 자산 중요도 식별
	나. 취약점 점검 및 위험평가	
	다. 보안대책 수립	
제3절 운영 관리	가. 원격 접속 통제	9. 통신보안 – 원격접속
	나. 외부 유지보수 관리	10. 시스템 도입·개발·유지보수 11. 공급자 관계 – 용역계약 보안요구 사항 – 협력업체의 내·외부 네트워크 접속
	다. 외주 개발 관리 감독	
	라. 로깅과 모니터링	6. 운영보안 – 로깅과 모니터링 13. 재난시 업무연속성
	마. 백업·복구 및 연속성 관리	9. 통신보안 10. 정보보호 사고관리 13. 재난시 업무연속성

보안대책	세부 보안대책	정보보호 안내서
제4절 물리 보안	가. 보호구역 지정	7. 물리적 환경적 보안 – 제한 및 통제 구역 지정 – 환경적 위험 보호 적용 – 출입/외부인 통제 – 중요시설 격리
	나. 재난·재해 대비 물리적 보호대책 수립	
	다. 출입 통제	
	라. 작업 통제	
제5절 환자 개인정보보호	가. 개인정보 개요	3. 인적보안 – 병원 종사자 유의사항 14. 법적 준수성 『분야별 개인정보 보호 안내서(2024.12) 내(內) 의료기관 편』
	나. 개인정보의 수집·이용	
	다. 개인정보의 제3자 제공	
	라. 개인정보 처리 업무위탁	
	마. 영업의 양도	
	바. 개인정보파일의 등록(공공의료기관)	
	사. 개인정보의 파기	
	아. 개인정보 처리방침의 수립 및 공개	
	자. 개인정보 보호 책임자 지정	
	차. 정보주체의 권익보호	
	카. 피해 구제 방법	

부록2 참고문헌

[1] 식약처, 의료기기의 사이버보안 허가·심사 가이드라인, *https://mfds.go.kr,* 2024

[2] 개인정보보호위원회, 분야별 개인정보 보호 안내서 내(內) 의료기관 편, *https://pipc.go.kr,* 2024.12

[3] 개인정보보호위원회, 개인정보의 암호화 조치 안내서, *https://pipc.go.kr,* 2020

[4] 개인정보보호법, *https://law.go.kr*, 2024

[5] 개인정보보호법 시행령, *https://law.go.kr*, 2024

[6] 의료법, *https://law.go.kr*, 2024

[7] 보건복지부, 한국보건산업진흥원(KHDI) 개발 및 공개, 의료기관을 위한 정보보호 안내서(병원편), *khidi.or.kr*, 2016

[8] 보건복지부, 한국보건산업진흥원(KHDI) 개발 및 공개, 의료기관을 위한 정보보호 안내서(의원편), *khidi.or.kr*, 2016

[9] 보건복지부, 한국보건산업진흥원(KHDI) 개발 및 공개, 의료기관을 위한 정보보호 안내서(약국편), *khidi.or.kr*, 2016

[10] 보건복지부, 한국보건산업진흥원(KHDI) 개발 및 공개, 의료기관을 위한 직무별 정보보호 안내서(IT 담당자 편), *khidi.or.kr*, 2016

[11] 보건복지부, 한국보건산업진흥원(KHDI) 개발 및 공개, 의료기관을 위한 직무별 정보보호 안내서(최고경영자, 의사, 간호사 편), *khidi.or.kr*, 2016

[12] 보건복지부, 한국보건산업진흥원(KHDI) 개발 및 공개, 의료기관을 위한 직무별 정보보호 안내서(의료기기 담당자 편), *khidi.or.kr*, 2016

[13] 보건복지부, 한국보건산업진흥원(KHDI) 개발 및 공개, 의료분야 정보보호안내서, *khidi.or.kr*, 2016

병원정보시스템
보안가이드라인

국가정보원 NSR 국가보안기술연구소