개 인 정 보 보 호 위 원 회
심의·의결

안건번호 제2023-013-158호

안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 학교법인 가톨릭학원(법인등록번호 : -)

대표자

의결연월일 2023. 7. 26.

주 문

1. 피심인에 대하여 다음과 같이 과태료를 부과한다.

   가. 과 태 료 : 21,600,000원

   나. 납부기한 : 고지서에 명시된 납부기한 이내

   다. 납부장소 : 한국은행 국고수납 대리점

2. 피심인 산하 종합병원에 대하여 다음과 같이 개선할 것을 권고한다.

   가. 개인정보 유출이 발생한 개인정보처리시스템을 포함하여 피심인이 운영 중인 개인정보처리시스템 전반에 대해 「개인정보 보호법」 제29조(안전조치 의무) 준수 여부를 자체적으로 점검하고, 재발방지 대책을 수립할 것

   나. 대표자를 비롯한 개인정보 보호책임자 및 개인정보취급자를 대상으로 개인정보 보호에 대한 인식 제고를 위한 정기적인 개인정보 보호 교육 계획을 수립하고 실시할 것

다. 상기 개선 권고 통지를 받은 날로부터 60일 이내에 조치결과를 제출할 것

3. 피심인 산하 종합병원의 법 위반행위에 따른 행정처분의 내용 및 결과를 개인정보보호위원회 홈페이지에 공표한다.

이 유

Ⅰ. 피심인의 일반 현황

피심인은 개인정보처리시스템( )으로 개인정보를 처리하는 「개인정보 보호법」(법률 제16930호, 이하 "보호법"이라 함) 제2조제5호에 따른 개인정보처리자인 종합병원을 운영하는 학교법인으로 일반현황은 다음과 같다.

< 일반현황 >

학교법인명 (법인등록번호)	**병원명*** (사업자등록번호)	**설립일자**	**병원 대표자**	**상시 종업원수**	**자본금** (억원)	**매출액** ('21년, 억원)

Ⅱ. 사실조사 결과

개인정보보호위원회는 개인정보보호 포털에 유출 신고('21.11.1.)가 접수된 건과 관련하여 현장조사 및 이와 관련된 제출자료를 토대로 조사한 결과, 다음과 같은 사실을 확인하였다.

1. 개인정보 유출 개요

가. 유출 규모 및 경위

○ **(유출 규모)** 피심인 산하 서울성모병원 등 6개 병원에서 총 66,949명의 환자정보*가 유출되었고, 이중 진료과와 처방코드는 민감정보에 해당한다.

* 성명, 환자등록번호, 생년월일, 나이, 성별, 처방일, 처방의, **진료과**, 처방내역(수량, 용량, 횟수, 일수, **처방코드**)

< 병원별 유출 규모 >

개인정보처리시스템	병원명	유출시기	유출규모
병원정보시스템 ( )	서울성모병원	'18.11월~'19.12월	16,463명
	여의도성모병원	'19.1월 ~ '19.4월	17,115명
	은평성모병원	'19.6월, '19.12월	3,633명
	의정부성모병원	'19.2월~'19.12월	20,027명
	부천성모병원	'18.10월 ~ '20.1월	9,673명
	성빈센트병원	'19.4월	38명

○ **(유출 경위)** 의사 등 내부 직원이 다운로드한 환자정보를 이메일이나 보조저장매체(USB)를 통해 제약사 직원에게 송부하거나, 병원 직원이 로그인한 PC에서 제약사 직원이 화면을 촬영하거나 환자정보를 다운로드하였다.

< 병원별 유출 경위 >

병원명	유출 경위
가톨릭대학교 서울성모병원	
가톨릭대학교 여의도성모병원	
가톨릭대학교 은평성모병원	
가톨릭대학교 의정부성모병원	
가톨릭대학교 부천성모병원	
가톨릭대학교 성빈센트병원	

나. 유출 경과 및 대응

일 시	유출 인지·대응 내용
‘21. 2월 ~ 5월	ㅇ 경찰청으로부터 수사 사항 비공개 공문을 접수 후 인지 및 미신고 ㅇ 경찰청의 1차 참고인(정보보호·시스템 담당 등) 조사
‘21.10.26.	ㅇ KBS 언론보도
‘21.11. 1.	ㅇ 유출 신고
‘21.10월 ~ 11월	ㅇ 경찰청의 2차 참고인(병원장) 조사
’21.12.23 ~ 12.31	ㅇ 경찰청 수사 결과 통보
’22. 2. 9. ~ 2.18.	ㅇ 유출 파일 확인 및 수령(경찰청 → 개인정보위 → 병원)
’22. 2.23.	ㅇ 유출 통지(문자, 홈페이지 게시 등)

2. 행위사실

○ 개인정보처리시스템의 안전성 확보 조치를 소홀히 한 행위

- 피심인 산하 병원 중 ❶3개 병원(은평성모, 부천성모, 성빈센트)은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 2년 이상 보관하지 않고(6개월 보관), 월 1회 이상 점검하지 않았으며, ❷6개 병원 모두는 ‘개인정보 다운로드 사유’ 등 접속기록 일부를 누락한 사실이 있다.

3.. 위법성 판단

○ 개인정보취급자가 개인정보처리시스템에 접속한 기록을 2년 이상 보관·관리하지 않은 행위는 보호법 제23조제2항과 제29조, 같은 법 시행령 제30조제1항 및 개인정보 안정성 확보조치 기준(이하 ‘고시’) 제8조제1항 위반에 해당하고,

- 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 점검하지 않거나, 접속기록 일부(개인정보 다운로드 사유 등)를 누락한 행위는 보호법 제23조제2항과 제29조, 같은 법 시행령 제30조제1항 및 고시 제8조제2항 위반에 해당한다.

Ⅲ 처분의 사전통지 및 의견 수렴

개인정보보호위원회는 '23. 5. 23. 예정된 처분에 대한 사전통지서를 송부하고 이에 대한 의견을 요청하였으며, 피심인 산하 각 병원은 '23. 6. 7. 의견제출을 통해 보호법 위반 사실을 인정하고 처분의 사전통지 및 의견제출 기간이 종료되기 이전에 시정을 완료하면서 선처를 요청하였다.

Ⅳ. 처분 및 결정

1. 과태료 부과

피심인 산하 6개 병원의 보호법 제23조제2항 및 제29조 위반에 대해 같은 법 제75조제2항제6호, 같은 법 시행령 제63조 [별표2]의 「과태료의 부과기준」에 따라 다음과 같이 병원별로 산정된 과태료 금액(360만 원)을 합산하여 총 2,160만 원의 과태료를 부과한다.

가. 기준금액 산정

피심인 산하 6개 병원은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 1회 위반에 해당하는 금액 총 600만 원을 적용한다.

< 과태료 부과기준 2. 개별기준>

위반행위	근거 법조문	과태료 금액(단위 : 만 원)		
		1회 위반	2회 위반	3회 이상
자. 법 제23조제2항 또는 법 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조 제2항제6호	600	1,200	2,400

나. 과태료의 가중

「개인정보 보호법 위반에 대한 과태료 부과기준」(2023. 3. 8. 개인정보보호위원회 의결, 이하 '과태료 부과지침') [별표2] 과태료의 가중기준(제8조 관련)에 따라 법 위반상태의 기간이 3개월 이상인 점을 고려하여 해당 기준금액(600만원)의 10%를 가중한다.

< 과태료의 가중기준(제8조 관련) >

기준	가중사유	비율
위반기간	법 위반상태의 기간이 3개월 이상인 경우	기준금액의 50% 이내

다. 과태료의 감경

과태료 부과지침 [별표1] 과태료의 감경기준(제7조 관련)에 따라 각 병원이 과태료의 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 중지하는 등 시정을 완료한 점, 개인정보 보호 자율규제 규약을 이행하는 등 개인정보 보호 활동을 성실히 수행한 점 등을 고려하여 기준금액(600만원)의 50%를 감경한다.

< 과태료의 감경기준(제7조 관련) >

기준	감경사유	감경비율
조사협조 · 자진시정 등	1. 과태료의 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 중지하는 등 시정을 완료한 경우	기준금액의 50%이내
개인정보보호 노력정도	3. 개인정보 보호 자율규제 규약을 이행하는 등 개인정보 보호 활동을 성실히 수행한 것으로 확인된 경우	기준금액의 40%이내

※ 과태료 부과지침 제7조(과태료의 감경)에 따라 과태료의 감경은 기준금액의 50%를 초과할 수 없음

라. 최종 과태료

피심인 산하 각 병원의 보호법 제23조2항 및 제29조 위반행위에 대해 기준금액에서 가중·감경을 적용하여 총 360만 원을 각각 부과한다.

< 최종 과태료 산출내역 >

과태료 처분의 근거		과태료 금액 (단위:만 원)			
위반 조항	**처분 조항**	**기준금액(A)**	**가중액(B)**	**감경액(C)**	**최종액(D=A+B-C)**
제23조(민감정보의 처리 제한)② 제29조(안전조치의무)	제75조제2항제6호	600	60	300	**360**

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

2. 개선권고

의료데이터로서 사생활 침해 위험이 큰 민감정보가 대량으로 유출되었고, 개인정보 안전조치의무 위반이 확인된 점, 개인정보취급자의 개인정보 보호에 대한 인식 부족으로 인한 유출사고인 점 등을 고려하여 보호법 제61조제2항에 따라 다음과 같이 개선을 권고한다.

① 개인정보 유출이 발생한 개인정보처리시스템을 포함하여 피심인이 운영 중인 개인정보처리시스템 전반에 대해 「개인정보 보호법」 제29조(안전조치 의무) 준수 여부를 자체적으로 점검하고, 재발방지 대책을 수립할 것

② 대표자를 비롯한 개인정보 보호책임자 및 개인정보취급자를 대상으로 개인정보 보호에 대한 인식 제고를 위한 정기적인 개인정보 보호 교육 계획을 수립하고 실시할 것

③ 상기 개선 권고 통지를 받은 날로부터 60일 이내에 조치결과를 제출할 것

3. 처분결과의 공표

피심인 산하 6개 병원의 위반행위에 대해 보호법 제66조제1항 및 같은 법 시행령 제61조에 따라 처분결과를 다음과 같이 개인정보보호위원회 홈페이지에 공표한다.

<table>
<tr><td colspan="6">개인정보보호법 위반 행정처분 결과 공표</td></tr>
<tr><td rowspan="2">순번</td><td>위반행위를 한 자</td><td colspan="2">위반행위의 내용</td><td colspan="2">행정처분의 내용 및 결과</td></tr>
<tr><td>명칭</td><td>위반조항</td><td>위반내용</td><td>처분일자</td><td>처분내용</td></tr>
<tr><td>1</td><td></td><td>제23조제2항, 제29조</td><td>개인정보처리시스템 안전성 확보 조치 미이행</td><td rowspan="6">2023.7.26.</td><td>과태료 부과 360만 원 개선권고</td></tr>
<tr><td>2</td><td></td><td>상동</td><td>상동</td><td>상동</td></tr>
<tr><td>3</td><td></td><td>상동</td><td>상동</td><td>상동</td></tr>
<tr><td>4</td><td></td><td>상동</td><td>상동</td><td>상동</td></tr>
<tr><td>5</td><td></td><td>상동</td><td>상동</td><td>상동</td></tr>
<tr><td>6</td><td></td><td>상동</td><td>상동</td><td>상동</td></tr>
<tr><td colspan="6">2023년 0월 00일
개 인 정 보 보 호 위 원 회</td></tr>
</table>

Ⅴ. 결론

피심인 산하 각 병원의 보호법 제23조(민감정보의 처리 제한)제2항 및 제29조(안전조치의무) 위반에 대해서 같은 법 제61조(의견제시 및 개선권고) 제2항, 제75조(과태료)제2항제6호 및 제66조(결과의 공표)제1항에 따라 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 과태료 부과처분에 불복이 있는 경우,「질서위반행위규제법」 제20조의 규정에 따라 그 처분을 받은 날부터 60일 이내에 개인정보보호위원회에 서면으로 이의를 제기할 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 재판절차에 따라 결정한다. 이 경우 피심인은 관할법원의 과태료 재판이 확정된 이후 재판 결과에 따라 과태료의 납입 의무를 부담한다.

2023년 7월 26일

위 원 장　　고 학 수　(서 명)

부위원장　　최 장 혁　(서 명)

위　　원　　강 정 화　(서 명)

위　　원　　고 성 학　(서 명)

위　　원　　백 대 용　(서 명)

위　　원　　서 종 식　(서 명)

위　　원　　이 희 정　(서 명)

위　　원　　지 성 우　(서 명)