개 인 정 보 보 호 위 원 회
제 2 소 위 원 회
심의·의결

안 건 번 호 제2025-214-313호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 이화의대부속서울병원 (사업자등록번호 :)

대표자

의결연월일 2025. 7. 23.

주 문

1. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 1,200,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

2. 피심인의 법 위반행위에 따른 행정처분의 내용 및 결과를 개인정보보호위원회 홈페이지에 1년간 공표한다.

이 유

Ⅰ. 기초 사실

피심인은 환자진료정보 등 개인정보를 처리하는 「舊 개인정보 보호법」[1](이하 '舊 보호법')에 따른 개인정보처리자이며, 일반현황은 다음과 같다.

< 피심인의 일반현황 >

피심인명	사업자등록번호 (법인등록번호)	대표자	상시 종업원수	자본금	매출액('22년)
이화의대 부속서울병원					

Ⅱ. 사실조사 결과

1. 조사 배경

개인정보보호위원회는 이화의대부속서울병원(이하 '이대서울병원')의 개인정보 유출신고(′23.8.22.)에 따라 개인정보보호 법규 위반 여부를 조사하였으며, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

이대서울병원 에서는 를 위한 을 운영하면서 '23.8.3. 기준으로 다음과 같이 정보주체의 개인정보를 수집하고 있다.

< 개인정보 수집현황 >

구분	항목	수집일	건수

나. 개인정보 유출 관련 사실관계

1) 법률 제16930호, 2020. 2. 4. 일부개정, 2020. 8. 5. 시행

이대서울병원은 새로운 장비 도입(’22.9.2.) 당시 방화벽을 구축하면서 원격 접속 기능( )을 활성화하였는데, 해커는 해당 방화벽의 취약점*을 이용하여 에 원격 접속 후 환자정보가 포함된 DB 파일을 유출(’23.8.3.)하여 이를 다크웹에 공개(’23.8.19.)하였다.

* CVE-2023-27997(원격코드 실행 취약점) : 웹에 노출된 해당 방화벽( )의 IP와 SSL-VPN 인터페이스(방화벽 버전과 시리얼 넘버)를 통해 원격으로 코드를 실행할 수 있는 취약점(심각도 : 9.2/10.0)으로 ‘23.6.12. 방화벽 제조사( ) 및 KISA에서 취약점 경고 및 강화된 보안 패치 제공

유출 당시 시스템 관련 방화벽은 외부로 전송되는 통신을 별도 제한 없이 모든 IP, Port가 허용*(Accept All)되도록 정책이 구성되었고, 방화벽 로그는 기록되고 있지 않은 상태였다.

* 제조사 매뉴얼에 일부 IP, Port, 외부 URL만 허용하도록 요구되었으나 해당 정책이 방화벽에 제대로 적용되지 않음

1) (유출 내용) 환자 1,535명의 민감정보 등 개인정보*

* 영문성명 및 환자등록번호(1,535명), 성별(1,492명), 생년월일(1,217명), 치료부위(1,534명)

2) 유출 인지 및 대응

이대서울병원은 유출 인지 전 의 랜섬웨어 감염을 확인(’23.8.3.)하고, 제조사에 지원을 요청하여 방화벽의 취약점 관련 조치를 완료(’23.8.7.)하였다.

이후 제조사는 해커 집단의 협박메일을 미국본사로부터 전달받아(’23.8.18.) 이대서울병원에 전달하였고(’23.8.18.), 다크웹에 게시된 DB 파일을 확인 및 분석한 결과 해당 자료가 이대서울병원 환자정보임을 인지(’23.8.22.)하였다.

또한, 유출 인지(’23.8.22.) 후 유출 통지 기간(5일) 이내에 개인정보가 유출된 환자들에게 유출통지 및 홈페이지를 통하여 유출사실을 공지(’23.8.25.)하였다.

3. 개인정보의 취급·운영 관련 사실관계

가. 민감정보의 안전성 확보에 필요한 조치를 소홀히 한 행위

이대서울병원은 새로운 장비를 도입(’22.9.2.)하던 당시 방화벽을 구축하면서 원격 접속 기능( )을 활성화하도록 방화벽 정책을 구성하였는데, 이후 불필요한 원격 접속 기능이 계속 활성화되어 있었음에도 이를 점검하지 않았고,

원격 접속 기능을 통한 미상의 접속기록이 있었음에도 IP주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지, 대응 동의 조치와 접근 통제가 이루어지지 않았다.

또한, 유출 사고 발생 시점으로부터 1년 이내에 방화벽 정책을 업데이트한 이력이 없고, 특히 방화벽 제조사에서 강화된 보안 패치를 제공(’23.6.8.)하고, 방화벽 제조사 및 한국인터넷진흥원에서 해당 방화벽 버전의 원격 접속 기능에 대한 취약점을 경고(’23.6.12.)하였음에도, 랜섬웨어 감염 및 개인정보가 유출된 이후 방화벽을 업데이트(’23.8.7.)하는 등 접근 통제 조치를 소홀히 한 사실이 있다.

4. 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 2024년 10월 29일 피심인에게 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인은 2024년 11월 12일 법 위반사실을 인정하고 선처를 요청하는 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련 법 규정

舊 보호법 제23조제2항은 “개인정보처리자가 민감정보를 처리하는 경우에는 유출 · 위조 · 변조 또는 훼손되지 아니하도록 제29조에 따른 안전성 확보에 필요한 조치를 하여야 한다”라고 규정하고 있으며, 같은 법 제29조에서는 “개인정보처리자는 개인정보가 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손되지 아니하도록

내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다”라고 규정하고 있다.

또한, 같은 법 시행령[2](이하 ‘舊 시행령’) 제30조제1항제2호에서는 “개인정보처리자는 법 제29조에 따라 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치를 하여야 한다”라고 규정하고 있고,

舊 개인정보의 안전성 확보조치 기준[3](이하 ‘舊 고시’) 제6조제1항에서는 “개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP 주소 등으로 제한하여 인가받지 않은 접근을 제한하고(제1호), 개인정보처리시스템에 접속한 IP주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응(제2호)“을 하도록 규정하고 있으며,

舊 고시 제6조제3항에서는 “개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치”를 하도록 규정하고 있다.

2. 위법성 판단

가. 민감정보의 안전성 확보에 필요한 조치를 소홀히 한 행위

[舊 보호법 제23조(민감정보의 처리 제한)제2항]

피심인이 민감정보를 포함한 개인정보에 대한 접근 통제 조치와 보안 프로그램의 최신성을 유지하지 않아, 환자의 민감정보 가 포함된 개인정보가 유출되었으며, 민감정보에 해당하는 건강정보에 대한 안전관리를 소홀히 한 행위는 舊 보호법 제23조제2항, 舊 시행령 제30조제1항제2호, 舊 고시 제6조제1항 및 제3항 위반에 해당한다.

Ⅳ. 처분 및 결정

2) 舊「개인정보 보호법 시행령」(대통령령 제32813호, 2022. 7. 19. 일부개정)
3) 舊 개인정보의 안전성 확보조치 기준(개인정보보호위원회고시 제2021-2호, 2021. 9. 15. 시행)

1. 과태료 부과

피심인의 舊 보호법 제23조제2항, 舊 시행령 제30조제1항제2호 및 舊 고시 제6조제1항, 제9조제2호 위반행위에 대해 舊 보호법 제75조제2항제6호, 舊 시행령 제63조, [별표 2] 및 개인정보 보호법 위반에 대한 과태료 부과기준[4](이하 '과태료 부과지침')에 따라 다음과 같이 과태료를 부과한다.

가. 기준금액

舊 시행령 제63조 및 [별표 2]는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 기준금액을 600만원으로 산정한다.

< 舊 보호법 시행령 [별표 2] 2. 개별기준 >

위반행위	근거 법조문	과태료 금액(단위 : 만 원)		
		1회 위반	2회 위반	3회 이상 위반
자. 법 **제23조제2항**, 제24조제3항, 제25조제6항, 제28조의4 제1항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	**舊** 법 제75조제2항 제6호	600	1,200	2,400

나. 과태료의 가중

과태료 부과지침 제7조 제1항은 "당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표 3]의 가중기준(▲위반의 정도, ▲위반 기간, ▲조사 방해, ▲위반 주도)에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다"라고 규정하고 있으며, 같은 조 제2항은 "[별표 3]의 각 기준에 따른 과태료 가중 시 그 사유가 2개 이상 해당되는 경우에는 합산하여 가중하되, 기준금액의 100분의 50을 초과할 수 없다"라고 규정하고 있다.

피심인의 경우 과태료 부과지침 제7조 및 [별표3] 과태료의 가중기준에 해당하는 사항이 없어 과태료를 가중하지 않는다.

다. 과태료의 감경

4)「질서위반행위규제법」제3조제2항에 따라 과태료 부과 시 피심인에게 유리하게 변경된 지침(2023. 9. 15. 시행) 적용

과태료 부과지침 제6조제1항은 “당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표 2]의 감경기준(▲당사자 환경, ▲위반정도, ▲업무형태 및 규모, ▲개인정보보호 노력정도, ▲조사 협조 및 자진 시정 등)에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다”고 규정하고 있으며, 같은 조 제2항은 “[별표 2]의 각 기준에 따른 과태료 감경 시 그 사유가 2개 이상 해당되는 경우에는 합산하여 감경하되, 최종 합산 결과 기준금액의 100분의 90을 초과할 수 없다”고 규정하고 있다.

피심인의 경우 과태료 부과기침 제6조 및 [별표 2] 과태료의 감경기준에 따라, ▲비영리 법인 또는 비영리 단체인 경우(30%), ▲시정을 완료한 경우(20%), ▲조사에 적극 협력한 경우(20%), ▲자율규제 규약 이행 등 개인정보 보호활동을 성실히 수행한 경우(10%)에 해당하여 기준금액(600만 원)의 80%(480만 원)를 감경한다.

라. 최종 과태료

피심인의 舊 보호법 제23조제2항 위반행위에 대하여 기준금액에서 가중·감경을 거쳐 총 120만원의 과태료를 부과한다.

< 과태료 산출내역 >

과태료 처분		과태료 금액 (단위:만 원)			
위반조항	처분 조항	기준 금액(A)	가중액 (B)	감경액 (C)	최종액(D) D=(A+B-C)
舊 보호법 제23조(민감정보의 처리 제한)제2항	舊 보호법 제75조제2항제6호	600	-	480	**120**

※ 피심인이 과태료 고지서를 송달받은 날부터 14일 이내에 과태료를 자진납부 하는 경우, 100분의 20을 감경함(질서위반행위규제법 제18조 및 같은 법 시행령 제5조 준용)

2. 공표

舊 보호법 제66조제1항 및 舊 개인정보보호위원회 처분 결과 공표기준(2020. 11. 18. 시행) 제2조(공표요건)에 따라, 피심인의 위반행위는 ‘1천명 이상 정보주체의 민감정보를 유출한 행위로 과태료 부과 처분을 받은 경우(제2호)’ 및 ‘위반

행위 시점을 기준으로 위반상태가 6개월 이상 지속된 경우(제5호)’에 해당하므로, 다음과 같이 위반행위 처분결과를 개인정보보호위원회 홈페이지에 공표한다.

다만, 개정된 개인정보 보호법 위반에 대한 공표 및 공표명령 지침(2023. 10. 11. 시행)에 따라 공표 기간은 1년으로 한다.

개인정보보호법 위반 행정처분 결과 공표

개인정보보호법 위반에 따라 행정처분한 내용 및 결과를 아래와 같이 공표합니다.

순번	위반행위를 한 자	위반행위의 내용		행정처분의 내용 및 결과	
	명칭	위반조항	위반내용	처분일자	처분내용
1	이화의대부속서울병원	舊 보호법* 제23조제2항	민감정보에 대한 안전조치위반 (접근통제, 보안 최신성 유지의무 위반)	2025. 7. 23.	과태료 120만 원

* 舊 보호법 : 2020. 8. 5. 시행, 법률 제16930호

2025년 7월 23일

개 인 정 보 보 호 위 원 회

Ⅴ. 결론

피심인의 舊 보호법 제23조(민감정보의 처리 제한)제2항 위반에 대하여 같은 법 제75조(과태료)제2항제6호에 의한 과태료 부과 및 제66조제1항에 따른 공표를 의결한다.

이의제기 방법 및 기간

피심인은 이 과태료 부과처분에 불복이 있는 경우, 「질서위반행위규제법」 제20조제1항에 따라 과태료 부과 통지를 받은 날부터 60일 이내에 개인정보보호위원회에 서면으로 이의제기를 할 수 있다.

과태료 부과처분에 대한 피심인의 이의제기가 있는 경우, 개인정보보호위원회의 과태료 부과처분은 「질서위반행위규제법」 제20조제2항의 규정에 따라 그 효력을 상실하고 관할법원(피심인 주소지의 지방법원 또는 그 지원)이 과태료 재판 절차에 따라 결정한다. 이 경우 피심인은 관할법원의 과태료 재판이 확정된 이후 재판 결과에 따라 과태료 납부 의무를 부담한다.

이상과 같은 이유로 주문과 같이 의결한다.

2025년 7월 23일

위 원 장 김 진 환 (서 명)

위 원 김 일 환 (서 명)

위 원 김 휘 강 (서 명)