

이 보고서는 국립암센터의 영향평가 결과 요약 자료입니다.



「첨단IT기반 차세대 정보시스템 : 사업본부 정보시스템」

개인정보 영향평가 결과보고서 요약본

2025. 2.

 (주)지티시큐

개인정보 영향평가서 요약본							
공공기관 명칭		국립암센터					
평가기관		(주)지티시큐	평가 기간	2024. 10.28. ~ 2025. 02.14.	평가예산	☐ 1천만원 미만 ☐ 1천만원 이상~3천만원 미만 ☒ 3천만원 이상~5천만원 미만 ☐ 5천만원 이상~1억원 미만 ☐ 1억원 이상	
평가대상시스템 개요	시스템명	사업본부 정보시스템			시스템 구축 또는 변경 일정	2023.12.29 ~ 2027.4.28	
	추진개요 및 목적	○ 국가암관리사업본부는 암등록통계, 역학, 삶의 질 향상, 암정보·교육·홍보 등의 업무와 국가암관리정책 및 국가암관리사업 지침 개발, 지역암센터 지원 등 국가암관리사업을 기획하고 평가하는 기능 등을 수행하며 국가암관리종합계획의 성공적인 수행을 뒷받침하는 중추적인 역할을 수행 ○ 내·외부 환경변화에 능동적으로 대응하고 확장성 있는 통합 플랫폼 기반의 클라우드 환경 차세대 정보시스템 구축 ○ 데이터 기반의 암예방, 검진, 치료, 대응의 효율적인 정책수행을 위한 환경 전환으로 기존 정보시스템의 운영한계를 극복하고, 내외부 환경변화에 유연한 대응이 가능한 플랫폼 기반의 정보시스템 구축					
	추진성격	대상여부	① 5만 이상 민감정보·고유식별정보 처리 ② 50만 이상 개인정보파일 연계 ③ 100만 이상 개인정보파일 처리 ④ 기존에 영향평가를 받은 후 변경			추진 예산	34,392,000,000원 (VAT 포함) ※ 전체 사업 예산
		추진주체	차세대정보시스템 구축 추진단				
		추진근거	국립암센터 첨단CT기반의 차세대 정보시스템 구축 사업 계약			추진 유형	☒ 신규 구축 ☒ 변경(고도화) ☐ 운영
		신기술 유형	가상화 서버를 활용한 프라이빗 클라우드 구축				
	주요내용	○ 국가암관리사업본부 정책지원시스템 개발 및 내·외부 인터페이스 ○ 국가암관리사업본부 정책지원시스템 별 기능 개발 - 웹사이트(국립암센터, 국가암정보센터, 중앙호스피스센터) 콘텐츠 개편 및 사용자/관리자 별 기능 개선 - 암환자의료비지원정보시스템 (외부) 사용자 유형별 메뉴 구분 및 업무 수행 기능 개선 (내부) 호스피스·완화의료 사업 현황 정보 제공을 위한 연계 기능 - 호스피스종합정보시스템 (외부) 환자정보, 기관 관리 등 전문기관 사용자 유형별 관리 기능 (내부) 외부 업무 관리 및 교육 관리 등 기능 구성 - 국가암등록통계시스템					

		(외부) 암등록 자료 입력, 검색/다운로드 등 기능 개선 (내부) 외부 업무 관리 및 사용자 관리, 암발생 입력 자료 관리 등 - 중앙암등록본부자료제공시스템 (외부) 병기조사DB, 협력 병기 DB 등 사용자별 메뉴 구성 등 (내부) 외부 업무 관리 및 관리자/회원 계정 관리 등 기능 구성 - 국가암검진사업정보시스템 (외부) 검진 대상자, 검진기관, 검진결과, 수검자 통계 등 기능 구성 (내부) 외부 업무 관리 및 사용자 관리, 공단자료 등록 등 기능 구성 - 암생존자사업시스템 (외부) 권역센터 운영/서비스 운영, 실적통계 등 기능 구성 (내부) 외부 업무 관리 및 회원권한 관리, 권역센터 평가 등 기능 구성 - 발암요인통합정보시스템 (외부) 발암성 평가 협의체 업무 수행, 근거 질 평가 등 기능 구성 (내부) 외부 업무 관리 및 발암성 평가협의체 관리 등 기능 구성 - 암예방수칙근거평가시스템 (외부) 평가 위원회 업무 수행, 근거 질 평가 등 기능 구성 (내부) 외부 업무 관리 및 평가 위원 관리, 문헌 관리 등 기능 구성			
개 인 정 보 파 일 개 요	파일명	정보주체수	개인정보 항목	제3자 제공	개인정보 처리 목적
	국가암검진사업 대상자 및 검진 결과	35,309,049 건	이름:필수, 주민등록번호:필수 기타:필수(증번호, 종별, 암종 별 대상자 여부, 우편번호, 주소, 전화번호, 검진 정보, 문진내역, 검진비용)	-	국가암검진사업 대상자 및 검진결과 관리, 암검진 제도 개선 및 질평가 관련 연구, 국가암검진사업 지원 및 사업담당자 업무 효율 향상
	암환자 의료비지원사업 지원대상자 정보	871,193 건	이름:필수, 집연락처:필수, 집 주소:필수, 핸드폰(연락처):필 수, E-Mail:필수, 주민등록번 호:필수, 건강:필수 기타:필수 (건강정보, 소득 및 재산, 금 융정보, 성별, 계좌번호)	행정안전부, 보건복지부, 국민건강보험공단 등 사회보장급여를 제공하는 국가 및 지방자치단체	암환자 의료비지원사업 지원대상자 관리
	암등록통계파일	2,898,441 건	이름:필수, 집주소:필수, 주민 등록번호:필수 기타:필수(암병 력, 상병코드, 성별, 나이, 직 업, 주소)	-	국가암등록통계사업
	말기환자 보호자정보	17,152 건	이름:필수, 집연락처:필수, 집 주소:필수, 핸드폰(연락처):필 수, E-Mail 기타:필수(성별, 나이)	-	호스피스완화의료사업 의 질평가 및 서비스 개선
	말기환자정보	23,245 건	이름:필수, 주민등록번호:필 수, 건강:필수 기타:필수(종교, 결혼유무, 돌봄제공자, 돌봄 제공자의 관계)	-	호스피스완화의료사업 의 질평가 및 서비스 개선
	호스피스완화의료 전문인력정보	5,899 건	이름:필수, 생년월일:필수, 핸 드폰(연락처):필수, E-Mail:필 수 기타:필수(소속기관, 성별, 직종, 역할, 면허번호, 면허취 득년도, 근무형태, 근무시간, 경력정보, 교육정보)	-	호스피스완화의료 전문기관의 평가 및 기관 담당자 업무 수행

개인정보 처리 흐름분석		대상시스템(사업본부 정보시스템)은 인터넷망에서 Web기반으로 구축 예정 (국가암등록통계시스템) ▶자료입력 : 일년등록자료, 암발생조사자료, 협력병기, 간암병기, 폐암병기 자료 입력 ▶자료생성 : 전연도모자료, 일년자료, 암발생자료 병합, 사망 및 주소정보 정리 ▶조사비용 : 자료수집비, 병기조사자문비 신청 및 지급 관리 (국가암등록자료제공시스템) ▶표본조사자료 : 표본조사자료요청 및 사망원인연계자료 요청의 목록을 조회, 사후조치관리 및 비용청구 ▶맞춤형자료 : 맞춤형자료요청의 목록을 조회, 사후조치관리 및 비용청구 (호스피스종합정보시스템) ▶병상/대기 등록 현황 : 호스피스 병상에 대한 대기신청 환자정보의 목록을 조회/등록/수정 ▶환자정보 : 환자정보 등록, 오입력현황 조회 ▶기관정보 : 기관별 인력정보를 조회/등록/수정 ▶만족도조사 : 사별가족 만족도 조사 설문대상자 및 결과 관리 (국가암검진사업정보시스템 : 공공시스템) ▶공단자료등록 : 국민건강보험공단의 자료를 등록, 대상자 정보 조회 ▶검진대상자 : 검진대상자 및 검진결과 조회 ▶검진기관 : 검진기관별 수검자 조회 (암생존자통합정보시스템) ▶공단자료등록 : 국민건강보험공단의 자료를 등록, 대상자 정보 조회 ▶검진대상자 : 검진대상자 및 검진결과 조회 ▶검진기관 : 검진기관별 수검자 조회 (암환자의료비지원정보시스템 : 공공시스템) ▶등록카드 : 보건소에서 저소득층 암환자의 치료 영수증 확인 후 비급여 병원비에 대하여 지원(환급)함 ▶지원신청 : 저소득층 암환자 대상 의료비 지원자, 지급/환급 내역 조회 (발암요인통합정보시스템) ▶평가관리 : 회원이 평가의뢰 등록한 후보물질에 대하여 심사위원이 평가 내용을 등록함 ▶업무관리 : 발간지 자문의뢰를 위한 전문가(교수)를 관리 (암예방수칙근거평가시스템) ▶평가관리 : 회원이 평가의뢰 등록한 후보물질에 대하여 심사위원이 평가 내용을 등록함 ▶업무관리 : 발간지 자문의뢰를 위한 전문가(교수)를 관리 ※ 참조 : [붙임 1] 개인정보 흐름도(총괄)	
영 향 평 가 기 준	평가기준 변경사항 및 사유	구분	주요 내용
		추가	○ 특정IT 기술 활용 시 개인정보보호 영역 ▪ 공공시스템 (6개 평가항목) (5.7.1~5.7.6) : 시행령, 고시 개정사항 반영
		변경	○ 개인정보 처리단계별 보호조치 영역 ▪ 파기 계획 수립 (3.5.1) : 법률 개정 사항 반영 ○ 대상시스템 기술적 보호조치 영역 ▪ 인증 관리 (4.1.2) : 고시 개정 사항 반영

		▪ 인증 관리 (4.1.5) : 고시 개정 사항 반영 ▪ 안전한 파기 (4.7.1) : 고시 개정 사항 반영 ▪ 개인정보처리 화면 보안 (4.8.2) : 사업 특성 반영
	제외	○ 다른 정보시스템(병원정보시스템) 개인정보 영향평가 수행에 따라 대상기관 개인정보보호 관리체계 영역 생략 ▪ 개인정보 보호 조직 (2개 평가항목) : 1.1.1 ~ 1.1.2 ▪ 개인정보 보호 계획 (3개 평가항목) : 1.2.1 ~ 1.2.3 ▪ 개인정보 침해대응 (2개 평가항목) : 1.3.1 ~ 1.3.2 ▪ 정보주체권리보장 (3개 평가항목) : 1.4.1 ~ 1.4.3 ○ 대상시스템에서 특정 IT기술을 활용한 개인정보 처리업무를 수행하지 않음에 따라 관련 지표 제외 ▪ 고정형 영상정보처리기기 (6개 평가항목) : 5.1.1 ~ 5.1.6 ▪ RFID (7개 평가항목) : 5.2.1 ~ 5.2.7 ▪ 생체인식정보 (2개 평가항목) : 5.3.1 ~ 5.3.2 ▪ 위치정보 (2개 평가항목) : 5.4.1 ~ 5.4.2 ▪ 가명정보 (9개 평가항목) : 5.5.1 ~ 5.4.9 ▪ 이동형 영상정보처리기기 (4개 평가항목) : 5.6.1 ~ 5.6.4
주요 평가기준		○ 대상시스템의 개인정보보호 관리체계 - 개인정보취급자 지정(2.1.1~2.1.2) - 개인정보파일 관리(2.2.1~2.2.2) - 개인정보처리방침(2.3.1~2.3.2) ○ 개인정보 처리단계별 보호조치 - 수집의 적합성(3.1.1~3.1.5) - 동의를 받는 방법의 적절성(3.1.6~3.1.10) - 보유기간 산정(3.2.1) - 개인정보 제공의 적합성(3.3.1~3.3.2) - 목적 외 이용·제공 제한(3.3.3~3.3.6) - 제공시 안전성 확보(3.3.7) - 위탁사실 공개(3.4.1) - 위탁 계약(3.4.2) - 위탁사 관리·감독(3.4.3~3.4.4) - 파기 계획 수립(3.5.1) - 분리·보관 계획 수립(3.5.2) - 파기대장 작성(3.5.3) ○ 대상시스템의 기술적 보호조치 - 계정 관리(4.1.1) - 인증 관리(4.1.2~4.1.7) - 권한 관리(4.1.8~4.1.10) - 접근통제 조치(4.2.1~4.2.5) - 인터넷 홈페이지 보호조치(4.2.6) - 업무용 모바일기기 보호조치(4.2.7)(4.2.7해당없음) - 저장시 암호화(4.3.1~4.3.3)

		- 전송시 암호화(4.3.4) - 접속기록 보관(4.4.1) - 접속기록 점검(4.4.2) - 접속기록 보관 및 백업(4.4.3) - 백신 설치 및 운영(4.5.1) - 보안업데이트 적용(4.5.2) - 출입통제 절차 수립(4.6.1) - 반출·입 통제 절차 수립(4.6.2) - 안전한 파기(4.7.1) - 개발환경 통제(4.8.1) - 개인정보처리 화면 보안(4.8.2) - 출력시 보호조치(4.8.3~4.8.4) - 보호구역 지정(4.9.1~4.9.3) ○ 특정IT 기술 활용시 개인정보 보호 - 공공시스템 내부 관리계획의 수립·시행(5.7.1) - 공공시스템 접근 권한의 관리(5.7.2~5.7.4) - 공공시스템 접속기록의 보관 및 점검(5.7.5~5.7.6)
	평가기준에 따른 개인정보 침해요인 분석·평가	1. 개인정보 보호법 등 관련 법령 준수 사항 ○ 『암관리법』, 『암관리법 시행령』, 『암관리법 시행규칙』, 『국민건강보험법』, 『호스피스·완화의료 및 임종과정에 있는 환자의 연명의료결정에 관한 법률』, 정보주체의 동의에 근거하여 국가 암관리사업 본부 행정업무의 원활한 처리를 위해 암환자 및 보호자, 암검진대상자, 호스피스완화의료 전문인력 및 정보시스템 사용자의 정보를 수집함 ○ 정보주체에게 정확한 정보를 제공하지 못해 개인정보 자기결정권 침해 및 민원 발생 우려가 있음불필요한 접근권한을 부여하게 되며, 개인정보의 오·남용 위험이 증가하고 개인정보 유출등 사고 발생 우려가 있음(2.3.2) ○ 동의 받는 절차를 제대로 준수하지 않아 법적 준거성이 침해될 위험이 있으며, 정보주체의 민원이 증가할 수 있음(3.1.6) 2. 개인정보 처리(위탁 포함)와 기술적 조치사항 ○ 불필요한 정보가 노출되어 외부 공격의 빌미를 제공하여 개인정보 유출등 사고 발생 위험이 증가하며 법적준거성 침해 위험이 있음(4.8.2) ○ 출력물에 포함된 개인정보 유출등 사고 발생시 책임추적성을 확보하기 곤란하여 신속한 대응이 지연되어 피해범위가 증가할 수 있으며, 법적 준거성 침해 위험이 있음(4.8.3)
위험요인에 대한	주요 위험요소에 따른 개선 조치 방안	○ 개인정보 처리방침을 개선해야 함 ○ 필수동의 삭제 및 중요내용 강조 등 개인정보 수집·이용·제공 동의서식 개선, 개인정보 보유기간을 최소화 해야 함 ○ 오른쪽 마우스 버튼 제한 및 캐시 등 임시파일 통제, 외부 사용자에 대해서도 출력물 보호대책을 적용 해야 함

개 선 조 치	위험요소에 따른 정보주체 인지사항	○ 개인정보 수집·이용·제공 시 동의 서식의 중요 내용을 확인하고 자유로운 의사에 의해 명확한 의사를 표현할 수 있어야 함 ○ 각 부서의 개인정보 처리 현황을 개인정보 처리방침을 통해 확인해야 함
평가결과		○ 대상시스템의 개인정보보호 관리체계 - 대상시스템의 개인정보취급자를 최소한 지정 - 개인정보취급자 대상으로 개인정보 보호 서약서를 제출하도록 하고 있으며, 정기적으로 개인정보보호 교육 실시 등 관리·감독 수행 - 개인정보파일을 신규로 보유하거나 작성할 때 개인정보파일대장을 작성 또는 변경하고 있으며, 개인정보 보호위원회에 등록·변경등록 - 개인정보 처리방침을 수립하여 기관 대표 홈페이지에 링크를 통해 공개 - 개인정보 처리방침에 법령 등에 따라 포함하여야 할 사항을 적정하게 공개하고 있지 않음 ○ 개인정보 처리단계별 보호조치 - 대상시스템은 개인정보 수집 시 개인정보 보호법 제15조, 제17조, 제18조, 제22조, 제24조2의 등에 근거하여 적정하게 수집 및 제3자 제공하고 있으며, 관련 동의서식도 정기적으로 점검 개선 - 개인정보 수집·이용 시 필요 최소한의 범위에서만 수집하며, 민감정보를 처리하는 경우 구분하여 동의를 받거나 법령 등에 따라 적법하게 처리 - 고유식별정보(주민등록번호 제외)를 처리하는 경우 다른 개인정보의 처리에 대한 동의와 구분하여 동의를 받거나 법령 등에 따라 적법하게 처리 - 주민등록번호는 법적 근거가 있는 경우에 한하여 처리, 인터넷 홈페이지를 통해 회원가입하는 절차는 평가 대상에 포함되지 않음 - 필수항목에 대해 동의를 받고 있어 자유로운 의사에 따른 동의를 받고 있지 않음 - 14세 미만 아동의 개인정보 수집·이용시 적절한 방법으로 법정대리인으로부터 동의를 받고 있음 - 개인정보 수집·이용·제공 동의서식의 중요내용 강조 - 정보주체의 동의 없이 처리할 수 있는 개인정보의 항목과 정보주체의 동의를 받아 처리하는 개인정보의 항목을 구분하여 개인정보 처리방침을 통해 공개 - 개정된 개인정보 보호법 등에 따른 민감정보 공개가능성에 대한 정보주체 선택 사항을 알릴 수 있는 절차를 개인정보 처리방침에 공개 - 개인정보의 보유기간을 법령 기준 및 보유목적에 부합된 최소한의 기간으로 산정 - 개인정보를 제3자에게 제공하는 경우 정보주체의 동의를 받거나 관련 법률 근거하여 제공하도록 계획하고 있으며, 최소한의 항목으로 제한 - 외부 연계시 개인정보를 암호화 하는 등 안전성 확보조치 적용 - 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우를 별도 동의를 받거나 관련 법률에 근거하도록 계획하고 있고,

이용 목적에 맞는 최소한의 항목으로 제한하도록 설계하고 있고, 목적 외 이용 또는 제3자 제공 시 대표 홈페이지 공지사항을 통해 공개할 것을 계획하고 있음

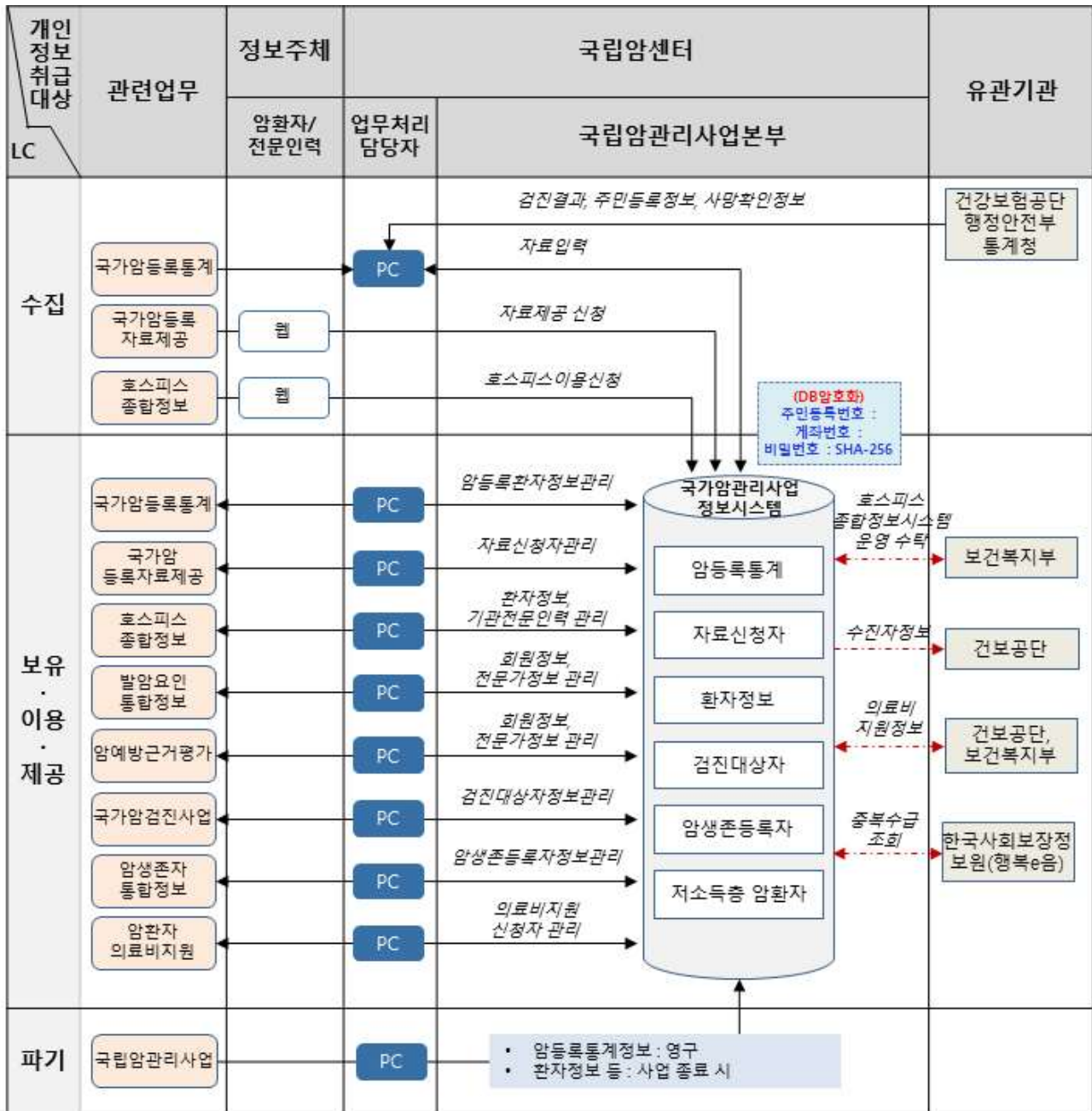
- 개인정보를 목적 외의 용도로 이용 또는 제3자 제공하는 경우 '목적 외 이용 및 제3자 제공 대장'을 기록·관리하고 있지 않음
- 개인정보 보호법 제26조에 따라 개인정보 처리 위탁 절차를 마련하여 준수하고 있으며, 재위탁시 위탁사의 승인을 받도록 정하고 있으며, 수탁사 관리·감독 절차를 마련하여 수행하고 있고, 위탁 사항을 개인정보처리방침을 통해 공개하고 있음
- 개인정보의 보유기간 경과, 처리 목적 달성, 가명정보의 처리 기간 경과 등 그 개인정보 불필요하게 되었을 때 파기 하거나 다른 법령에 따라 분리하여 저장·관리하도록 계획
- 개인정보파일 파기 시 파기 결과를 '개인정보파일 파기 관리대장'에 기록·관리

○ 대상시스템의 기술적 보호조치

- 개인정보 보호법 제29조에 따라 처리하는 개인정보를 안전하게 관리할 수 있도록 관리적·기술적·물리적 보호조치를 계획하고 있음
- 개인정보취급자 별로 책임추적성이 확보될 수 있도록 개별 계정을 부여하고 있음
- 개인정보취급자 인증시 아이디/비밀번호를 사용하고 있으며, 정보주체가 비밀번호 변경 시 비밀번호 재확인 등 추가적인 인증을 적용하고 있고, 비밀번호 작성규칙, 세션 타임아웃, 장기 미접속 시 계정잠금을 적용하고 있음
- 대량의 개인정보 취급자 및 관리자에 강화된 인증방식 적용
- 개인정보취급자 업무 변경시 접근권한을 변경 또는 말소하고 있으며, 접근권한 변경 이력을 3년 이상 보관하도록 계획하고 있고, 메뉴 별로 접근권한을 차등 부여하고 있음
- 개인정보처리시스템에 대한 접근통제를 적용하고 있고, P2P 등 유해사이트 차단을 적용하고 있고, 중요 개인정보취급자의 단말의 인터넷망 접속을 차단하고 있음
- 정보통신망을 통해 외부에서 관리자 페이지에 접속하는 경우 추가적인 인증수단 적용
- 관리용 단말을 지정하고 안전조치를 적용하고 있음
- 인터넷 홈페이지의 취약점 점검 및 대응 조치를 수행하고 있음
- 중요 개인정보 저장 시 안전한 방식으로 암호화 하여 저장하며, 고유식별정보를 개인정보취급자 컴퓨터에 저장 시에도 안전한 알고리즘으로 저장하도록 계획하고 있으며, 암호 키 관리 절차를 수립하고 있음
- 개인정보를 정보통신망을 통해 송·수신하는 경우 암호화 적용
- 개인정보처리시스템의 접속기록을 기록하여 관리하고 있고, 안전하게 보관하기 위한 조치를 접속기록 관리 시스템을 도입하여 적용
- 접속기록 및 다운로드 사유 점검 기준을 수립하여 점검 수행
- 악성프로그램을 점검, 치료할 수 있는 보안 프로그램을 설치하여 운영하고 있으며, 보안 업데이트 공지가 있는 경우 즉시 업데이트가 실시되도록 적용
- 개인정보를 보관하는 물리적 장소에 대한 출입통제 절차를 적용하고

	있고, 개인정보가 포함된 서류를 잠금장치가 있는 안전한 장소에 보관하며, 개인정보가 포함된 보조저장매체의 반출·입 통제 적용 - 개인정보를 파기할 경우 복구·복원되지 않는 방법으로 파기 계획 - 개발 환경을 별도로 구성하고 취약점을 점검하고 테스트 데이터를 주기적으로 파기하도록 계획 - 웹 브라우저 오른쪽 마우스 버튼 통제 미적용 및 임시 파일 개인정보 통제 미적용 - 외부사용자 개인정보 출력 시 출력기관, 출력자, 출력일시, 일련번호를 함께 출력하고 있지 않음 - 개인정보 표출(화면, 파일) 시 최소한의 항목으로 제한하고 있으며, 중요 개인정보에 대해 마스킹을 적용 - 개인정보가 저장된 장소에 출입통제 절차를 수립하여 운영 - 전산실에 보호설치를 설치·운영하고 있으며, 재해·재난 대비 위기대응 절차를 마련하고, 개인정보처리시스템 백업 및 복구를 위한 계획도 수립하여 운영 ○ 특정 IT기술 활용 시 개인정보보호 - 공공시스템 별로 관리책임자를 지정하고, 역할 및 책임에 관한 사항 등 관련 기준에 정한 사항을 포함하여 내부 관리계획을 수립·시행 - 공공시스템에 대한 접근권한을 인사정보와 연계하여 부여할 것을 계획하고 있고, 계정 발급 시 개인정보 보호 교육을 실시하고 보안서약을 받고 있으며, 접근권한 부여, 변경 또는 말소내역을 반기별 1회 이상 점검할 것을 계획 - 공공시스템에 접속한자의 접속기록 등을 자동화된 방식으로 분석하여 개인정보 유출 및 오·남용 시도를 탐지하고 그 사유를 소명하도록 하는 절차를 수립하고 있음(단, 외부에서 이용하는 기관은 없어 이용기관별 개인정보취급자 접속기록 점검 기능은 평가에서 제외) ○ 「사업본부 정보시스템」의 개인정보 침해 위험성을 분석·평가한 결과 개인정보 영향평가 73개 평가항목 중 이행 건수는 68건, 부분이행 건수는 4건, 미이행 건수는 0건, 해당없음 건수는 1건
--	---

[붙임 1] 개인정보 흐름도(총괄)



국립암센터
「사업본부 정보시스템」
개인정보 영향평가 결과보고서
요약본



개인정보영향평가기관 (주)지티시큐