



제423회국회(임시회)
제1차보건복지위원회

의료법 일부개정법률안

검 토 보 고

〈진료정보 침해사고 범위 확대〉

■ 전진숙의원 대표발의(의안번호 제8049호)

2025. 3.

보 건 복 지 위 원 회

수석전문위원 이지민

목 차

I . 개요	1
II . 주요 내용별 검토	2
1. 개정안의 내용	2
2. 검토의견	5
3. 관계 부처 및 관련 단체 의견	15

I. 개요

1. 제안경위

(1) 제 안 자 : 전진속의원 등 11인

(2) 제 안 일 : 2025. 2. 11.

(3) 회 부 일 : 2025. 2. 12.

2. 제안이유 및 주요내용

현행법은 의료기관으로 하여금 전자의무기록에 대한 전자적 침해행위로 진료정보가 유출되는 경우 이를 보건복지부장관에게 통지하도록 하고, 보건복지부장관은 진료정보 침해사고의 예방 및 대응을 위하여 진료정보 침해사고에 관한 정보의 수집·전파, 진료정보 침해사고에 대한 긴급조치 등을 실시하도록 규정하고 있음.

그런데 전자의무기록시스템 외에도 의료기관에서 운영하고 있는 영상정보시스템, 검사정보시스템 등에 대한 전자적 침해 또한 환자 및 의료기관의 정보 침해로 이어질 수 있으므로 진료정보 침해사고의 범위를 확대할 필요가 있음.

이에 전자의무기록 외에 의료기관에서 운용하는 전산시스템에 대한 전자적 침해행위로 정보가 유출된 경우에도 진료정보 침해사고로 관리하도록 함으로써 의료기관에 대한 정보 침해사고의 예방 및 대응의 실효성을 제고하려는 것임(안 제23조의3 및 제23조의4 등).

정보 침해사고”라 한다)가 발생한 때에는 보건복지부장관에게 즉시 그 사실을 통지하여야 한다.

② 보건복지부장관은 제1항에 따라 진료정보 침해사고의 통지를 받거나 진료정보 침해사고가 발생한 사실을 알게 되면 이를 관계 행정기관에 통보하여야 한다.

제23조의4(진료정보 침해사고의 예방 및 대응 등) ① 보건복지부장관은 진료정보 침해사고의 예방 및 대응을 위하여 다음 각 호의 업무를 수행한다.

1. 진료정보 침해사고에 관한 정보의 수집·전파
2. 진료정보 침해사고의 예보·경보
3. 진료정보 침해사고에 대한 긴급 조치
4. 전자의무기록에 대한 전자적 침해행위의 탐지·분석
5. 그 밖에 진료정보 침해사고 예방 및 대응을 위하여 대통령령으로 정하는 사항

<신 설>

-----진료정보등 침해사고-----

---.

② -----진료정보등 침해사고-----
---진료정보등 침해사고-----
-----.

제23조의4(진료정보등 침해사고의 예방 및 대응 등) ① -----진료정보등 침해사고-----
-----.

1. 진료정보등 침해사고-----

2. 진료정보등 침해사고-----
3. 진료정보등 침해사고-----

4. 전자의무기록 또는 보건복지부령으로 정하는 전산시스템-----

5. -----진료정보등 침해사고-----

② 보건복지부장관은 제1항제3호에 따른 긴급조치를 실시하기 위하여 필요한 경우 관계 행정기관의 장에게 진료정보등 침해사고와 관련이 있는

<신 설> ② (생 략) ③ 제1항에 따른 업무를 수행하는데 필요한 절차 및 방법, 제2항에 따른 업무의 위탁 절차 등에 필요한 사항은 보건복지부령으로 정한다. 제92조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자에게는 300만원 이하의 과태료를 부과한다. 1. (생 략) 1의2. 제23조의3제1항을 위반하여 진료정보 침해사고를 통지하지 아니한 자 1의3. · 1의4. (생 략) 2. ~ 5. (생 략) ② ~ ④ (생 략)	인터넷주소(「인터넷주소자원에 관한 법률」 제2조제1호에 따른 인터넷주소를 말한다) 등 필요한 정보를 요청할 수 있다. 이 경우 요청을 받은 관계 행정기관의 장은 정당한 사유가 없으면 이에 응하여야 한다. ③ 보건복지부장관은 진료정보등 침해사고의 예방 및 대응을 위하여 의료기관에 행정적·재정적 지원을 할 수 있다. ④ (현행 제2항과 같음) ⑤ ----- -----제4항----- ----- -----. 제92조(과태료) ① ----- ----- -----. 1. (현행과 같음) 1의2. -----진료정보등 침해사고----- ----- 1의3. · 1의4. (현행과 같음) 2. ~ 5. (현행과 같음) ② ~ ④ (현행과 같음)
공포 후 6개월이 경과한 날	

2. 검토의견

1) 전자의무기록에 대한 기술적 보호조치 의무

□ 현행법 제23조제2항에 따라 의료인 또는 의료기관 개설자는 전자의무 기록을 안전하게 관리·보존하는데 필요한 시설과 장비를 갖추어야 함.¹⁾

이때 필요한 시설과 장비는 보건복지부령으로 정하도록 위임하고 있는데, 동법 시행규칙에서는 다음과 같이 정하고 있음.²⁾

<전자의무기록 관리·보존을 위한 시설과 장비>

「의료법 시행규칙」제16조제1항 각 호

1. 전자의무기록의 생성·저장과 전자서명을 검증할 수 있는 장비
2. 전자서명이 있은 후 전자의무기록의 변경 여부 확인 등 전자의무기록의 이력관리를 위하여 필요한 장비
3. 전자의무기록의 백업저장장비
4. 네트워크 보안에 관한 시설과 장비(제1호부터 제3호까지에 따른 장비가 유무선 인터넷과 연결된 경우에 한정한다)
5. 법 제23조의2제1항에 따른 전자의무기록시스템(이하 “전자의무기록시스템”이라 한다) 보안에 관한 시설과 장비
6. 전자의무기록 보존장소에 대한 다음 각 목의 어느 하나에 해당하는 물리적 접근 방지 시설과 장비
가. 출입통제구역 등 통제 시설
나. 잠금장치
7. 의료기관(법 제49조에 따라 부대사업을 하는 장소를 포함한다) 외의 장소에 제1호에 따른 전자의무기록의 저장장비 또는 제3호에 따른 백업저장장비를 설치하는 경우에는 다음 각 목의 시설과 장비
가. 전자의무기록 시스템의 동작 여부와 상태를 실시간으로 점검할 수 있는 시설과 장비
나. 전자의무기록 시스템에 장애가 발생한 경우 제1호 및 제2호에 따른 장비를 대체할 수 있는 예비 장비
다. 폐쇄회로 텔레비전 등의 감시 장비
라. 재해예방시설

- 1) 「의료법」 제23조(전자의무기록) ①의료인이나 의료기관 개설자는 제22조의 규정에도 불구하고 진료기록부등을 「전자서명법」에 따른 전자서명이 기재된 전자문서(이하 “전자의무기록”이라 한다)로 작성·보관할 수 있다.
② 의료인이나 의료기관 개설자는 보건복지부령으로 정하는 바에 따라 전자의무기록을 안전하게 관리·보존하는 데에 필요한 시설과 장비를 갖추어야 한다.
- 2) 「의료법 시행규칙」 제16조(전자의무기록의 관리·보존에 필요한 시설과 장비 등) ① 의료인이나 의료기관의 개설자는 법 제23조제2항에 따라 전자의무기록(電子醫務記錄)을 안전하게 관리·보존하기 위하여 다음 각 호의 시설과 장비를 갖추어야 한다. (각 호 생략)

□ 개정안은 이러한 시설과 장비를 갖추는 때, 전자의무기록의 불법 유출·위조·변조·삭제 등을 방지하기 위한 기술적 보호조치를 하도록 명시하려는 것으로 타당한 입법조치로 보임.

- 참고로, 현행 「의료법 시행규칙」 제16조에서는 제1항에서 전자의무기록 관리·보존을 위한 시설과 장비를 정하면서, 제3항에서 그 구체적인 사항은 보건복지부장관이 정하여 고시하도록 하고 있는데,³⁾ 이에 따른 ‘전자의무기록의 관리·보존에 필요한 시설과 장비에 관한 기준’(보건복지부고시)에서 ‘전자의무기록의 분실·도난·유출·위조·변조 또는 훼손 등의 사고를 대비할 수 있는 백업 저장장비’, ‘불법적인 접근 및 침해사고를 방지하기 위한 안전성 확보 조치’ 등을 규정하고 있음.⁴⁾

3) 「의료법 시행규칙」 제16조(전자의무기록의 관리·보존에 필요한 시설과 장비 등) ③ 제1항 각 호에 따라 갖추어야 하는 시설과 장비 및 제2항에 따른 접속 기록 보관에 관한 구체적인 사항은 보건복지부장관이 정하여 고시한다.

4) ‘전자의무기록의 관리·보존에 필요한 시설과 장비에 관한 기준’ (보건복지부고시 제2023-245호) 제5조(전자의무기록의 백업 저장장비) 전자의무기록 관리자는 전자의무기록의 분실·도난·유출·위조·변조 또는 훼손 등의 사고를 대비할 수 있도록 다음 각 호의 구분에 따른 장비와 장소를 확보하여야 한다.

1. 전자의무기록을 주기적으로 안전하게 백업할 수 있는 기능을 갖춘 백업 저장장비
2. 백업 저장장비에 대한 잠금장치가 구비된 보관장소

제6조(네트워크 및 전자의무기록 시스템 보안에 관한 시설과 장비 등) 전자의무기록 관리자는 불법적인 접근 및 침해사고를 방지하기 위하여 「의료법 시행규칙」(이하 "규칙"이라 한다) 제16조제1항제4호부터 제6호까지의 시설과 장비에 대하여 「개인정보보호법」 제29조에 따른 안전성 확보 조치를 하여야 한다. 이 경우 시설과 장비별 구체적인 조치는 다음 각 호의 구분에 따른다.

1. 규칙 제16조제1항제4호·제5호에 따른 시설 및 장비 : 「개인정보보호법 시행령」 제30조제1항제2호부터 제5호까지에 따른 안전성 확보 조치
2. 규칙 제16조제1항제6호에 따른 시설 및 장비 : 「개인정보보호법 시행령」 제30조제1항제6호에 따른 안전성 확보 조치

제7조(의료기관 외의 장소 관리·보존시 추가적인 조치) ① 전자의무기록 관리자가 의료기관 외의 장소에서 전자의무기록을 관리·보존하는 경우에는 규칙 제16조제1항제3호부터 제7호까지에 따른 시설과 장비에 대하여 별표1에 따른 추가적인 조치를 하여야 한다.

② 제1항에도 불구하고 다음 각 호의 어느 하나를 충족하는 클라우드컴퓨팅서비스를 이용하여 전자의무기록을 관리하는 자가 별표 2에 따른 조치를 하면 별표 1에 따른 조치를 한 것으로 간주한다.

1. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조에 따른 정보보호 관리체계 인증과 국제표준화기구 및 국제전기기술위원회(ISO/IEC)의 클라우드 서비스 정보보호 관리체계 인증을 받은 서비스
2. 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제23조제2항에 따른 클라우드컴퓨팅서비스의 정보보호에 관한 기준을 충족하는 서비스

- 특히 동 고시에서는 전자의무기록을 의료기관 외의 장소에서 관리·보존하는 경우 추가적인 조치를 하도록 관리를 강화하고 있음.

<의료기관 외의 장소에 전자의무기록 보관시 필요한 추가적인 조치>

구 분		세 부 조 치 내 용
1. 전자의무기록의 백업 저장장비	1.1. 시스템 무중단 백업	- 전자의무기록 등의 정보를 백업할 경우, 전자의무기록 시스템을 중단하지 않고 백업업무를 할 수 있도록 장비를 마련하여야 한다.
	1.2. 백업데이터 긴급복구	- 백업된 데이터는 필요시 신속하게 복구될 수 있도록 관련된 시스템 및 관리절차를 갖추어야 한다.
	1.3. 백업데이터 위.변조 방지	- 백업된 데이터의 위.변조 및 비정상적으로 삭제되지 않도록 백업데이터의 보호조치를 하여야 한다.
	1.4. 백업설비의 물리적 분리	- 백업을 위한 장비 및 시스템은 전자의무기록 시스템을 위한 장비 및 설비와 분리하여 운영되어야 한다.
2. 네트워크 보안에 관한 시설과 장비	2.1. 이중화된 네트워크의 구성	- 의료데이터 전송을 위한 이중화된 네트워크를 구성하여야 하며 아래 조건을 충족하여야 한다. .물리적 또는 그에 준하는(논리적 포함) 둘 이상의 회선 분리 .둘 이상의 경로를 제공하는 내부망 구성 .라우터의 이중화 구성 .장애발생 시에도 지속적인 서비스 제공 대책 수립
	2.2. 네트워크 보호시스템 운영	- 침입차단시스템, 침입탐지시스템 등 인증된 정보보호시스템을 운영하여 내.외부 네트워크를 보호하여야 한다.
3. 전자의무기록 시스템 보안에 관한 시설과 장비	3.1. 인증된 정보보호.보안제품의 사용	- 국가정보원장이 인증 필요성을 인정하는 정보보호시스템의 경우 CC 인증 제품 등 도입요건을 만족한 제품을 사용하여야 한다.
	3.2. 데이터 및 소프트웨어의 무결성 보장 및 암호화	- 전자의무기록 및 소프트웨어의 무결성을 확인하여야 하며, 데이터 처리에 대한 위변조 방지 등 보호기능을 제공하여야 한다. - 전자의무기록 시스템 운영을 통해 관리되고 있는 중요정보에 대해 암호화하여야 한다.
	3.3. 접근통제 강화를 위한 시스템의 구성 등	- 안전성 및 신뢰성 향상을 위해 필요한 외주개발 보안, 시스템 주기적 모니터링, 시각 동기화 등 기술적 보호조치를 위한 시스템(장비)을 구성하여야 한다. - 비인가자의 접근을 통제할 수 있도록 접근통제 영역 및 범위, 접근통제 규칙, 방법 등을 포함하여 접근통제 정책을 별도 수립하여야 한다.
	3.4. 데이터 관리방안 수립 및 모니터링	- 데이터 무결성을 보장하기 위한 보호조치 및 데이터변경에 대한 관리방안을 마련하고, 모니터링하여야 한다. - 데이터 훼손.유출이 발생한 경우, 이를 즉시 의료기관에 통보하여야 한다.
4. 전자의무기록 보존장소에 대한 물리적 접근방지 시설과 장비	4.1. 출입통제 구역의 설치	- 전자의무기록 시스템이 위치한 공간의 출입통제가 가능해야 한다. - 전자의무기록 시스템이 위치한 보호구역내에서의 작업 절차를 수립하고 작업에 대한 기록을 주기적으로 검토하여야 한다.
	4.2. 출입 통제 및 현황정보 모니터링	- 출입통제 및 이력관리 시스템을 갖추어 출입자(권한)별 감사기록을 생성, 저장하여야 하며, 출입통제시스템에 대한 접근통제 및 암호화 기능을 갖추어야 한다.
	4.3. 물리적 위치의 한정	- 전자의무기록 시스템 및 그 백업장비의 물리적 위치는 국내로 한정한다.

5. 전자의무기록시스템을 실시간으로 점검할 수 있는 시설과 장비	5.1. 전자의무기록 시스템 실시간 점검	- 전자의무기록시스템의 전산자원(H/W) 및 소프트웨어(프로그램)의 동작여부와 상태를 점검할 수 있는 장비를 갖추어, 이상이 발생한 경우 이를 기록하여 관리자에게 알려주어야 한다.
	5.2. 네트워크 시스템 모니터링	- 스위치.라우터 등 네트워크 장비에서 발생하는 트래픽을 기록하고 실시간으로 네트워크 상태를 점검할 수 있어야 한다.
6. 예비 장비	6.1. 보조시스템 운영	- 전자의무기록 시스템 장애 시 안정적인 서비스 제공을 보장할 수 있도록 보조서버가 작동.운영될 수 있어야 한다.
7. 폐쇄회로 텔레비전 등의 감시 장비	7.1. CCTV 설치운영	- 전자의무기록 관리시설은 사각지대 없이 24시간 CCTV 실시간 촬영(월단위 백업)이 되어야 한다. - CCTV 시스템에 대한 접근통제 정책을 마련하여야 한다.
	7.2. 외부 침입감지장치 설비 운영	- 아래 조건을 충족하는 침입감지장치를 설치 운영하여야 한다. .침입감지시 관리자에게 신속히 알리는 기능 .침입감지, 경보장치와 연결된 침입 발생위치 확인 기능
	7.3. 출입현황 정보의 확인	- 출입통제장치로부터 출입현황정보를 확인할 수 있는 장비를 갖추어야 한다. - 정당한 관리자만이 감사기록을 조회하고, 감사기록을 백업한다.
8. 재해예방 시설	8.1. 화재경보장치	- 화재발생에 대비하여 연기감지장치, 온도감지장치 등의 설비를 갖추어야 한다.
	8.2. 소화장치	- 소규모 및 대규모 화재에 대비한 소화장치를 구비하되, 시스템에 악영향을 미치지 않는 소화약제를 사용하여, 시스템의 오작동에 대처하여야 한다.
	8.3. 수재 예방설비	- 시스템 및 네트워크설비 등이 물에 노출되지 않도록 바닥으로부터 이격하여 설치하고 콘센트 등 전원접속장치는 바닥으로부터 이격하여 설치하여야 한다.
	8.4. 전원 공급시설	- 정전발생시 지속적인 업무의 수행이 가능하도록 추가연료보충 없이 2시간 이상 발전할 수 있는 자가발전설비, 30분이상 전원을 공급해 줄 수 있는 무정전 전원공급장치(UPS) 설비를 갖추어야 한다.
	8.5. 온도 및 습도 유지	- 온도 및 습도를 일정하게 유지하기 위한 항온.항습장비를 갖추어 시스템의 오작동에 대비할 수 있어야 한다.

□ 다만, 개정안에서의 ‘기술적 보호조치’에 대한 구체적인 기준을 하위 법령에 위임할 필요가 있는 것으로 보임. 참고로 현행법령에서 ‘기술적 보호조치’를 규정하고 있는 사례는 다음과 같음.

- 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제45조 제2항은 “과학기술정보통신부장관은 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치의 구체적 내용을 정한 정보보호조치에 관한 지침(이하

“정보보호지침”이라 한다)을 정하여 고시”할 수 있도록 하면서 제3항에서 정보보호지침에 다양한 기술적 보호조치를 포함하도록 규정하고 있음. 이에 따라 ‘정보보호조치에 관한 지침’(과학기술정보통신부고시)에서 관리적·기술적·물리적 보호조치의 구체적인 내용을 정하고 있음.[참고자료1]

- 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제23조는 “과학기술정보통신부장관은 클라우드컴퓨팅서비스의 품질·성능에 관한 기준 및 정보보호에 관한 기준(관리적·물리적·기술적 보호조치를 포함한다. 이하 “보안인증기준”이라 한다)을 정하여 고시”할 수 있도록 규정하고 있고, 동 고시에서 클라우드컴퓨팅서비스의 보안인증기준으로 ① 관리적 보호조치, ② 물리적 보호조치, ③ 기술적 보호조치를 각각 마련하고 있음.[참고자료2]
- 「지능정보화 기본법」 제59조는 “과학기술정보통신부장관은 초연결지능정보통신기반의 안전성·신뢰성에 관한 기준 및 정보보호에 관한 기준(관리적·물리적·기술적 보호조치를 포함한다)을 행정안전부장관 등 관계 기관의 장과 협의하여 고시”할 수 있도록 규정하고 있음.
- 「공직선거법」 제148조제5항은 “중앙선거관리위원회는 사전투표소에서 통합선거인명부를 사용하기 위한 선거전용통신망을 구축하여야 하며, 정보의 불법 유출·위조·변조·삭제 등을 방지하기 위한 기술적 보호조치를 하여야 한다”고 규정하고 있고, 제6항에서 사전투표소의 설치·공고·통보 및 사전투표사무원의 위촉, 그 밖에 필요한 사항은 중앙선거관리위원회규칙으로 정하도록 하위법령에 위임하고 있음.

2) '진료정보 침해사고'의 범위 확대

□ 현행법 제23조의3에 따라 의료기관은 전자의무기록시스템에 대한 '진료정보 침해사고'(정보 유출·손상, 전자의무기록시스템의 교란·마비 등)가 발생한 경우 보건복지부장관에게 즉시 통지해야 함(위반시 300만원이하의 과태료 부과).⁵⁾

□ 안 제23조의3은 침해사고 통지의무 대상의 범위를, 현행 '전자의무기록' 시스템뿐만 아니라 '보건복지부령으로 정하는 전산시스템'에 대한 침해까지 확대하면서, '진료정보 침해사고'의 용어를 '진료정보등 침해사고'로 변경하려는 것임.

보건복지부에 따르면 개정안에 따라 침해사고의 대상으로 확대될 수 있는 전산시스템으로는 의료영상저장정보시스템(CT·MRI·X-Ray 등), 검사정보시스템(진단검사·병리검사 등), 약제 관련 시스템, 원무·청구 등 환자관련 시스템, 임상연구 관련 시스템, 홈페이지 시스템 등이 있음.

전자의무기록시스템뿐만 아니라 검사·약제·청구 등 의료기관 내 다양한 전산시스템에 대한 해킹, 악성코드 감염, 랜섬웨어 등 정보

5) 「의료법」 제23조의3(진료정보 침해사고의 통지) ① 의료인 또는 의료기관 개설자는 전자의무기록에 대한 전자적 침해행위로 진료정보가 유출되거나 의료기관의 업무가 교란·마비되는 등 대통령령으로 정하는 사고(이하 "진료정보 침해사고"라 한다)가 발생한 때에는 보건복지부장관에게 즉시 그 사실을 통지하여야 한다.

「의료법 시행령」 제10조의9(진료정보 침해사고의 유형) ① 법 제23조의3제1항에서 "진료정보가 유출되거나 의료기관의 업무가 교란·마비되는 등 대통령령으로 정하는 사고"란 다음 각 호의 어느 하나에 해당하는 사고를 말한다.

1. 진료정보의 도난·유출
2. 진료정보의 파기·손상·은닉·멸실
3. 전자의무기록시스템의 교란·마비

「의료법」 제92조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자에게는 300만원 이하의 과태료를 부과한다.

1의2. 제23조의3제1항을 위반하여 진료정보 침해사고를 통지하지 아니한 자

통신망 공격으로도 개인정보가 유출되고 의료기관 업무가 교란될 수 있음을 고려할 때, 침해사고의 범위를 확대하여 그 예방·대응의 실효성을 높이고자 하는 것은 타당한 입법으로 보임.

- 참고로, 「의료법」과 유사하게 침해사고의 통지·대응 등에 관하여 규정하고 있는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하, ‘정보통신망법’), 「전자금융거래법」 등에서도 침해사고의 대상을 특정 시스템에 한정하지 않고, 각각 ‘정보통신망’, ‘전자금융기반시설’로 폭넓게 규정하고 있음.⁶⁾

- 또한 정보통신망법 제48조의3에 따라 정보통신서비스 제공자는 침해사고가 발생하면 즉시 그 사실을 과학기술정보통신부장관이나 한국인터넷진흥원에 신고하여야 할 의무가 있는데,⁷⁾ 이때

6) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조(정의) ① 이 법에서 사용하는 용어의 뜻은 다음과 같다.

7. “침해사고”란 다음 각 목의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위로 인하여 발생한 사태를 말한다.

가. 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스거부 또는 고출력 전자기파 등의 방법

나. 정보통신망의 정상적인 보호·인증 절차를 우회하여 정보통신망에 접근할 수 있도록 하는 프로그램이나 기술적 장치 등을 정보통신망 또는 이와 관련된 정보시스템에 설치하는 방법

「전자금융거래법」 제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.

21. “전자금융기반시설”이란 전자금융거래에 이용되는 정보처리시스템 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호에 따른 정보통신망을 말한다.

22. “전자적 침해행위”란 해킹, 컴퓨터 바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 전자금융기반시설을 공격하는 행위를 말한다

제21조의5(침해사고의 통지 등) ① 금융회사 및 전자금융업자는 전자적 침해행위로 인하여 전자금융기반시설이 교란·마비되는 등의 사고(이하 “침해사고”라 한다)가 발생한 때에는 금융위원회에 지체 없이 이를 알려야 한다.

「정보통신기반 보호법」 제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.

1. “정보통신기반시설”이라 함은 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호에 따른 정보통신망을 말한다.

2. “전자적 침해행위”란 다음 각 목의 방법으로 정보통신기반시설을 공격하는 행위를 말한다.

가. 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부 또는 고출력 전자기파 등의 방법

나. 정상적인 보호·인증 절차를 우회하여 정보통신기반시설에 접근할 수 있도록 하는 프로그램이나 기술적 장치 등을 정보통신기반시설에 설치하는 방법

3. “침해사고”란 전자적 침해행위로 인하여 발생한 사태를 말한다.

7) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제48조의3(침해사고의 신고 등) ① 정보통신서비스 제공자는 침해사고가 발생하면 즉시 그 사실을 과학기술정보통신부장관이나 한국인터넷진흥원에 신고하여야 한다. 이 경우 정보통신서비스 제공자가 이미 다른 법률에 따른 침해사고 통지 또는 신고를 했으면 전단에 따른 신고를 한 것으로 본다.

정보통신서비스 제공자는 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 포함하는 의미이며, 의료기관도 의료업을 위해 정보통신서비스를 제공한다면 정보통신서비스 제공자에 해당함. 따라서 현재도 일부 의료기관의 경우 정보통신망법상의 침해사고가 발생하면 과학기술정보통신부장관(한국인터넷진흥원)에게 신고할 의무가 있음.⁸⁾

- 다만, 진료정보 침해사고의 범위 확대 시 전산시스템 구축, 전문인력 확보 및 법적의무 추가에 따른 의료기관의 부담이 가중될 우려가 있다는 등의 이유로 개정안에 반대하는 의견도 있음.

3) 침해사고 긴급조치를 위한 정보제공 요청

- 현행법 제23조의4에 따라 보건복지부장관은 진료정보 침해사고의 예방 및 대응을 위하여 정보의 수집·전파·분석, 침해사고의 예보·경보 및 긴급조치 등의 업무를 수행함.⁹⁾

- 보건복지부장관은 현재 이러한 예방·대응 업무를 현행법 제23조의4제2항 및 동법 시행규칙 제16조의4에 따라 한국사회보장정보원(의료정보보호센터)에 위탁하여 수행하고 있음.¹⁰⁾

8) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조(정의) ① 이 법에서 사용하는 용어의 뜻은 다음과 같다.

3. “정보통신서비스 제공자”란 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다.

9) 「의료법」 제23조의4(진료정보 침해사고의 예방 및 대응 등) ① 보건복지부장관은 진료정보 침해사고의 예방 및 대응을 위하여 다음 각 호의 업무를 수행한다.

1. 진료정보 침해사고에 관한 정보의 수집·전파

2. 진료정보 침해사고의 예보·경보

3. 진료정보 침해사고에 대한 긴급조치

4. 전자의무기록에 대한 전자적 침해행위의 탐지·분석

5. 그 밖에 진료정보 침해사고 예방 및 대응을 위하여 대통령령으로 정하는 사항

□ 이 중 긴급조치는 ‘전자의무기록시스템에 대한 접속경로의 차단 요청’과 ‘침해사고 원인·경위 조사’를 말하는데,¹¹⁾ 개정안은 보건복지부장관이 긴급조치를 실시하기 위하여 필요한 경우 관계 행정기관의 장에게 진료정보등 침해사고와 관련이 있는 인터넷주소 등 필요한 정보를 요청할 수 있도록 하고, 이 경우 요청을 받은 관계 행정기관의 장은 정당한 사유가 없는 한 이에 따라야 할 의무를 부여하려는 것임.

현행 제23조의3제2항에 따르면,¹²⁾ 보건복지부장관은 침해사고를 통지받거나 알게 된 경우 관계 중앙행정기관인 과학기술정보통신부(한국인터넷진흥원)에 통보하게 되는데, 이때 과학기술정보통신부장관은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」¹³⁾에

10) 「의료법」 제23조의4(진료정보 침해사고의 예방 및 대응 등) ② 보건복지부장관은 제1항에 따른 업무의 전부 또는 일부를 전문기관에 위탁할 수 있다.

③ 제1항에 따른 업무를 수행하는 데 필요한 절차 및 방법, 제2항에 따른 업무의 위탁 절차 등에 필요한 사항은 보건복지부령으로 정한다.

「의료법 시행규칙」 제16조의4(진료정보 침해사고의 예방 및 대응을 위한 업무의 위탁) 보건복지부장관은 법 제23조의4제2항에 따라 같은 조 제1항 각 호에 따른 진료정보 침해사고의 예방 및 대응을 위한 업무를 「사회보장급여의 이용·제공 및 수급권자 발굴에 관한 법률」 제29조에 따른 한국사회보장정보원에 위탁한다.

11) 「의료법 시행규칙」 제16조의3(진료정보 침해사고에 대한 긴급조치) ① 보건복지부장관은 의료인, 의료기관 개설자 또는 관계 행정기관 등을 통해 진료정보 침해사고가 발생한 사실을 알게 된 경우 그 피해의 확산을 방지하기 위하여 법 제23조의4제1항제3호에 따라 다음 각 호의 조치를 할 수 있다.

1. 의료기관의 전자의무기록시스템에 대한 접속경로의 차단 요청

2. 진료정보 침해사고의 원인·경위 등에 관한 조사. 이 경우 현장조사에 관한 사항은 해당 의료기관의 장과 미리 협의해야 한다.

② 의료인 또는 의료기관의 개설자는 특별한 사유가 없으면 제1항에 따른 조치에 협조해야 한다.

12) 「의료법」 제23조의3(진료정보 침해사고의 통지) ② 보건복지부장관은 제1항에 따라 진료정보 침해사고의 통지를 받거나 진료정보 침해사고가 발생한 사실을 알게 되면 이를 관계 행정기관에 통보하여야 한다.

13) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제48조의4(침해사고의 원인 분석 등) ① 정보통신서비스 제공자 등 정보통신망을 운영하는 자는 침해사고가 발생하면 침해사고의 원인을 분석하고 피해의 확산을 방지하여야 한다.

② 과학기술정보통신부장관은 정보통신서비스 제공자의 정보통신망에 중대한 침해사고가 발생하면 피해 확산 방지, 사고대응, 복구 및 재발 방지를 위하여 정보보호에 전문성을 갖춘 민·관합동조사단을 구성하여 그 침해사고의 원인 분석을 할 수 있다.

③ 과학기술정보통신부장관은 제2항에 따른 침해사고의 원인을 분석하기 위하여 필요하다고 인정하면 정보통신서비스 제공자와 집적정보통신시설 사업자에게 정보통신망의 접속기록 등 관련 자료의 보존을 명할 수 있다.

근거하여 원인분석을 위하여 정보통신망의 접속기록 등을 제출받거나 직접 출입조사할 수 있는 등의 권한이 있음.

따라서 개정안에 따를 경우 보건복지부장관은 접속차단 요청 등 긴급조치에 필요한 정보를 관계 행정기관인 과학기술정보통신부로부터 확보할 수 있을 것으로 기대됨.

- 유사입법례로 「전자금융거래법」 제21조의6 및 동법 시행령 제11조의6제2항에서, 금융위원회가 전자금융기반시설의 침해사고에 대응하기 위하여 필요한 경우, 관계 행정기관 등에 관련 정보제공 등의 협조를 요청할 수 있다고 규정하고 있음.¹⁴⁾

④ 과학기술정보통신부장관은 침해사고의 원인을 분석하기 위하여 필요하면 정보통신서비스 제공자와 집적정보통신시설 사업자에게 침해사고 관련 자료의 제출을 요구할 수 있으며, 제2항에 따른 민·관합동조사단에게 관계인의 사업장에 출입하여 침해사고 원인을 조사하도록 할 수 있다. 다만, 「통신비밀보호법」 제2조제11호에 따른 통신사실확인자료에 해당하는 자료의 제출은 같은 법으로 정하는 바에 따른다.

⑤ 과학기술정보통신부장관이나 민·관합동조사단은 제4항에 따라 제출받은 자료와 조사를 통하여 알게 된 정보를 침해사고의 원인 분석 및 대책 마련 외의 목적으로는 사용하지 못하며, 원인 분석이 끝난 후에는 즉시 파기하여야 한다.

⑥ 제2항에 따른 민·관합동조사단의 구성과 제4항에 따라 제출된 침해사고 관련 자료의 보호 등에 필요한 사항은 대통령령으로 정한다.

14) 「전자금융거래법」 제21조의6(침해사고의 대응) ① 금융위원회는 침해사고에 대응하기 위하여 다음 각 호의 업무를 수행한다.

1. 침해사고에 관한 정보의 수집·전파
2. 침해사고의 예보·경보
3. 침해사고에 대한 긴급조치
4. 그 밖에 침해사고 대응을 위하여 대통령령으로 정하는 사항

② 제1항에 따른 업무를 수행하는 데 필요한 절차·방법 등은 대통령령으로 정한다.

「전자금융거래법 시행령」 제11조의7(침해사고 대응을 위한 금융위원회의 업무 등) ② 금융위원회는 법 제21조의6제1항에 따른 업무를 수행하기 위하여 필요한 경우 관계 행정기관 등에 관련 정보제공 등의 협조를 요청할 수 있다.

3. 관계 부처 및 관련 단체 의견

1) 보건복지부(수정)

- 국민의 생명과 안전을 위협하는 사이버 침해사고로부터 안전하게 의료정보를 보호하고, 침해사고의 예방 및 대응의 실효성을 제고하고자 하는 입법취지에 공감함.
- 다만, 침해사고 신고대상 확대에 따른 의료기관 안내, 사고대응 인력 및 체계마련, 관련 행정기관 업무 협의 등을 위해 시행일을 공포 후 1년으로 수정할 필요가 있음.

2) 대한의사협회(신중검토)

- 동 개정안에 따라 진료정보 침해사고의 범위를 확대(전산시스템 추가)할 경우 의료기관의 전산시스템 구축에 따른 비용 발생, 전문 인력 확보에 따른 어려움과 의료기관의 법적 의무에 따른 행정 부담이 가중될 것임.
- 의료기관에 대한 규제 강화가 아닌, 정부 주도의 의료 데이터 보호 및 해킹 대응정책 강화가 선행되어야 할 것임.
 - 특히, 보건복지부와 한국사회보장정보원에서 ‘의료정보보호센터’를 운영·유지하고 있는바, 의료기관의 전자적 침해 예방을 위하여 동 센터를 통한 적극적인 홍보와 다양한 정보 침해사고에 대한 대응 서비스를 강화해야 할 것임.

3) 대한치과의사협회(반대)

- 진료정보 침해사고는 의무 미이행에 대한 고의, 주의의무 위반 및 과실과 진료정보 침해사고 결과의 인과관계를 입증해 내는 것이 현실적으로 매우 어려워, 자칫 의료기관을 운영하는 치과의사들에게 피해가 발생할 수 있음.
- 특히, 치과의원에서 정보유출 사고가 발생할 경우 치과의사는 피해자인 동시에 피의자가 될 우려가 높고, 법률의 가능성과 한계를 고려할 필요가 있어, 법률개정보다 실효적인 방안을 강구해야 할 것으로 보임.

4) 대한간호조무사협회(찬성)

- 최근 국내 산부인과 진료실 등의 민감한 의료기관 영상이 중국 음란 사이트에 유출되는 등 전국 의료기관에서 220건에 달하는 해킹과 같은 사이버 침해사고가 발생함.
- 이에 진료정보 침해사고의 범위를 의료기관 EMR 외에도 영상정보시스템, 검사정보시스템까지 범위를 넓히고자 하는 본 개정안의 취지에 공감하며, 개정안은 환자의 생명과 밀접하게 연관되어 있는 정보를 안전하게 관리하여, 의료시스템 보안을 전반적으로 강화할 수 있을 것으로 사료됨.

5) 한국환자단체연합회(찬성)

- 개정안은 전자의무기록 외에 전자시스템에 대한 전자적 침해행위로 환자의 정보가 유출된 경우에도 진료정보 침해사고로 관리 할 수 있도록 범위를 확대하여 환자 정보 침해사고 예방 및 대응 실효성을 제고하고 환자의 비밀을 보호받을 권리를 보장하고자 하는 것으로, 이에 찬성함.

문 의 처
02)6788-5494

[참고자료 1]

<정보보호조치에 관한 지침 상 보호조치의 구체적인 내용>

구 분			세 부 조 치 사 항
1. 관 리 적 보 호 조 치	1.1. 정보보호 조직의 구성.운영	1.1.1. 정보보호조직 의 구성	▶ 정보보호 최고책임자, 정보보호관리자, 정보보호담당자로 구성된 정보보호조직을 운영
		1.1.2. 정보보호 최고 책임자의 지정	▶ 기업의 정보보호를 책임지는 이사 이상의 상근임원으로 지정
		1.1.3. 정보보호조직 구성원의 역할	▶ 정보보호 최고책임자는 정보보호 업무와 조직을 총괄 지휘 ▶ 정보보호관리자는 정보보호 업무의 실무를 총괄하고 관리 ▶ 정보보호담당자는 정보보호 업무의 분야별 실무를 담당
	1.2. 정보보호 계획 등의 수립 및 관리	1.2.1. 정보보호 방침의 수립.이행	▶ 정보보호 목표, 범위, 책임 등을 포함한 정보보호 방침(policy) 수립 ▶ 정보통신서비스와 관련된 모든 법, 규제, 계약, 정책, 기술상의 요구사항을 문서화하고 시행
		1.2.2. 정보보호 실행계획의 수립.이행	▶ 정보보호 방침을 토대로 예산, 일정 등을 포함한 당해 연도의 정보보호 실행계획을 수립 ▶ 최고경영층이 실행계획을 승인하고 정보보호 최고책임자가 추진 상황을 매 반기마다 점검
		1.2.3. 정보보호 실무지침의 마련.준수	▶ 정보통신설비 및 시설에 대한 관리적.기술적.물리적 보호조치의 구체적인 시행 방법.절차 등을 규정한 정보보호 실무지침을 마련 ▶ 정보보호 최고책임자가 실무지침을 승인하고 관련 법.제도, 설비의 교체 등 변경사유가 발생할 경우 보완하여 관리
		1.2.4. 정보보호 사전점검	▶ 새로운 정보통신망을 구축하거나 정보통신서비스를 제공하고자 하는 때에는 그 계획, 설계, 구현, 테스트 등에서 정보보호에 관한 사항을 고려
	1.3. 인적 보안	1.3.1. 내부인력 보안	▶ 임직원의 전보 또는 퇴직시 즉시 관련 계정 등에 대한 접근 권한을 제거 ▶ 임직원에게 정보보호 인식을 제고할 수 있는 홍보(정보보호 실천수칙 보급 등)를 실시 ▶ 정보보호조직의 구성원 및 정보보호와 관련된 업무에 종사하는 자에게 정기적으로 정보보호 교육 실시
			▶ 자사 직원이 아닌 자를 업무에 활용할 경우 보안서약을 징구
		1.3.3. 위탁운영 보안	▶ 전산업무를 외부에 위탁할 경우 보안계약서 또는 서비스수준 협약 등에 '정보보호에 관한 위탁업체의 책임범위', '위탁업무 중단에 따른 비상대책' 등을 반영
	1.4. 이용자 보호	1.4.1. 정보보호 정보 제공	▶ 이용자에게 침해사고 예.경보, 보안취약점, 계정.비밀번호 관리방안 등의 정보를 지속적으로 제공
		1.4.2. 정보보호 현황 공개	▶ 정보보호 투자 및 인력 현황, 정보보호 관련 인증 등 정보보호 현황을 자사 홈페이지 등에 공개

구 분			세 부 조 치 사 항
	1.5. 침해사고 대응	1.5.1. 침해사고 대응 계획의 수립.이행	▶ 침해사고 정의 및 범위, 대응체계(보고 및 조치 체계), 대응 방법 및 절차, 복구 방법 및 절차, 증거자료 수집 및 보관 등을 포함한 침해사고 대응계획을 마련.시행
	1.6. 정보보호 조치 점검	1.6.1. 정보보호조치 의 자체 점검	▶ 정보보호관리자는 매년 정보보호조치 및 정보보호 실무지침의 기준에 따라 자체적으로 정보보호 현황을 점검
	1.7. 정보자산 관리	1.7.1. 정보통신설비 및 시설의 현황 관리	▶ 정보통신망 구성도를 마련하고 변경사항이 있을 경우 보완.관 리 ▶ 정보통신설비, 시설의 목록(용도 및 위치 등 포함) 작성 및 네트워크와 분리된 환경에서 안전하게 관리
	1.8. 정보보호 투자	1.8.1. 정보보호 투자계획 수립.이행	▶ 기업의 정보보호를 위해 위험관리에 기반한 적정 수준(정보기술 부문 예산의 5%이상)의 정보보호 예산 편성 및 집행
2. 기 술 적 보 호 조 치	2.1. 네트워크 보안	2.1.1. 트래픽 모니터링	▶ 네트워크 모니터링 도구를 이용하여 백본망, 주요노드 및 외부망과 연계되는 주요회선의 트래픽 소통량을 24시간 모니터 링
		2.1.2. 무선서비스 보안	▶ 무선랜서비스, 무선인터넷서비스를 제공할 경우에는 사용자인증, 데이터암호화 등 보안조치를 마련
		2.1.3. 정보보호시스 템 설치.운영	▶ 외부망과 연계되는 구간에 침입차단시스템, 침입탐지시스템 등 네트워크의 안전성을 제고할 수 있는 정보보호시스템을 설치. 운영
		2.1.4. 정보보호를 위한 모니터링	▶ 주요시스템.네트워크 사용 및 접근이 명확하게 허용된 범위 안에 있는지를 확인하기 위한 모니터링 시스템 구축 또는 위탁 운영을 통하여 침해사고 탐지.대응 체계 운영
	2.2. 정보통신 설비 보안	2.2.1. 웹서버 보안	▶ 외부에 서비스를 제공하는 웹서버는 단독서버로 운영하고 DMZ에 설치
		2.2.2. DNS서버 보안	▶ 과부하에 대비한 부하분산 대책을 마련 ▶ 설정파일 백업 실시
		2.2.3. DHCP서버 보안	▶ 과부하에 대비한 부하분산 대책을 마련 ▶ 설정파일 백업 실시 ▶ IP 할당 상황 등에 대한 로그기록 유지.관리
		2.2.4. DB서버 보안	▶ 내부망에 설치 ▶ 외부망에서 직접 접속할 수 없도록 네트워크를 구성
		2.2.5. 라우터/스위치 보안	▶ ACL(Access Control List) 등의 접근제어 기능을 적용할 수 있는 설비를 사용
		2.2.6. 정보보호시스 템 보안	▶ 이상징후 탐지를 알리는 경고 기능을 설정하여 운영 ▶ 정보보호시스템 보안기능(비정상 트래픽 차단 등)의 정상 작동 여부를 주기적으로 점검(월 1회 이상)
		2.2.7. 취약점 점검	▶ 연 1회 이상 취약점 점검을 실시하고 발견된 취약점을 보완

구 분			세 부 조 치 사 항
		2.2.8. 접근통제 및 보안설정 관리	▶ 인가된 자만 시스템에 접속할 수 있도록 설정하고, 인터넷 등을 통해 외부에서 접속할 경우 일회용 패스워드 사용 등 인가 절차를 강화 ▶ 불필요한 프로토콜 및 서비스 제거 등 보안설정
		2.2.9. 관리자 계정의 비밀번호 관리	▶ 관리자 계정의 비밀번호는 8자리 이상으로 설정. 단, 설정 가능한 자리수가 8자리 미만일 때는 설정 가능한 최대의 자리수로 설정 ▶ 최소 3개월에 1회 이상 비밀번호 변경
		2.2.10. 로그 관리	▶ 최소 1개월 이상 로그기록 유지.관리(정보보호시스템은 3개월)
		2.2.11. 보안패치 관리	▶ 보안패치 정보를 주기적으로 입수하고 적용 ▶ 주요 보안패치에 대해서는 적용일 등 패치정보를 기록.관리
		2.2.12. 백업 및 복구	▶ 주요정보를 주기적으로 백업 ▶ 백업 담당자, 백업 및 복구 방법.절차.주기 등을 기록.관리
		2.2.13. 중요정보의 암호화	▶ 비밀번호는 복호화 되지 않도록 일방향 암호화하여 저장 ▶ 주민등록번호, 신용카드번호 및 계좌번호, 정보자산현황 등은 안전한 암호알고리즘으로 암호화하여 저장
		2.2.14. 관리용 단말 보안	▶ 일반적인 업무 및 개인적인 용도의 사용을 금지하고 DB서버, 웹서버 등 주요 정보통신설비의 접속에만 사용 ▶ 전용 또는 인터넷과 격리된 환경(필요시 접근통제 정책을 수립하고 제한적 접속 허용)에서 인가된 이용자만 이용할 수 있도록 통제 ▶ 관리용 단말로의 외부접속 차단, 주기적 보안패치 및 악성 소프트웨어 예방.탐지 활동 실시
3. 물 리 적 보 호 조 치	3.1. 출입 및 접근 보안	3.1.1. 정보통신시설 의 출입.접근 통제	▶ 비인가자가 출입할 수 없도록 잠금장치를 설치 ▶ 출입자의 기록을 1개월 이상 유지.보관
	3.2. 부대설비 및 시설 운영.관리	3.2.1. 백업설비 및 시설 설치.운영	▶ 주요정보를 백업하여 보관할 수 있는 백업설비 및 시설을 설치.운영

[참고자료2]

<클라우드컴퓨팅서비스 보안인증에 관한 고시 상 기술적 보호조치>

구 분			세 부 조 치 사 항
9. 가상화 보안	9.1. 가상화 인프라	9.1.1. 가상자원 관리	가상자원(가상 머신, 가상 스토리지, 가상 소프트웨어 등)의 생성, 변경, 회수 등에 대한 관리 방안을 수립하여야 한다.
		9.1.2. 가상자원 회수	이용자와의 계약 종료 시 가상자원 회수 절차에 따라 백업을 포함한 모든 클라우드 시스템에서 삭제하여야 한다.
		9.1.3. 가상자원 모니터링	가상자원에 대한 무결성 보장하기 위한 보호조치 및 가상자원의 변경(수정, 이동, 삭제, 복사)에 대해 모니터링 하여야 한다. 또한, 가상자원에 손상이 발생한 경우 이를 이용자에게 알려주어야 한다.
		9.1.4. 하이퍼바이저 보안	가상자원을 관리하는 하이퍼바이저의 기능 및 인터페이스에 대한 접근 통제 방안을 마련하여야 한다. 또한 하이퍼바이저에 대한 소프트웨어 업데이트 및 보안패치를 최신으로 유지하여야 한다.
		9.1.5. 공개서버 보안	가상자원을 제공하기 위한 웹사이트와 가상소프트웨어(앱, 응용프로그램)를 배포하기 위한 공개서버에 대한 물리적, 기술적 보호대책을 수립하여야 한다.
		9.1.6. 상호 운용성 및 이식성	클라우드컴퓨팅서비스 제공자는 표준화된 가상화 포맷, 이식성이 높은 가상화 플랫폼, 공개 API 등을 이용하여 클라우드컴퓨팅서비스 간의 상호 운용성 및 이식성을 높여야 한다.
	9.2. 가상 환경	9.2.1. 악성코드 통제	바이러스, 웜, 트로이목마 등의 악성코드로부터 이용자의 가상 환경(가상PC, 가상 서버, 가상 소프트웨어 등)을 보호하기 위한 악성코드 탐지, 차단 등의 보안기술을 지원하여야 한다. 또한 이상 징후 발견 시 이용자 통지하고 사용 중지 및 격리 조치를 수행하여야 한다.
		9.2.2. 인터페이스 및 API 보안	가상 환경(가상PC, 가상 서버, 가상 소프트웨어 등) 접근을 위한 인터페이스 및 API에 대한 보안 취약점을 주기적으로 분석하고, 이에 대한 보호방안을 마련하여야 한다.
		9.2.3. 데이터 이전	이용자가 기존 정보시스템 환경에서 클라우드컴퓨팅서비스의 가상 환경으로 전환 시 안전하게 데이터를 이전하도록 암호화 등의 기술적인 조치방안을 제공하여야 한다.
		9.2.4. 가상 소프트웨어 보안	클라우드컴퓨팅서비스 제공자는 출처, 유통경로 및 제작자가 명확한 소프트웨어로 구성된 가상환경을 제공하여야 한다.
10. 접근 통제	10.1. 접근통제 정책	10.1.1. 접근통제 정책 수립	비인가자의 접근을 통제할 수 있도록 접근통제 영역 및 범위, 접근통제 규칙, 방법 등을 포함하여 접근통제 정책을 수립하여야 한다.
		10.1.2. 접근기록 관리	접근기록 대상을 정의하고 서비스 통제, 관리, 사고 발생 책임 추적성 등을 보장할 수 있는 형태로 기록되고 유지하여야 한다.
10. 접근 통제	10.2. 접근 권한 관리	10.2.1. 사용자 등록 및 권한부여	클라우드 시스템 및 중요정보에 대한 접근을 통제하기 위하여 공식적인 사용자 등록 및 해지 절차를 수립하고 업무 필요성에 따라 사용자 접근권한을 최소한으로 부여하여야 한다.
		10.2.2. 관리자 및	클라우드 시스템 및 중요정보 관리 및 특수 목적을 위해 부여한 계정 및 권한을 식별하고 별도 통제하여야 한다.

구 분			세 부 조 치 사 항
		특수 권한관리	
		10.2.3. 접근권한 검토	클라우드 시스템 및 중요정보에 대한 접근을 관리하기 위하여 접근권한 부여, 이용(장기간 미사용), 변경(퇴직 및 휴직, 직무변경, 부서변경)의 적정성 여부를 정기적으로 점검하여야 한다.
	10.3. 사용자 식별 및 인증	10.3.1. 사용자 식별	클라우드 시스템에서 사용자를 유일하게 구분할 수 있는 식별자를 할당하고 추측 가능한 식별자 사용을 제한하여야 한다. 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하고 책임자의 승인을 받아야 한다.
		10.3.2. 사용자 인증	클라우드 시스템에 대한 접근은 사용자 인증, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증 절차에 의해 통제하여야 한다.
		10.3.3. 강화된 인증 수단 제공	이용자가 클라우드컴퓨팅서비스에 대해 다중 요소 인증 등 강화된 인증 수단을 요청하는 경우 이를 제공하기 위한 방안을 마련하여야 한다.
		10.3.4. 패스워드 관리	법적 요구사항, 외부 위협요인 등을 고려하여 패스워드 복잡도 기준, 초기 패스워드 변경, 변경 주기 등 사용자 및 이용자 패스워드 관리 절차를 수립·이행하고 패스워드 관리 책임이 사용자 및 이용자에게 있음을 주지시켜야 한다. 특히 관리자 패스워드는 별도 보호대책을 수립하여 관리하고, 이용자 패스워드 관리절차는 공지하여야 한다.
11. 네트워크 보안	11.1. 네트워크 보안	11.1.1. 네트워크 보안 정책 수립	클라우드컴퓨팅서비스와 관련된 내·외부 네트워크에 대해 보안 정책과 절차를 수립하여야 한다.
		11.1.2. 네트워크 모니터링 및 통제	DDoS, 비인가 접속 등으로 인한 서비스 중단 및 중요 정보 유출 등을 막기 위해 네트워크를 모니터링하고 통제하여야 한다.
		11.1.3. 네트워크 정보보호시스템 운영	클라우드컴퓨팅서비스와 관련된 내·외부 네트워크를 보호하기 위하여 정보보호시스템(방화벽, IPS, IDS, VPN 등)을 운영하여야 한다.
		11.1.4. 네트워크 암호화	클라우드 시스템에서 중요정보가 이동하는 구간에 대해서는 암호화된 통신채널을 사용하여야 한다.
		11.1.5. 네트워크 분리	클라우드컴퓨팅서비스 제공자의 관리 영역과 이용자의 서비스 영역, 이용자 간 서비스 영역의 네트워크 접근은 물리적 또는 논리적으로 분리하여야 한다.
		11.1.6. 무선 접근통제	클라우드 시스템은 무선망과 분리하고, 무선접속에 대한 접근을 통제하여야 한다. 무선접속을 사용하는 경우 그 사유와 타당성을 검토하고 책임자의 승인을 받아야 한다.
12. 데이터 보호 및	12.1. 데이터 보호	12.1.1. 데이터 분류	데이터 유형, 법적 요구사항, 민감도 및 중요도에 따라 데이터를 분류하고 관리하여야 한다.
		12.1.2. 데이터 소유권	이용자와 서비스 수준 협약 단계에서 데이터의 소유권을 명확하게 확립하여야 한다.
		12.1.3. 데이터 무결성	입·출력, 전송 또는 데이터 교환 및 저장소의 데이터에 대해 항상 데이터 무결성을 확인하여야 한다.

구 분		세 부 조 치 사 항		
암 호 화		12.1.4. 데이터 보호	데이터에 대한 접근제어, 위·변조 방지 등 데이터 처리에 대한 보호 기능을 이용자에게 제공하여야 한다.	
		12.1.5. 데이터 추적성	이용자에게 데이터를 추적하기 위한 방안을 제공하고, 이용자가 요구하는 경우 구체적인 제공정보(이용자의 정보가 저장되는 국가의 명칭 등)를 공개하여야 한다.	
		12.1.6. 데이터 폐기	클라우드컴퓨팅서비스 종료, 이전 등에 따른 데이터 폐기 조치 시 이용자와 관련된 모든 데이터를 폐기하여야 하며, 폐기된 데이터를 복구할 수 없도록 삭제 방안을 마련하여야 한다.	
	12.2. 매체 보안	12.2.1. 저장매체 관리	중요정보를 담고 있는 하드디스크, 스토리지 등의 저장매체 폐기 및 재사용 절차를 수립하고 매체에 기록된 중요정보는 복구 불가능하도록 완전히 삭제하여야 한다.	
		12.2.2. 이동매체 관리	중요정보 유출을 예방하기 위해 외장하드, USB, CD 등 이동매체 취급, 보관, 폐기, 재사용에 대한 절차를 수립하여야 한다. 또한 매체를 통한 악성코드 감염 방지 대책을 마련하여야 한다.	
	12.3. 암호화	12.3.1. 암호 정책 수립	클라우드컴퓨팅서비스에 저장 또는 전송 중인 데이터를 보호하기 위해 암호화 대상, 암호 강도(복잡도), 키관리, 암호 사용에 대한 정책을 마련하여야 한다. 또한 정책에는 개인정보 저장 및 전송 시 암호화 적용 등 암호화 관련 법적 요구사항을 반드시 반영하여야 한다.	
클라우드컴퓨팅서비스에 저장 또는 전송 중인 데이터를 보호하기 위해 암호화 대상, 암호 강도(복잡도), 키관리, 암호 사용에 대한 정책을 마련하여야 한다.				
12.3.2. 암호키 관리		암호키 생성, 이용, 보관, 배포, 파기에 관한 안전한 절차를 수립하고, 암호키는 별도의 안전한 장소에 보관하여야 한다.		
13. 시 스 템 개 발 및 도 입 보 안	13.1. 시스템 분석 및 설계	13.1.1. 보안요구 사항 정의	신규 시스템 개발 및 기존 시스템 변경 시 정보보호 관련 법적 요구사항, 최신 보안취약점, 정보보호 기본요소(기밀성, 무결성, 가용성) 등을 고려하여 보안요구사항을 명확히 정의하고 이를 적용하여야 한다.	
		13.1.2. 인증 및 암호화 기능	클라우드 시스템 설계 시 사용자 인증에 관한 보안요구사항을 반드시 고려하여야 하며 중요정보의 입·출력 및 송수신 과정에서 무결성, 기밀성이 요구될 경우 법적 요구사항을 고려하여야 한다.	
		13.1.3. 보안로그 기능	클라우드 시스템 설계 시 사용자의 인증, 권한 변경, 중요정보 이용 및 유출 등에 대한 감사증적을 확보할 수 있도록 하여야 한다.	
		13.1.4. 접근권한 기능	클라우드 시스템 설계 시 업무의 목적 및 중요도에 따라 접근권한을 부여할 수 있도록 하여야 한다.	
		13.1.5. 시각 동기화	로그기록의 정확성을 보장하고 법적인 자료로서 효력을 지니기 위해 클라우드 시스템 시각을 공식 표준시각으로 정확하게 동기화 하여야 한다. 또한 서비스 이용자에게 시각 정보 동기화 기능을 제공하여 한다.	
	13.2. 구현 및 시험	13.2.1. 구현 및 시험	안전한 코딩방법에 따라 클라우드 시스템을 구현 하고, 분석 및 설계 과정에서 도출한 보안요구사항이 정보시스템에 적용되었는지 확인하기 위하여 시험을 수행하여야 한다.	
		13.2.2. 개발과 운영환경 분리	개발 및 시험 시스템은 운영시스템에 대한 비인가 접근 및 변경의 위험을 감소하기 위해 원칙적으로 분리하여야 한다. 단 분리하여 운영하기 어려운 경우 그 사유와 타당성을 검토하고 안전성 확보 방안을 마련하여야 한다.	

구 분		세 부 조 치 사 항
	13.2.3. 시험 데이터 보안	시스템 시험 과정에서 운영데이터 유출을 예방하기 위해 시험데이터 생성, 이용 및 관리, 파기, 기술적 보호조치에 관한 절차를 수립하여 이행하여야 한다.
	13.2.4. 소스 프로그램 보안	소스 프로그램에 대한 변경관리를 수행하고 인가된 사용자만이 소스 프로그램에 접근할 수 있도록 통제절차를 수립하여 이행하여야 한다. 또한 소스 프로그램은 운영환경에 보관하지 않는 것을 원칙으로 한다.
13.3. 외주 개발 보안	13.3.1. 외주 개발 보안	클라우드 시스템 개발을 외주 위탁하는 경우 분석 및 설계단계에서 구현 및 이관까지의 준수해야 할 보안요구사항을 계약서에 명시하고 이행여부를 관리·감독하여야 한다.
13.4. 시스템 도입 보안	13.4.1. 시스템 도입 계획	클라우드 시스템의 처리 속도와 용량에 대하여 주기적인 모니터링을 수행하고 안정성의 확보에 필요한 시스템 도입 계획을 수립하여야 한다.
	13.4.2. 시스템 인수	새로 도입되는 시스템에 대한 인수 기준이 수립되어야 하며, 인수 전에 테스트가 수행되어야 한다.