개인정보 영향평가서 요약본

<table>
<tr><td colspan="2">공공기관 명</td><td colspan="6">한국산업안전보건공단 산업안전보건연구원</td></tr>
<tr><td colspan="2">평가기관</td><td>한국전산감리원</td><td>평가
기간</td><td>2023.10.14
~
2023.12.15</td><td>평가
예산</td><td colspan="2">☐ 1천만원 미만
☐ 1천만원 이상 ~ 3천만원 미만
☐ 3천만원 이상 ~ 5천만원 미만
☑ 5천만원 이상 ~ 1억원 미만
☐ 1억원 이상</td></tr>
<tr><td rowspan="6">평가대상시스템 개요</td><td>시스템명</td><td colspan="3">한국산업안전보건공단 K2B시스템
유지관리(1차년도)</td><td colspan="2">시스템 구축 또는
변경 일정</td><td>2023.04.01. ~
2023.12.31.</td></tr>
<tr><td>추진개요
및 목적</td><td colspan="6">○ 산재예방 사업 추진 방식의 변화로 재해예방기관에 대한 위탁·대행 확대에 따른 정보화 지원체계 강화.
○ 재해예방기관 위탁·대행 등의 사업수행 결과에 대한 종합관리 및 분석 시스템의 체계적인 관리.
○ 재해예방기관과 정보 공유 및 교류를 실현하고, 수집되는 정보의 체계적인 관리를 통하여 종합적인 산재예방업무 정보화 지원 체계 강화.
※ K2B(KOSHA To Business) 서비스 : 공단과 기관간 업무 협력을 위해 제공되는 서비스)
- K2B서비스 포털
- 확장형 ERP(Extended ERP) 시스템
: 기관(기업) 내의 모든 자원을 통합 구축한 ERP 시스템의 확장개념으로 기관(기업) 외부의 필요한 자원을 통합하여 최적화 한 시스템</td></tr>
<tr><td rowspan="4">추진성격</td><td>대상여부</td><td colspan="2">▪ 개인정보보호법 시행령 제35조 제1호 5만명 이상 민감정보 또는 고유식별정보 처리
▪ 개인정보보호법 시행령 제35조 제2호 50만명 이상 개인정보파일 연계
▪ 개인정보보호법 시행령 제35조 제3호 100만명 이상 개인정보파일 처리</td><td>추진예산</td><td>800,000,000원
(주관부서 담당자의 M/M기준 추산금액)</td></tr>
<tr><td>추진주체</td><td colspan="2">한국산업안전보건공단</td></tr>
<tr><td>추진근거</td><td colspan="2">▪ 한국산업안전보건공단법
▪ 산업안전보건법
▪ 통계법</td><td>추진유형</td><td>운영/유지보수</td></tr>
<tr><td>신기술
유형</td><td colspan="4">해당 없음</td></tr>
<tr><td>주요내용</td><td colspan="6">○ K2B 서비스 유지보수 대상 업무(특수(임시)건강진단결과 관련)
- 작업환경측정 및 특수건강진단 비용지원 프로그램 기능개선
- 특수건강진단 비용지원 파일 근로자별 개별 전송
- 특수건강진단 및 작업환경측정 심사 프로그램</td></tr>
</table>

<table>
<tr><td></td><td></td><td colspan="4">- 작업환경측정 비용지원 파일 사업연도별 수가 적용
- 작업환경측정 및 특수건강진단 통합 신청에 따른 비용지원 대상 선정
- 사업장 정보, 인적정보 등 현황 자료추출
- 화학물질정보 통합DB 관리
- 위험성 평가(작업환경측정 자료 분석)
- 직업건강 위험진단/정보안내
- 고용노동부 화면 연동</td></tr>
<tr><td></td><td>운용체계 변경내용 (변경인 경우)</td><td colspan="4">해당 없음</td></tr>
<tr><td rowspan="2">개인정보파일개요</td><td>파일명</td><td>정보주체 수</td><td>개인정보 항목</td><td>제3자 제공</td><td>개인정보 처리 목적</td></tr>
<tr><td>특수(임시) 건강진단 결과 파일</td><td>24,942,617 건</td><td>- 필수항목 : 이름, 직장 연락처, 직장주소, 주민 등록번호, 건강진단결과
- 선택항목 : 해당없음</td><td>해당없음</td><td>근로자 직업병 예방 등 산업보건 정책 수립 기초자료 제공</td></tr>
<tr><td>개인정보 처리 흐름분석</td><td colspan="4">■ 개인정보 흐름표
<table>
<tr><th rowspan="2">평가 업무</th><th rowspan="2">프로세스</th><th colspan="3">수집·보유·이용</th></tr>
<tr><th>수집·이용 항목</th><th>수집·이용 대상</th><th>수집·이용 근거</th></tr>
<tr><td rowspan="3">특수(임시) 건강진단 관리 업무</td><td>특검 접수현황 관리</td><td>성명, 주민등록번호(외국인등록번호), 성별, 나이, 생년월일, 사업장명, 부서, 직종, 사원번호, 주소, 전화번호, 문진정보, 진찰내용, 검사결과, 판정내역, 진단의사정보, 핸드폰, 이메일, 국가</td><td>특수(임시) 건강진단 수검 근로자, 진단의사</td><td>-한국산업안전보건공단법 제1조, 제6조
-산업안전보건법 제130조, 제131조, 제134조 제1항, 제165조 제2항
-산업안전보건법 시행령 제117조
-산업안전보건법 시행규칙 제209조 제4항
-근로자 건강진단 실시기준 제16조 제1항, 제2항
-통계법 제20조, 제29조</td></tr>
<tr><td>특검 수검자 명단 조회</td><td>성명, 주민등록번호(외국인등록번호), 성별, 나이, 생년월일, 사업장명, 부서, 직종, 사원번호, 주소, 전화번호, 문진정보, 진찰내용, 검사결과, 판정내역, 진단의사정보</td><td>특수(임시) 건강진단 수검 근로자, 진단의사</td><td>-한국산업안전보건공단법 제1조, 제6조
-산업안전보건법 제130조, 제131조, 제134조 제1항, 제165조 제2항
-산업안전보건법 시행령 제117조</td></tr>
<tr><td>사업장별 검진내역 조회</td><td>성명, 성별, 나이, 사업장명, 판정내역, 진단의사정보</td><td>특수(임시) 건강진단 수검 근로자,</td><td>-한국산업안전보건공단법 제1조, 제6조
-산업안전보건법 제130조, 제131조, 제134조 제1항, 제165조 제2항</td></tr>
</table></td></tr>
</table>

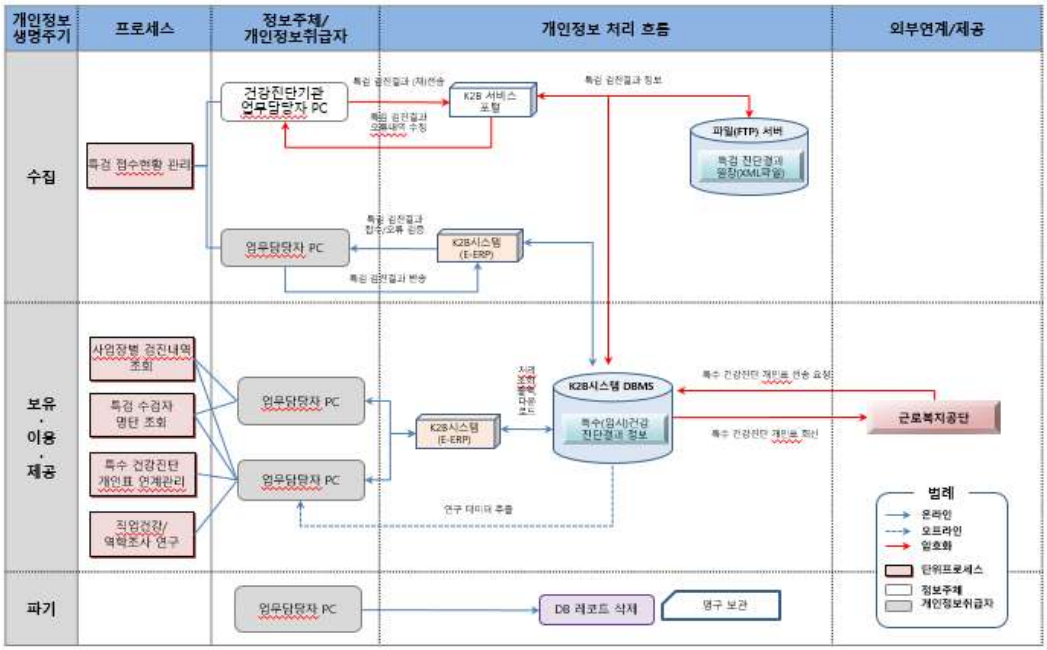
평가 업무	프로세스	수집·보유·이용		
		수집·이용 항목	수집·이용 대상	수집·이용 근거
			진단의사	-산업안전보건법 시행령 제117조
	특수 건강진단 개인표 연계 관리	성명, 주민등록번호(외국인등록번호), 성별, 나이, 생년월일, 사업장명, 부서, 직종, 사원번호, 주소, 전화번호, 문진정보, 진찰내용, 검사결과, 판정내역, 진단의사정보	특수 (임시) 건강진단 수검 근로자, 진단의사	-산업재해보상보험법 제31조 -산업재해보상보험법 시행령 제127조의2 제1호
	직업건강/역학조사 연구	성명, 주민등록번호(외국인등록번호), 성별, 나이, 생년월일, 사업장명, 부서, 직종, 사원번호, 주소, 전화번호, 문진정보, 진찰내용, 검사결과, 판정내역, 진단의사정보, 국가	특수 (임시) 건강진단 수검 근로자, 진단의사	-한국산업안전보건공단법 제1조, 제6조 -산업안전보건법 제130조, 제131조, 제134조 제1항, 제165조 제2항 -산업안전보건법 시행령 제117조

평가 업무	프로세스	제공·연계·위탁			
		제공목적	수신자	제공정보	제공근거
특수 (임시) 건강진단 관리 업무	특검 접수현황 관리	-	-	-	-
	특검 수검자 명단 조회	-	-	-	-
	사업장별 검진내역 조회	-	-	-	-
	특수 건강진단 개인표 연계 관리	업무 관련성 질환 산재심의처리 사실관계 입증자료 제공	근로복지공단	성명, 주민등록번호(외국인등록번호), 성별, 나이, 생년월일, 사업장명, 부서, 직종, 사원번호, 주소, 전화번호, 문진정보, 진찰내용, 검사결과, 판정내역, 진단의사정보	-산업재해보상보험법 제31조 -산업재해보상보험법 시행령 제127조의2 제1호
	직업건강/역학조사 연구	-	-	-	-

평가 업무	프로세스	개인정보파일	파기		
			보유기간	파기절차	분리보관
특수 (임시) 건강진단 관리 업무	특검 접수현황 관리	특수(임시) 건강진단 결과 파일	영구	보유기간이 경과하거나, 처리목적을 달성한 개인정보에 대해 개인정보 보호책임자의 승인을 득하여 파기	-
	특검 수검자 명단 조회				
	사업장별 검진내역 조회				
	특수 건강진단				

평가 업무	프로세스	개인정보파일	파기		
			보유기간	파기절차	분리보관
	개인표 연계 관리				
	직업건강/역학 조사 연구				

■ 개인정보 흐름도



■ 평가기준 점검항목 조정내역

구분	추가 또는 변경 항목		추가 또는 변경 사유
	코드	내용	
항목 추가	1.2.2	개인정보보호책임자는 연1회 이상으로 접근권한관리, 접속기록 보관 및 점검, 암호화 조치 등 내부관리계획의 이행 실태를 점검·관리하고 있습니까?	『개인정보의 안전성 확보조치 기준』 개정 반영(2019.06. 시행)하여 지표 변경.
항목 변경	2.2.2	대상시스템에서 개인정보파일을 신규로 보유하거나 기존파일을 변경하는 경우, 개인정보보호위원회에 등록하도록 계획하고 있습니까?	『개인정보보호법(2023.09. 15. 시행)』 개정사항을 반영하여 지표 변경
	2.3.2	개인정보처리방침은 법률 등에서 규정된 내용을 모두 반영하도록 계획하고 있습니까?	『개인정보보호법(2023.09. 15. 시행)』 개정사항과 같은 법 제20조 제1항을 반영하여 지표 변경
	3.1.1	개인정보를 수집하는 경우 법률에 근거하거나 정보주체의 동의를 받도록 계획하고 있습니까?	『개인정보보호법(2023.09. 15. 시행)』 개정사항을 반영하여 지표 변경
	3.1.5	만14세 미만 아동의 개인정보를 수집하는 경우 법정 대리인의 동의를 받도록 계획하고 있습니까?	상동
	3.1.6	개인정보 관련 동의를 서면 등으로 받을	상동

영향평가기준 변경사항 및 사유

구분	추가 또는 변경 항목		추가 또는 변경 사유
	코드	내용	
		때에는 중요한 내용을 명확히 표시하여 알아보기 쉽게 하고 개인정보 수집·이용, 제3자 제공, 목적 외 이용 등에 대해 각각 구분하여 동의를 받도록 계획하고 있습니까?	
	3.1.7	민감정보, 고유식별정보를 처리하는 경우 다른 개인정보의 처리에 대한 동의와 별도로 구분하여 동의를 받도록 계획하고 있습니까?	상동
	3.3.1	개인정보를 제3자에게 제공하는 경우 법률에 근거하거나 정보주체의 동의를 받도록 계획하고 있습니까?	상동
	3.3.3	개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우 별도의 동의를 받거나 관련 법률에 근거 하도록 계획하고 있습니까?	상동
	3.3.7	개인정보를 제3자(목적 외 제공, 위탁 포함)에게 제공하거나 연계하는 경우 암호화 조치, 보유기간 지정 등 안전성 확보를 위해 필요한 조치를 적용하도록 계획하고 있습니까?	『개인정보보호법(2023.09.15. 시행)』, 『개인정보의 안전성 확보조치 기준(2023.09.22. 시행)』 개정사항을 반영하여 지표 변경
	3.4.1	개인정보 처리에 관한 업무 위탁시 위탁하는 업무의 내용, 수탁자 등의 사항을 정보주체에게 공개 또는 통지하도록 계획하고 있습니까?	『개인정보보호법(2023.09.15. 시행)』 개정사항을 반영하여 지표 변경
	3.4.2	개인정보 처리에 관한 업무 위탁 시 개인정보 관리에 관한 책임사항 등이 포함된 문서를 작성하도록 계획하고 있습니까?	상동
	4.1.1	정당한 사유가 없는 한 개인정보취급자별로 책임추적성이 확보될 수 있도록 개별 계정을 부여하도록 계획하고 있습니까?	『개인정보의 안전성 확보조치 기준』 개정 반영(2023.09.22. 시행)하여 지표 변경.
	4.1.2	개인정보취급자 또는 정보주체의 인증수단을 안전하게 적용하고 관리하도록 계획하고 있습니까?	상동
	4.1.5	정당한 권한을 가진 개인정보취급자 또는 정보주체만이 개인정보처리시스템에 접근할 수 있도록 일정 횟수 이상 인증에 실패한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 조치를 취하고 있습니까?	상동
	4.1.6	개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여	상동

구분	추가 또는 변경 항목		추가 또는 변경 사유
	코드	내용	
		개인정보취급자가 일정시간 이상 업무 처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하는 등 필요한 조치를 계획하고 있습니까?	
	4.1.8	개인정보취급자가 또는 개인정보취급자의 업무가 변경될 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하도록 계획하고 있습니까?	상동
	4.2.3	인터넷 홈페이지, P2P, 공유설정 등을 통해 개인정보가 노출되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터, 모바일기기 등에 보호조치를 계획하고 있습니까?	『개인정보의 안전성 확보조치 기준』 개정 반영(2023.09.22. 시행)하여 지표 변경.
	4.2.4	개인정보처리자는 개인정보 유출 등 개인정보 침해사고 방지를 위하여 관리용 단말기에 대한 안전 조치를 적용하도록 계획하고 있습니까?	『개인정보의 안전성 확보조치 기준』 개정 반영(2023.09.22. 시행)하여 기존 평가항목 삭제.
		개인정보의 유출, 도난 방지 등을 위한 취약점 점검을 수행하도록 계획하고 있습니까?	『개인정보의 안전성 확보조치 기준』 개정 반영(2023.09.22. 시행)하여 지표 변경.
	4.2.5	개인정보를 처리하는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일기기에 비밀번호 설정 등의 보호조치를 계획하고 있습니까?	상동
	4.3.1	인증정보, 고유식별정보 등 중요 개인정보를 저장하는 경우, 안전한 방식으로 암호화 저장하도록 계획하고 있습니까?	상동
	4.3.3	개인정보를 정보통신망 또는 인터넷망 구간으로 송・수신하는 경우 안전한 암호 알고리즘으로 암호화하도록 계획하고 있습니까?	상동
	4.4.1	개인정보처리시스템의 접속기록을 식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등 필요한 사항이 모두 기록되도록 계획하고 있습니까?	상동
	4.4.2	개인정보의 유출・변조・훼손 등에	상동

구분	추가 또는 변경 항목		추가 또는 변경 사유
	코드	내용	
		대응하기 위하여 개인정보처리시스템의 접속기록을 정기적(월 1회 이상)으로 점검하고 있으며, 접속기록 점검 시 다운로드한 것이 확인된 경우 내부관리계획 등으로 정하는 바에 따라 반드시 그 사유를 확인하도록 계획하고 있습니까?	
	4.4.3	개인정보처리시스템의 접속한 기록을 최소 1년 또는 2년 이상 보관하고 위변조 및 도난, 분실되지 않도록 안전하게 보관하기 위한 조치를 하도록 계획하고 있습니까?	『개인정보의 안전성 확보조치 기준』 개정 반영(2023.09.22. 시행)하여 지표 변경.
	4.5.1	개인정보처리단말기에 악성프로그램을 점검, 치료할 수 있는 보안 프로그램을 설치하고 최신업데이트 및 악성프로그램의 주기적 점검 등 대응조치를 실시하도록 계획하고 있습니까?	상동
	4.8.3	개인정보처리시스템에서 개인정보의 출력시용도 특정 및 용도에 따라 출력 항목을 최소화하여야 하며, 개인정보의 출력·복사물을 안전하게 관리하기 위해 필요한 안전조치를 적용하도록 계획하고 있습니까?	상동
항목 제외	5.1.1	CCTV 설치 시 관계 전문가 및 이해관계인의 의견을 수렴하도록 계획하고 있습니까?	CCTV 평가분야의 경우 대상시스템과 연관이 없어 평가 제외.
	5.1.2	CCTV 설치 후 정보주체가 이를 쉽게 인식할 수 있도록 안내판을 설치하거나 홈페이지, 이메일 등을 통해 안내하도록 계획하고 있습니까?	상동
	5.1.3	CCTV 사용 시 임의조작 및 음성녹음을 사용할 수 없도록 계획하고 있습니까?	상동
	5.1.4	CCTV 운영 시 CCTV에 대한 운영·관리방침을 수립하도록 계획하고 있습니까?	상동
	5.1.5	CCTV 관리 위탁 시 개인정보보호에 필요한 전문장비 및 기술을 갖춘 기관을 선정하도록 계획하고 있습니까?	상동
	5.2.1	RFID 태그에 기록된 개인정보를 수집하는 경우 이용자에게 통지하거나 알아보기 쉽게 표시하도록 계획하고 있습니까?	RFID 평가 분야의 경우 대상시스템과 연관이 없어 평가 제외
	5.2.2	RFID 태그의 물품정보 등과 개인정보를 연계하는 경우 그 사실을 이용자에게 통지하거나 알기 쉽게 표기하도록	상동

<table>
<tr><td></td><td></td><td>
<table>
<tr><th rowspan="2">구분</th><th colspan="2">추가 또는 변경 항목</th><th rowspan="2">추가 또는 변경 사유</th></tr>
<tr><th>코드</th><th>내용</th></tr>
<tr><td></td><td></td><td>계획하고 있습니까?</td><td></td></tr>
<tr><td></td><td>5.2.3</td><td>RFID 태그의 물품정보 등과 개인정보를 연계하여 생성된 정보를 수집 목적 외로 이용하거나 제3자에게 제공할 경우 이용자의 동의를 얻도록 계획하고 있습니까?</td><td>상동</td></tr>
<tr><td></td><td>5.2.4</td><td>RFID 태그에 기록된 개인정보를 판독할 수 있는 리더기를 설치한 경우 설치 사실을 이용자가 인식하기 쉽게 표기하도록 계획하고 있습니까?</td><td>상동</td></tr>
<tr><td></td><td>5.2.5</td><td>구입 및 제공받은 물품에 RFID 태그가 내장 및 부착 되어 있을 경우 부착 위치, 기록정보 및 기능에 대해 표시하도록 계획하고 있습니까</td><td>상동</td></tr>
<tr><td></td><td>5.2.6</td><td>RFID 태그가 내장 및 부착되어 있는 경우 판매 혹은 제공하는 자로부터 태그 기능을 제거할 수 있는 방법 또는 수단을 제공하도록 계획하고 있습니까?</td><td>상동</td></tr>
<tr><td></td><td>5.2.7</td><td>이용자의 신체에 RFID를 지속적으로 착용하지 않도록 계획하고 있습니까?</td><td>상동</td></tr>
<tr><td></td><td>5.3.1</td><td>수집된 바이오 원본정보와 제공자를 알 수 있는 신상정보(성명, 연락처 등)를 별도로 분리하도록 계획하고 있습니까?</td><td>바이오정보 평가 분야의 경우 대상시스템과 연관이 없어 평가 제외</td></tr>
<tr><td></td><td>5.3.2</td><td>원본정보의 경우 특징정보 생성 후 지체 없이 파기하여 복원할 수 없도록 계획하고 있습니까?</td><td>상동</td></tr>
<tr><td></td><td>5.4.1</td><td>개인위치정보 수집 시 정보주체 또는 위치정보 수집장치 소유자에 대해 사전고지와 명시적 동의를 거치도록 계획하고 있습니까?</td><td>위치정보 평가 분야의 경우 대상시스템과 연관이 없어 평가 제외</td></tr>
<tr><td></td><td>5.4.2</td><td>개인위치정보를 정보주체가 지정하는 제3자에게 제공하는 경우에는 개인위치정보주체에게 제공받는 자, 제공일시 및 제공목적을 통보하도록 계획하고 있습니까?</td><td>상동</td></tr>
</table>
</td></tr>
<tr><td></td><td>주요
평가기준</td><td>▪ ‘개인정보보호법(2023.09.15. 시행)’
▪ ‘개인정보보호법 시행령(2023.09.15. 시행)’
▪ ‘개인정보의 안전성 확보조치 기준(2023.09.22. 시행)’
▪ ‘개인정보 처리방법에 관한 고시(2023.10.16. 시행)’
▪ ‘(개인정보보호위원회) 표준 개인정보보호지침(2020.8.11. 시행)’
▪ ‘개인정보영향평가에 관한 고시(2023.10.16. 시행)’
▪ ‘개인정보 영향평가 수행안내서(2020.12. 개정)’
▪ ‘개인정보 처리방침 작성지침(2022.3. 개정)’</td></tr>
<tr><td colspan="2">평가기준에 따른 개인정보 침해요인</td><td>1. 개인정보 보호법 등 관련 법령 준수 여부에 대한 분석평가
• 개인정보취급자 관리(개인정보보호법 제28조, 개인정보의 안전성 확보조치 기</td></tr>
</table>

분석·평가	준 제4조), 개인정보파일 관리(개인정보보호법 제32조, 개인정보보호법 시행령 제33조), 개인정보 처리방침(개인정보보호법 제30조, 개인정보보호법 시행령 제31조)은 관련 법령에서 요구하는 사항을 적절히 준수하고 있음 - 다만, 개인정보취급자 대상 역할 및 책임 부여, 개인정보파일대장 작성항목, 개인정보 처리방침 공개내용에 대한 일부 보완이 필요 • 개인정보 수집(개인정보보호법 제15조, 제16조, 제24조의2, 제22조, 제23조, 제24조), 보유(표준개인정보보호지침 제60조), 이용·제공(개인정보보호법 제17조, 제18조, 제19조, 제29조), 위탁(개인정보보호법 제26조, 제30조), 파기(개인정보보호법 제21조)는 관련 법령에서 요구하는 사항을 적절히 준수하고 있음 - '특수(임시) 건강진단결과 파일' 개인정보파일은 개인정보 수집 시 개별 법령(한국산업안전보건공단법 제1조, 제6조, 산업안전보건법 제130조, 제131조, 제134조, 제165조, 산업안전보건법 시행령 제117조, 산업안전보건법 시행규칙 제209조, 근로자 건강진단 실시기준 제16조, 통계법 제20조, 제29조)에 근거하여 적법하게 수집·이용하고 있으며, 근로복지공단에 개인정보 제공 시 개별 법령(산업재해보상보험법 제31조, 산업재해보상보험법 시행령 제127조의2)에 근거하여 적법하게 제공하고 있음 • 개인정보에 대한 접근권한 관리(개인정보보호법 제23조, 개인정보의 안전성 확보조치 기준 제5조, 제6조), 접근통제(개인정보의 안전성 확보조치 기준 제6조, 제10조), 개인정보의 암호화((개인정보보호법 제23조), 악성프로그램 등 방지(개인정보보호법 제29조, 개인정보의 안전성 확보조치 기준 제9조), 물리적 접근방지(개인정보보호법 제29조, 개인정보의 안전성 확보조치 기준 제11조), 개인정보의 파기(개인정보보호법 제21조, 개인정보의 안전성 확보조치 기준 제13조), 개인정보처리구역 보호(개인정보의 안전성 확보조치 기준 제12조)는 관련 법령에 따라 적법하게 처리하고 있음 - 다만, 고유식별정보 저장시 암호화, 접속기록 보관 및 점검, 서버시스템의 최신 보안 업데이트 관리, 출력물 보안대책, 관리자에 대한 비정상 접근방지, 개인정보 처리화면 보안대책 등에 대한 일부 보완이 필요 **2. 개인정보 처리, 개인정보처리시스템 운영관리 및 기술적 조치사항에 따른 분석평가** • [개인정보 처리단계별 조치사항]

구분	개인정보보호 조치사항
수집	- 법률의 특별한 규정, 법령상 의무준수, 법령 등에서 정한 소관업무 수행을 위해 법령에 근거하여 정보주체의 개인정보를 목적에 필요한 최소한의 범위에서 수집·이용하고 있음 - 고유식별정보, 민감정보는 법령에 근거하여 처리하고 있음
보유	- '공공기록물 관리에 관한 법률 시행령'과 '표준 개인정보보호지침'의 별표에서 제시하고 있는 책정 기준에 근거하여 보유기간 산정
이용·제공	- 법령에 근거하여 목적에 맞는 최소한의 항목만 제공하고 있으며, 제공받는 자(위탁 포함)에 대한 이용 제한, 제공사항 기록, 전용선을 통한 전송 등 안전성 확보를 위해 필요한 조치를 적용하고 있음

구분	개인정보보호 조치사항
위탁	- 개인정보 처리업무 수탁자에 대한 위탁계약, 개인정보보호 서약서 징구, 개인정보보호 교육, 주기적인 실태 점검을 수행하고 홈페이지 개인정보 처리방침에 위탁내용을 공개하고 있음
파기	- 내부관리계획에 따라 보유기간이 경과하거나, 처리목적을 달성한 개인정보에 대해 개인정보 보호책임자의 승인을 득하여 파기하도록 계획하고 있으며, 보유기간이 영구로 책정되어 있어 파기가 발생하지 않음

- [개인정보처리시스템 운영관리 및 기술적 조치사항]

구분	개인정보보호 조치사항
접근권한 관리	- 계정관리, 권한관리는 안전성 확보를 위해 필요한 조치를 적용하고 있음 - 다만, 인증관리의 일부 항목은 개선을 권고함.
접근통제	- 접근통제 조치, 업무용 모바일 기기 보호조치 등은 안전성 확보를 위해 필요한 조치를 적용하고 있음
개인정보의 암호화	- 전송시 암호화 부분은 안전성 확보를 위해 필요한 조치를 적용하고 있음 - 특검진단결과 파일 저장시 일부 암호화 적용이 필요함
접속기록의 보관 및 점검	- 접속기록 보관은 안전성 확보를 위한 조치를 취하고 있으나 - 접속기록의 점검주기 및 보존기간에 대하여 안전성 확보조치 기준을 준수토록 함.
악성 프로그램 등 방지	- 백신 설치 및 운영 항목은 양호하나 서버 및 DBMS보안 업데이트 등에 대한 관리체계 구축이 필요함.
물리적 접근 방지	- 안전성 확보를 위해 적절한 조치를 취하고 있음
개인정보의 파기	안전성 확보를 위해 적절한 조치를 취하고 있음
기타 기술적 보호조치	- 개인정보 처리화면, 출력시 보호조치 일부 항목에 대하여 개선을 권고함.
개인정보 처리구역 보호조치	안전성 확보를 위해 적절한 조치를 취하고 있음

3. 개인정보 침해에 따른 위험요소 사항

구분	침해요인
개인정보보호계획	개인정보보호 활동에 대한 연간 수행 계획의 수립·시행 및 책임자 보고 활동이 미흡한 경우 체계적이고 지속적인 개인정보보호 관리 미흡에 따른 침해사고가 발생할 가능성이 높아짐
정보주체권리보장	정보주체 요구에 대한 개인정보처리자의 조치에 불복이 있는 경우 이의를 제기할 수 있는 절차의 마련 및 안내가 미흡한 경우 정보주체의 정당한 권리 행사를 저해할 우려가 있음
개인정보취급자 관리감독	개인정보취급자에게 법률 등에서 규정된 업무에 대한 구체적인 역할 부여가 미흡한 경우, 개인정보 취급에 대한 중요성이나 책임에 대한 인식이 소홀해지기 쉬움
개인정보파일 대장관리	보유하거나 변경되는 개인정보파일에 대해 개인정보파일 대장의 필수항목 작성이 미흡한 경우, 개인정보파일 현황을 정확하게 파악하지 못하고 이에 따른 보호조치를 적절히 적용할 수 없게 될 우려가 있음
개인정보처리 방침의 작성	개인정보처리방침은 법률 등에서 규정한 사항을 모두 포함하여 오류 및 누락사항 없이 공개되어야 하는데, 이를 준수하지 못할 경우 정보주체의 개인정보 자기결정권과 알권리를 침해할 우려가 있음
접근권한 관리	대상시스템의 비정상적인 접근을 방지하기 위한 관리자 로그인 알림 등의 보호대책이 적용하지 않을 경우 계정 도용, 비인가자에 의한 접근 등에 따른 개인정보의 유·노출, 변조, 훼손 등의 침해사고가 발생할 우려가 있음.
접근통제	안전성 확보를 위해 적절한 조치를 취하고 있음
개인정보의 암호화	중요정보가 포함된 자료를 암호화 하지 않고 보관하게 되면 인가된 개인정보취급자 외의 인원도 중요한 개인정보에 쉽게 접근하게 되어 개인정보 유출 및 침해, 위·변조 위험성이 있음.
접속기록의 보관 및 점검	개인정보 유출, 변조, 훼손 등에 대응하기 위한 접속기록 점검계획 및 활동이 미흡한 경우, 비인가자에 의한 개인정보 처리, 대량의 개인정보 조회, 다운로드, 삭제 등의 비정상적 개인정보 처리에 대한 탐지·대응·관리 미흡에 따른 침해사고 발생 가능성이 높아짐.
악성 프로그램 등 방지	사용 중인 응용프로그램 및 운영체제 소프트웨어 등에 최신의 보안 업데이트를 적용하지 않으면 신종 바이러스나 해킹을 당하고 정보 유출의 위험이 큼
물리적 접근 방지	안전성 확보를 위해 적절한 조치를 취하고 있음

구분	침해요인
개인정보의 파기	안전성 확보를 위해 적절한 조치를 취하고 있음
기타 기술적 보호조치	- 웹 브라우즈 우측마우스 버튼 제한 등의 보안기능이 적용되지 않을 경우 다양한 개인정보의 노출 위험이 발생할 수 있음 - 중요 개인정보가 포함되어있는 문서를 PC에서 출력할 경우 인쇄자, 인쇄일시 표시(최소 조건), 워터마킹 기능이 적용되지 않으면 문서 유출에 대한 책임추적성을 확보하기가 어려워짐
개인정보 처리구역 보호조치	안전성 확보를 위해 적절한 조치를 취하고 있음

위험요인에 대한 개선조치

주요 위험요소에 따른 개선조치 방안

구분	개선과제	개선내용
대상 시스템의 개인 정보 보호 관리 체계	개인정보파일 대장 보완 및 개인정보보호 위원회 변경등록 이행	- 평가대상 업무에서 운용하고 있는 개인정보파일대장의 운영근거, 운영목적, 개인정보항목, 제공받는 자 작성항목에 대해 보완하고, 개인정보보호위원회에 변경등록 하는 절차 이행 권고
대상 시스템의 개인 정보 보호 관리 체계	홈페이지 개인정보 처리방침 공개내용 보완	- 개인정보 처리방침의 개인정보 처리목적·보유항목·보유기간, 개인정보의 제 3 자 제공에 관한 사항, 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항, 개인정보의 열람청구를 접수·처리하는 부서 등 잘못 안내하고 있거나 누락된 내용을 보완하여 정보주체에게 관련사항을 오류 및 누락 없이 공개
대상 시스템의 개인 정보 보호 관리 체계	개인정보 내부관리계획 보완	- 법률 등에서 규정된 개인정보취급자 역할 중 '표준 개인정보보호지침' 제 52 조, 제 56 조에 따른 역할 누락 사항을 내부관리계획에 명시
접근권한 관리	관리자에 대한 비정상 접근방지 보호대책 적용 권고	대상시스템의 비정상적인 접근을 방지하기 위한 관리자 로그인 알림 등의 보호대책 적용을 권고함.
접근통제	해당 없음	해당 없음
개인정보의 암호화	고유식별정보 저장시 암호화 보호대책 적용	건강진단기관으로부터 수집된 중요정보의 서버 저장시 암호화 보호대책을 적용함.
접속기록의 보관 및 점검	접속기록 보관 및 점검 활동 보호대책 강화	- 서버 및 DBMS 접속기록의 점검방법, 점검기준, 점검 주기/시점, 담당자, 비정상 행위 발견 시 대응 절차, 보고 절차 등이 포함된

<table>
<tr><td></td><td></td><td>
<table>
<tr><th>구분</th><th>개선과제</th><th>개선내용</th></tr>
<tr><td></td><td></td><td>접속기록 점검계획을 수립하고, 그 계획에 따라 월 1 회 이상 접속기록을 점검하여 개인정보보호 책임자에게 보고하는 절차를 이행하여야 함.
- 서버 및 DBMS 접속기록의 위·변조, 분실, 도난 방지를 위해 접속기록을 2 년 이상 보관하도록 함</td></tr>
<tr><td>악성 프로그램 등 방지</td><td>서버시스템의 최신 보안 업데이트 관리</td><td>서버 및 DBMS 등에 대해 최신 보안 업데이트 등 보안패치를 수행할 수 있는 관리체계를 운영토록 함.</td></tr>
<tr><td>물리적 접근 방지</td><td>해당 없음</td><td>해당 없음</td></tr>
<tr><td>개인정보의 파기</td><td>해당 없음</td><td>해당 없음</td></tr>
<tr><td>기타 기술적 보호조치</td><td>- 개인정보 처리화면 보안대책 적용
- 출력물 보안대책 적용</td><td>- 처리화면을 통한 개인정보 유·노출 등을 방지하기 위하여 개인정보 마스킹, 웹브라우저 우측 마우스 버튼 제한, 임시 파일 및 캐시 통제 등 보호대책의 적용을 권고함.
- 개인정보가 포함된 출력·복사물에 대한 안전조치로서 인쇄자, 인쇄일시 표시 등 보안대책 및 워터마킹 기능의 적용을 권고함.</td></tr>
<tr><td>개인정보 처리구역 보호조치</td><td>해당 없음</td><td>해당 없음</td></tr>
</table>
</td></tr>
<tr><td></td><td>위험요소에 따른 정보주체 인지사항</td><td>해당 없음</td></tr>
<tr><td colspan="2">평가결과</td><td>○ 평가항목별로 이행여부를 점검한 결과,
• 대상기관 K2B시스템의 특수(임시) 건강진단 관리 업무에 대한 개인정보 영향평가 결과는 평가대상 항목 총 68개 평가항목 중 이행 44개, 부분이행 11개, 미이행 1개, 해당없음 12개로 평가되었으며, 해당없음을 제외한 56개 항목의 이행률은 88%로 확인되었음.
• 개인정보 침해요인을 도출한 결과 대상기관 개인정보보호 관리체계 2건, 대상시스템의 개인정보보호 관리체계 3건, 대상시스템의 기술적 보호조치 7건 등 총 12건의 개인정보 침해요인을 도출하였음
- 개선과제는 단기 조치사항 6건, 장기 조치사항 3건이 도출되었으며, 제시된 개선계획을 참조하여 자체 실행계획을 수립하고 개선 및 보완이 필요함.

○ 대상기관 개인정보보호 관리체계 점검 결과,
• 대상기관 개인정보보호 관리체계(1장)는 9개 평가항목 중 이행 항목 7개, 부분이행 항목 1개, 미이행 항목 1개로 평가되어 일부 개선이 필</td></tr>
</table>

	요한 사례가 식별됨. • 이에 따라, ①홈페이지 개인정보 처리방침 공개내용 보완, ②내부관리계획 및 개인정보보호 연간계획 보완의 개선과제가 도출됨. ○ **대상시스템의 개인정보보호 관리체계 점검 결과,** • 대상시스템 개인정보보호 관리체계(2장)는 6개 평가항목 중 이행 항목 3개, 부분이행 항목 3개로 평가되어 일부 개선이 필요한 사례가 식별됨. • 이에 따라, ①개인정보파일대장 보완 및 개인정보보호위원회 변경등록 이행, ②홈페이지 개인정보 처리방침 공개내용 보완, ③개인정보 내부관리계획 보완의 개선과제가 도출됨. ○ **개인정보 처리단계별 보호조치에 대한 점검 결과,** • 개인정보 처리단계별 보호조치(3장)는 21개 평가항목 중 이행 항목 11개, 해당없음 항목 10개로 평가되어 양호한 상태로 확인됨. ○ **대상시스템의 기술적 보호조치 점검 결과,** • 대상시스템 개인정보보호 관리체계(2장)는 6개 평가항목 중 이행 항목 3개, 부분이행 항목 3개로 평가되어 일부 개선이 필요한 사례가 식별됨. • 이에 따라, ①개인정보파일대장 보완 및 개인정보보호위원회 변경등록 이행, ②홈페이지 개인정보 처리방침 공개내용 보완, ③내부관리계획 및 개인정보보호 연간계획 보완의 개선과제가 도출됨.