

# 2022년 공공기관 개인정보 관리수준 진단 준비사례

〈국립암센터 정보보호팀〉







# 01 기관소개



## 01 기관소개



국립암센터는 암에 대한 전문적인 연구와 진료를 통하여, 우리나라 국민의 암 발생률과 사망률을 낮추고 암 환자의 삶의 질을 높이는 등 국민보건향상에 이바지하고자 설립된 정부출연기관

## <기관연혁>

- 1. 2000.01.12. 국립암센터 공포
- 2. 2001.06.20. 국립암센터 개원
- 3. 2005.06.20. 연구동 개관
- 4. 2007.06.19. 국가암검진센터 및 양성자치료실개관
- 5. 2014.03.01. 국제암대학원대학교 개교
- 6. 2021.01.01. 제8대 서홍관 원장 취임



## 01 기관소개



2020.2.1.일부 국립암센터 정보보호팀 조직운영

정원: 2명(정보보호, 개인정보보호전담 각 1명)

☞ 2023년 현재

1) 정규직: 2명

2) 임시직: 1명

3) 과제연구원 및 내부통합관제 용역: 3명





# 02 시작하면서



## 02 시작하면서



■ 기관 개인정보보호담당자

P/E/II/E/ WEHLLERY 환자비대면진료지원 서비스?▼ 집중관리시스템선정?

타부서 이동, 이직이 답이다.

정기감사? 개인정보 관리수준 현황조사?





# 03 공공기관 개인정보 관리수준 진단



# 03 공공기관 개인정보 관리수준 진단



공통업무	혁신업무 평가지표	정책업무 평가지표	기타
61	2	3	
			■ 유출사고
정량지표	정성지표	정성지표	■ 행정처분
			■ 거짓허위
00	7		

## 03 공공기관 개인정보 관리수준 진단



- 2022년 공공기관 관리수준 진단의 의미
- 1. 공통지표 : 자체 평가 지표
  - 기관 지표, 시스템지표로 나뉜다
  - 기관 지표는 정보보호팀에서, 시스템 지표는 각 운영부서에서
  - ☞ 현실적인 측면을 고려가 필요

- 2. 혁신업무, 정책업무 지표 : 개인정보보호위원회 평가지표
  - ☞ 법적준거성을 고려한 것이 "공통지표"라면, 혁신업무, 정책업무 지표는 실질적인 기관 활동에 대한 것을 평가







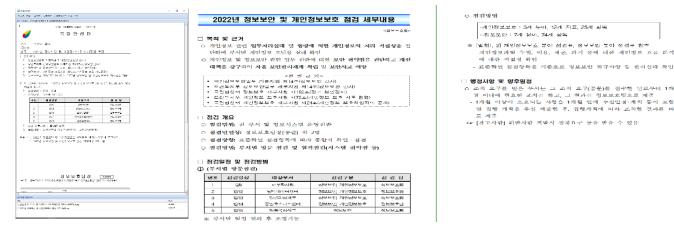


- 의료데이터, 암연구자료, 국가암관리사업자료, 학사정보 등 다양한 개인정보를 처리하고 있으며, 기관성격상 각종 통제정책 수립에 있어 정부부처나 일반 공공기관에 비해 복잡도가 매우 큰 편
- 개인정보보호관리체계 수립에 기초가 되는 관리적, 기술적, 물리적 보호체계의 구축
- 개인정보처리시스템의 접근권한 및 접속기록에 대한 점검과 위탁업체에 대한 점검을 매월 실시
- 상급기관 개인정보관제센터와의 연계를 통한 실시간 개인정보통합관제와 내부통합관제체계 운영





- 개인정보 보호 전사적 관리체계 구축 운영
  - (개인정보보호지침 및 내부관리계획) 상급기관 관련 지침 개정반영
  - (내부점검체계구축)



☞ 업무전반에 대한 보안취약점을 진단 및 개선, 자율보안관리체계 확립을 통해 보안사고 예방

- (개인정보파일일제정비 및 개인정보파일 처리방침 개정)





### ■ 임직원 및 수탁자 맞춤형 개인정보보호 교육 프로그램 운영

- 개인정보보호 교육계획에 따른 대상별 차별화 교육추진 ☞ CPO, 개인정보보호담당자, 부서별 보직자, 개인정보취급자 등 맞춤형 교육
- 개인정보보호 담당자 전문교육 및 개인정보처리시스템 운영실무자 교육
- 전 직원 대상교육(연 2회, 코로나-19로 인한 온라인교육)
- 수탁자 맞춤형 개인정보보호 교육(연2회)

		개인정보보호 교육	비획.	서					보안 교	육 참석기	다 명단		
28 9	상 : 개인정	보 취급 직원(연 200) 및 일반 직원(연 100)											
■ 교육 시기 : 22.5.30일 오후 2시 , 22.10.20일 오전 10시						* 일 시 : 2022. 06.07(화)							
■ 개안점보보호 교육 설시 사용 1. 개인정보여 대한 전반적인 이해 - 개인정보여 중요성에 대한 인식은 있으나 세우나들에 있어서 명확한 인식이 무목하여 요무를 적 리되면 있어서 전반적으로 미국을 무용이 있음						* 감사명 : 넥스프론 * 주 제 : 개인정보 보안교육							
2. 개인정보 관리는 단점성 회보 , 개인정보의 수집 이용 처음 시 법칙한 관점사람들 준수하지 않아 개인정보 질때 사례 활성						- 개인정보보호법에 따른 장비별 개인정보보안 교육 - 사업기간 내 보안준수ほ동 보안교육 - 보안병당 시례 공유							
	이지 개인정: 정보보프랑	6 관리 일에 대한 공지 및 게시가 부족하여 관련 분의	<u>후</u> 가				- 모안물등	가게 공유					
							순번	소속	직책	성명	날인	비교	
1. 정보화의 진전에 따라 개인정보의 수집 이용과 유통이 급증하여, 각종 병회와 프라이버시 집에 동의 부탁용 증가로 교육을 통해 예방법, 대학에 대한 방안을 점립						1	네스프론	수석	김도윤	220	개인정보 취급지		
2. 00016	무배이스파틴	개인정보의 안전한 저희 관리에 대한 시뮬규칙	-	이 입무를 다	なかり	수별	2	네스프론	책임	고영아	200+	개인정보 취급자	
<ul> <li>개성법항에 (전한 어제를 제고하고 원활한 법 참정을 도모</li> <li>가인정보보로 암무추진제화를 수힘 및 시험하여 고객의 경리와 이익을 보로</li> </ul>					3	넥스프론	수석	권정수	12				
					4	넥스프론	선임	이은빈	6120				
2022\6	도 교육운영	7811					5	넥스프론	책임	흥민우	(8)		
44	구분	교적 열	7121	22 Al 21	20	비교	6	넥스프론	선임	한국일	-4º5		
		사례로 살펴보는 개인정보보호날 주요나를	16	22.5.30	1		7	넥스프론	선임	강경민	252010	/	
1		(출제-개인정보보호위원회)		22.10.20	1		8	넥스프론	선임	박진탁	백진막		
							9	넥스프론	선임	이정민	25.07		
							10	넥스프론	선임	홍종희	易为到		
							11	넥스프론	이사	이창욱	6/ 3/2		



- 자체 개인정보보호 교육 동영상 콘텐츠 제작 및 온라인 교육





## ■ 내·외부 통합망분리 구축 운영





#### 업무 영역(로컬PC)

- ✓ 로컬PC는 기존과 같은 업무 처리 가능
- ✓ 인터넷 사용 불가
- ✓ 자료전송 프로그램을 통해 인터넷망에 자료 전달

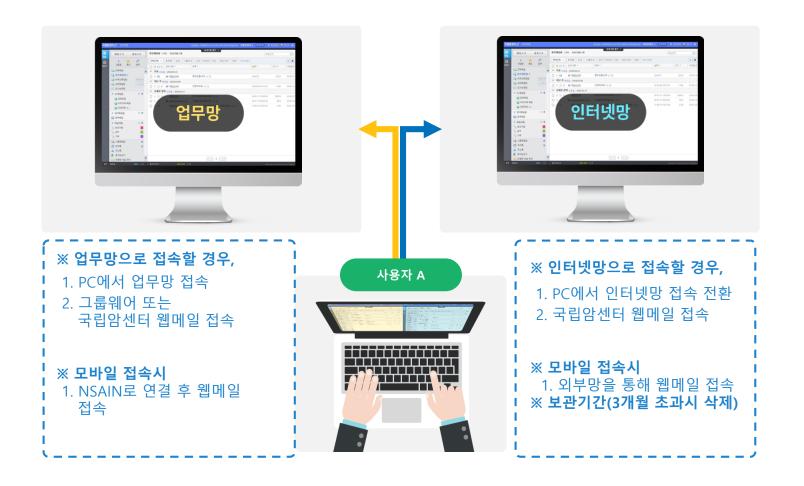
#### 인터넷 영역(가상영역)

- ✓ 가상화 PC 영역에서 인터넷 사용
- ✓ 업무 영역의 자료 접근 불가
- ✓ 이동식 저장매체 이용 불가!(USB, 외장하드 등)





■ 메일 분리구성(상용메일 원천차단)







## ■ 개인정보처리시스템 및 사용자 보안체계 강화

- 개인PC 보안체계 강화 : 백신, 개인PC검출솔루션, 유해사이트차단 등
- 서버내 보안체계 강화 : 패스워드관리, 소스코드 취약점, 서버접근제어, 서버내 개인정보 검출, 서버백신, 패치관리, 웹 필터링, 웹 노출점검

### • 개인정보처리시스템 접속기록의 보관 및 점검 안정성 확보조치 강화

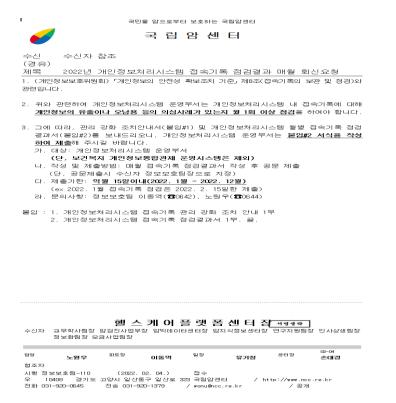
- 법률에 따라 시스템별로 최소 1년간 접속기록을 보관
- 개인정보처리시스템 접속기록은 매달 담당자가 점검 및 보고체계 확립
- 서버 접근제어 솔루션, DB 접근제어 솔루션으로 시스템 접근 권한 관리
- 외부 원격 접속 VPN 이력 점검하여 부서장 결재 득하여 공문 제출





## ■ 접근권한 및 접속기록에 대한 점검(위탁 포함)

- 개인정보처리시스템의 월별 접속기록을 점검하고, 원격 유지보수업체에 대한 접속기록 점검으로 토대로 개인정보유출 방지체계 강화



국민을 암으로부터 보호하는 국립암센터



국 립 암 센 터

수신 수신자 참조

(경유)

제목 개인정보처리시스템 원격유지보수 접속기록 점검결과 회신 요청

#### 1. 관련근거

- 가. 국가정보보안 기본지침 제59조(원격근무보안)
- 나. 보건복지부 정보보안 기본지침 제50조(정보시스템 유지보수)
- 다. 정보보호팀-91(2020.03.05.)개인정보처리시스템 원격 유지보수 관련 정보보안 강화 조치 시행
- 이와 관련하여 개인정보처리시스템 원격 유지보수 점검결과서 및 접속기록 대장을 보 내드리오니, 개인정보처리시스템 원격 유지보수 부서는 작성하여 제출해 주시기 바랍 니다.
- 가. 점검대상: 개인정보처리시스템 원격 유지보수 운영부서
- 나. 작성 및 제출방법: 2022년 3분기(7월~9월)의 점검결과서 작성 후, 공문제출
- 다. 제출요청문서: 개인정보처리시스템 원격 유지보수 점검결과서 1부 개인정보처리시스템 원격 유지보수 접속 기록 대장 1부
- 라. 제출기한: ~ 2022. 10. 19. (수)
- 마. 문의사항: 정보보호팀 최민우(☎0643), 전수진(☎0646)

붙임 1. 개인정보처리시스템 원격유지보수 점검결과서 1부

2. 개인정보처리시스템 원격 유지보수 접속 기록 대장 1부. 끝





## ■ 개인정보 처리업무 위·수탁 현황 파악(요청 및 현황관리)

		명으로부터 보여 로 립 양	세 EI			72	개인정보처리 위탁명	위탁 부서	수탁 업체	•개인정보 교육 현황	관리감독취과/ 작성 여부
		4 8 0	(m)			1	국가암정보선터 통합유지보수	양지시정보센터	AMARE	완료	원로
						2	전자용의서 시스템 유지보수	의료정보관하실	다중누리메디컴	彩虹	원보
						3	검색을 검사 위탁	진단정사외학과	속성취업통제단	設度	완료
4	수십자 참조					4	검색물 검사 위탁	진단점사의학과	시전성호제단	완료	원보
유)						5	국가발경진 정보시스템 유지보수	임검진사업부	MAARE	砂草	원로
2	2022년 개인정보 차	김업무 위로	(원화 제출)	유원)		6	환사권리시스템(LMS) 유기보수	교무한사형	(최이아)이 유니케이션	砂点	환호
_						7	의효영상 원칙용급단독 위탁	의료자원임(영상의학교)	휴면영상의학과의원	記皿	원보
20	크게 : 개인정보보호텔 제	26조, 시험성	N262			8	온라인 및 오프라인(일부) 교육 위학 운영	28209	神楽년	완료	문로
	거에 의거하여 개인정보				양식물 참고하	9	국가암감한 집량상 온라인교육 시스템 유지보수	임점된사업부	(42.595)	완료	완료
	인정보 처리얼두 위탁 한 이정보 처리얼두 위탁 이		주시길 바랍니	Cr.		10	국가매암검진 판독지원 및 정관리 정보시스템 교도함 및 유지보수	양합진시업부	*国内科型企業性	55.00	원로
	田田工 おいます 名号 日	6(84)				-11	채용사이트 운영	인사상생림	(with clark)	완료	원로
(HP)	개인정보 처리업무 위탁명	위탁부서	수탁기관	계약기간	계약 형태	12	호스피스완화의로 시스템 유지보수	중앙로스피스센터	#ipto atri	お耳	- 野里
	100-110	-0.11.00	1.1.1.	3500	4101	.13	호스리스완화의로 이러닝 운영	중앙호스피스센터	(40)이에듀	완료	완료
1	해) 전투시스템 유지보수	SHREE	ASMSU	2022 1 1 - 2022 12 33	조달/자체	14	양예방암진년터 전화상당시스행전화상당API 유지보수 제약	Bookstries	MANE	9.5	64
-			-	_		15	무인수날기 임대제약	원무함	공간소프트	원트	완료
	mi21 m : - 2022		-			16	신용적도 보가가처용신앙 서비스 구축	548	나이스정보통신	완료	완료
	호망력 : 공연	NAPA IN				17	연구시업관리정보시스템 유지보수 및 운영지원	연구지원당	시스템케이트바	20年	SE
- 5	. 개입장보 처리업무를	위탁하지 않는	부서는 최신	製品品		18	결합전문기관 서비스 및 운영시스템 개발	はの計算品の	HETBO	완료	완료
						.19	최판 가입 휴대폰 본인인증	대이하겠합님	NEE BYSE	砂車	記載
병장.	나많(위학 부서별 하입사)	8)				20	국립암센터 모바일업	정보했답	라운함스적어	완료	원로
1 2	함여 의거하여, 함보주차	의 개인정보	가 분실 - 도년	유승 위조	변조 또는 확	21	휴대폰 본인확인 서비스	정보하십	한국모바일만층	- 砂皿	원보
	되지 아니하도의 수확자	ON DIE	TEAT OF	THE WOLFE	NEINE D	22	이이된 본인확인 서미스	정보환당	NICE 평가정보	완료	원로
						23	정보찬산시스템관리용역 계약	등보호님	(4등은정보기술	완료	원로
	타, 목록 의 이용 - 제권	년부· 전취학	이 너무, 많은	경 체로소치 어	두 등로 의기	24	정보전산시스템관리용역 계약	정보회담	HARIOTETE.	크당	원로
0	으로 관리감독 현아함					25	건명인 업무 협약서	간호본부	(428C) (100M)	왕보	8.0
	왕자 교육 관리감독 이번	자료 보유 :	위탁계약서.	中醫及 直接的想	여루, 관리함	26	간병인 업무 협약서	간호본부	(6.에니얼에디컬	新年	원로
. 4	이번대부 등(당. 이번지	0 = 0 = 3	e was			27	추차당 위탁운영	운영지원임	하이그린파티	20年	원보
					and the second of the second	28	환자급식 등 운영 위탁 제약	84884	동원음부드	완료	완료
-	BATARIE SERVICE - SEWI						WEST CONTROL	일업된AY업부	1812/2018/6	24.00	9.8
9. 8	탁관현 분의사항 : 정보! (#1845)	<b>ESS 0/84</b>	(1100-11			29					

## ■ 개인정보 처리 위·수탁 관리 감독 강화(연1회 이상 검토)

- 용역계약 시 수탁자 교육 및 관리감독 방안 , 보안관리 준수지침 안내

	부 서 명	정보화팀	. 6. 276. 30. 2022. 7. 1. 전 인 선택하		
	사 업 명	정보전산시스템 관리용역계약			
	용역책임자/ 위탁사업자	박동균 / 까동은정보기술 하필라테크			
엔번	진단지표	3	검항목		정검결과
, 개인정보보호교		1.1. 연간 개인정보보 있는가?	A. O.		
1	욕추진	1.2 개인정보취급자. 교육이 모두 이행되고	DA DI		
2	재위탁급지	2.1. 재위탁은 하고 있	WY ON		
3	개인정보목적의 이용 : 제3자제 공절차운영	3.1. 제공한 개인정보 제3자에게 제공하지	DY DI		
4	개인정보침해사 고대용절차	4.1. 제공한 개인정보 침해사고 발생시 대설 전파하였는가?	DY DI		
5	개인정보 파기 및 관리	5.1. 제공한 개인정보 보유기간이 정과한 경 해당 개인정보를 복원 파기하고 있는가?	D. 01		
	4/1 × #4	5.2 개인정보 취급과 임시파일을 즉시 삭제	정에서 발생한 출력물  하는가?	및	D. D.
6	업무PC 개인정보보호	6.1. 업무용 컴퓨터(PI 별도로 암호화하거나	O에 적장된 개인정보 보안 USB에 저장하는	는 가?	Dr 01

#### 용역업체는 계획부터 완료시까지의 다음 보안관리 지침을 준수하여야 한다. ● 입찰시 ⇒ 용역사업에 대한 보안관리 계획 평가 □ 계약시 ⇒ 보안준수 사항 및 배상책임 명시 ● 수행시 ⇒ 참여인원 보안조치, 인원·문서·장비 등 보안관리실대 점검·교육 ② 종료시 → 제공자료 · 산출문 전량 회수 등 보안조치 표 본 자료에 명시되지 않은 사항은 아래의 관계 제 규정 적용 ○ 국가정보원 「국가·공공기관 발주 용역사업 보안관리 요령 ○ 보건복지부 「보안업무규정운용세칙」, 「정보보안업무세부지칭 ○ 국립암센터「보안업무규칙」,「정보보호세부지침」,「개인정보보호처리지침」등 ○ 용역사업에 투입되는 자료·장비 등에 대한 대외보안이 필요한 경우 보안의 범위·책임을 명확히 하기 위하여 사업수행 계약서와 별도로 "비밀유지계약서 - 비밀유지계약서에는 비밀정보의 범위, 보안준수 사항, 위반시 손해배상 책임, 지격재산권 문제, 자료의 반환 등이 포함됨 ○ 사업착수시 용역업체 자체 보안관리 및 직원 관리감독 강화를 독려하고 보안 의 중요성 인식계고를 위해 업체대표 명의 "보안서약서-대표자용(불입2)" 작성 . 유연사업과 과취하 보안과진 했인은 유연업체 대표에게 있으며 대표는 유연 사업 전반의 보안업무를 수행하는 '보안관리책임자'를 지정하여 사업부서에 - 보안관리책임자는 용역사업과 관련된 인원·장비·자료에 대한 보안업무 및 사업과 판련된 하도급업체의 보안관리 전반을 총괄함 용역사업 참여인원은 용역업체 임의로 교체할 수 없으며, 신상변동(해외여행 포함) 사항발생시 발주기관에 즉시 보고하여야 한다.

용역업체 보안관리 준수 지침

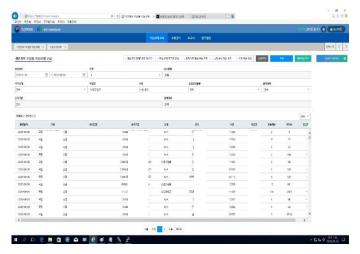




■ 상급기관과 실시간 개인정보통합관제연계



< 개인정보통합관제 >



< 관제에 대한 소명처리 >

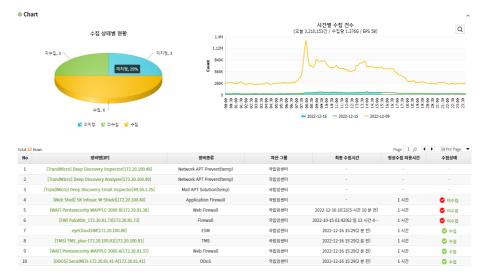


< 조치사항 메일 안내 >





- 자체 내부통합관제체계 구축(2022년 추진)
  - 최근 정보보호 기술을 활용하여, 보안시스템의 보안로그를 분석 및 대응
  - 24시간 보안관제 및 보안시스템운영
  - ☞ 상급기관 사이버안전센터 연계, 보안관제 절차수립 및 운영체계 마련





1016 건

1 만 8976 건

분석 시간 | 2022-10-14 08:25:00 ~ 2022-10-14 09:24:59

мы 139 / TCP

[통합로그분석시스템 운영]

[위협관리시스템 운영]





### ■ 2022년 ISMS-P 인증획득

☞ 개인정보보호 관련 기술적 보호체계 확립 완료







# 05 정보보호 추진계획



# 05 정보보호 추진계획



■ 차세대 EMR 추진에 따른 정보보호체계 관리를 위한 중장기 계획수립

#### 차세대 정보시스템 구축

- ◇ ICT 기술을 활용한 **가치기반 암전문 헬스케어시스템** 구축
- ◇ 전자의무기록인증제 및 표준화 기반의 플랫폼 구축
- ◇ 자기주도형 정보를 활용한 환자안전 및 맞춤형 서비스 기반마련

### 전사적 정보보호 관리·운영체계 마련

- ◇ 중장기적 정보보호 솔루션 도입 등 **정보보호 관리체계 강화**
- ◇ 개인정보처리시스템 구축시 필요한 개인정보보호영향평가
- ◇ 서비스 연속성 확보를 위한 재해재난 체계 수립 및 기반설비 개선

### 안정적인 정보서비스 제공을 위한 차세대 인프라 구축

- ◇ 노후 인프라의 교체를 통해 장애 발생 가능성을 낮추어 정보서비스의 연속성 강화
- ◇ 정보인프라의 고도화를 통해 신속한 정보서비스 제공 및 의료 업무 서비스 품질 제고
- ◇ 사업본부 정보시스템의 통합운용으로 관리운영 효율 제고



## 05 정보보호 추진계획



## ■ 차세대EMR 추진에 따른 정보보호 관리체계 구축

#### 차세대PACS구축

엔터프라이즈 시스템 다학제 PACS구축

#### 기반인프라구축

노후네트워크교체 신관 인프라 구축

#### 차세대EMR

환자별 최적화를 통한 개인별 맞춤형 관리 업무효율과 협업을 위한 차세대 행정시스템 EMR인증제 및 진료정보교류 기반 시스템 데이터 재사용성을 고려한 표준화 및 자동화 실시간 통합재고관리체계 구축 노후화된 인프라시스템의 교체

#### 통합연구정보시스템구축

연구중심병원기반마련을위한 데이터활용체계 암정복 선도를 위한 정보기술환경 구축

#### 그룹웨어, 홈페이지 재구축

업무효율 고객중심

#### 데이터분석 및 지표관리

데이터기반 효율개선

#### 정보보호 관리체계 구축

노후보안솔루션교체 정보보호체계 정비 등 ISMS-P 인증 재해재난체계 구축(DR) 개인정보보호영향평가

#### 국가암관리정보시스템정보기술거버넌스확립

통합구축 및 운영컨설팅

노후화된 정보시스템 재구축 단위시스템의 개별성 분절성 개선

공공성 강화 및 업무효율제고

변화에 친화적인 환경구축

가용성 증대와 운영효율 향상

정보보호 체계 강화



# 06 맺음말



# 06 맺음말



- 정부부처의 조직 강화
  - 정부에서는 지난 몇년간 주요병원 해킹 사고 및 개인정보 유출에 따른 신당역 살인사건 등 급증하는 정보보안 관련 사고에 대한 대안으로, 각종 법령정비 및 처벌기준을 강화하고 집중관리시스템을 선정하는 등 관리체계 전반을 고도화

■ (현실태) 산하기관 및 공공의료기관 등 정보보호 관련 전문인력 양성 부족



- 정부차원의 정보보호 전문인력 확보의 중요성에 대한 적극적인 홍보
- ☑ 법적 의무기준 신설 등 제도화된 정책 마련이 시급





