BAYADA®
Home Health Care

Compassion. Excellence. Reliability.

Data Protection

목차

학습목표

1. Data Protection 의 정의와 중요성을 확인한다.
2. BAYADA Data Protection을 확인하고 실제 업무에 적용한다.
3. Data Protection 실천수칙을 이해하고 업무 중에 실천한다.

개인데이터란?

BAYADA Home Health Care

개인데이터란 무엇입니까?

개인데이터는 직간접적으로 해당 데이터에서 식별할 수 있는 개인과 관련된 모든 데이터(종이 및 전자 형식 포함)로 정의한다.

직접적으로 식별 가능한 정보(이름, 주민등록번호, 거주지)와 개인을 식별하기 위해 두 가지 이상의 데이터가 필요한 정보를 통틀어 개인정보로 취급한다.

사진출처: CCTV뉴스(보안뉴스) 데이터가 돈이 되는 시대, 당신의 개인정보 '얼마에 제공하겠습니까?' 기사

개인정보의 정의

사진출처: 이글루 > 개인정보보호법 동향

개인정보호보법 제2조(정의)

1. “개인정보”란 살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다.

가. 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보

나. 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보. 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다.

(중략)

개인정보의 처리 절차

BAYADA Home Health Care

01 개인정보의 수집

서비스 제공에 필요한 최소한의 개인정보를 동의절차 수행(명시적인 서면 또는 녹취) 후, 수집한다.

02 개인정보의 이용

이용자에게 동의 받은 목적으로만 개인정보를 이용한다.

03 개인정보의 삭제

수집 및 이용목적이 달성된 이용자의 개인정보는 지체없이, 그리고 안전하게 삭제한다.

04 동의자의 권리 보호

동의자(환자 또는 고객) 의 ' 개인정보 자기결정권 ' 을 보장한다.
동의자는 언제든지 자신의 개인정보를 조회하거나 수정·삭제, 처리정지, 수집 및 이용 동의를 철회할 수 있다.

개인정보의 처리 기준

BAYADA Home Health Care

BAYADA는 OECD Privacy Guidelines 등의 국제 기준을 준수한다.

사진출처: divinalaw site > Compliance with Data Privacy Act

- OECD Privacy Guidelines

개인 데이터 수집에는 제한이 있어야 하며, 이러한 데이터는 합법적이고 공정한 방법으로, 그리고 적절한 경우 데이터 주체의 동의를 통해 획득되어야 한다.

(중략)

개인 정보는 다음을 제외하고 명시된 목적 이외의 목적으로 공개, 제공 또는 사용되어서는 안 된다.

a) 데이터 주체의 동의를 얻은 경우

b) 다른 법률에서 예외를 명시한 경우

전문 : https://www.oecd.org/digital/privacy/

개인정보의 분류

	개념	활용가능범위
개인정보	특정 개인에 관한 정보, 개인을 알아볼 수 있게 하는 정보	사전적이고 구체적인 동의를 받은 범위 內 활용가능
가명 정보	추가 정보의 사용 없이는 특정 개인을 알아볼 수 없게 조치한 정보	다음 목적에 동의 없이 활용 가능 1. 통계작성(상업적 목적 포함) 2. 연구(산업적 연구 포함) 3. 공익적 기록 보존 목적 등
익명 정보	더 이상 개인을 알아볼 수 없게 (복원 불가능할 정도로) 조치한 정보	개인정보가 아니기 때문에 제한없이 자유롭게 활용

개인정보의 분류

BAYADA Home Health Care

개인정보/가명정보/익명정보 구분 방법

01 개인정보(동의서를 받은 경우에만 사용)
성명, 나이, 주소 등을 통하여 개인을 알아볼 수 있는 정보
예) 홍길동/35세/남성/경기도 분당시 불정로 6/식당운영/월소비액 100만원

02 가명정보(통계 업무 등에 사용)
처리된 개인정보 추가 없이는 특정 개인을 식별할 수 없는 정보
예) 20번 손님/35세/자영업/경기도 분당시 거주/월소비액 150만원

03 익명정보(자유롭게 사용)
추가적인 정보와 결합을 통해 재식별이 불가능한 정보
예) 30대/남성/경기도 분당시 거주/월소비액 100~200만원

민감정보의 정의

사진출처: 이코노미조선 기사 전자의무기록(EMR) 기업, 데이터 결국 잘 활용해야 생존한다

개인정보 보호법 제 23조(정의)

민감정보란 ① 사상•신념, ② 노동조합•정당의 가입•탈퇴, ③ 정치적 견해, ④ 건강, 성생활 등에 관한 정보, ⑤ 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령이 정하는 정보를 의미한다.

(중략)

이러한 민감정보는 아무래도 다른 개인정보 항목과 비교하여 보다 민감(Sensitive)하여, 침해나 유출 시 정보주체의 프라이버시에 보다 큰 영향을 미칠 수 있기 때문에 일반 개인정보와 구분하여 그 처리를 보다 엄격하게 규정하고 있다.

민감정보의 처리

민감정보의 처리 권한 및 사용(환자의 진료기록 등)

01 정보주체의 별도 동의가 있는 경우
다른 개인정보의 처리와 분리하여 민감정보 처리에 대해 정보주체가 이를 명확히 인지하고 명시적으로 자신의 동의 의사를 밝힌 경우

02 다른 법률에서 명시적으로 민감정보 처리를 요구하거나 허용하는 경우
다른 법령에서 민감정보의 처리를 구체적으로 언급하고 있거나 해석 상 요구되는 경우

▶ 민감한 개인정보를 수집 또는 처리함에 있어 구체적인 동의(즉, 처리활동 이전에 민감정보 처리 동의)가 명시적인 서면 또는 녹취 등으로 필요함

Data Protection 이란?

BAYADA Home Health Care

Data Protection은 'Data Privacy'와 'Data Security'으로 구성된다.

Data Protection	Data Privacy	Data Security
"데이터 보호" 데이터 가용성, 불변성, 보존, 삭제/파괴, "데이터 개인 정보 보호" 및 "데이터 보안"을 포함	"데이터 개인정보 보호" 개인이 자신의 데이터에 액세스, 사용 또는 공유하는 방법을 제어할 수 있도록 함으로써 개인 데이터의 적절한 사용을 보장	"데이터 보안" 적절한 기술 제어, 메커니즘 및 절차를 구현하여 무단 액세스, 사용 또는 파괴로부터 데이터를 보호

BAYADA Data Protection_Server

BAYADA Home Health Care

Category	Email	SharePoint	CRM
Data Privacy	개인별 계정 발급 Password 주기적 변경, 암호화	부서별 폴더운용, 자료실 접근 제한	Password 6개월 주기 변경 그룹 별 접근 권한 제한
Data Security	IDC 내 클라우드 네트워크 서버 운용 SSL/TLS를 사용한 동적 암호화를 통해 사용자와 Microsoft 간에 전송되는 데이터 보호 Office 365 메시지 암호화		KT Bizmeka 콜센터 솔루션 사용 (KT Firewall, Cloud 보안 정책 적용) 접속 허가 IP 리스트 관리 SSL 암호화 통신
Data Backup	Office 365 모든 사서함 DB는 여러 데이터 센터로 복제되어 보호	SharePoint Online 데이터 백업은 12시간 마다 수행되며 14일 동안 보존	CRM 데이터는 매일 백업

BAYADA Data Protection_PC

Category	Laptop PC
Data Privacy	PC 사용시, 로그인 ID/비밀번호 설정
Data Security	정품 프로그램 사용(Windows, Microsoft Office 365 등)
	백신 프로그램 사용(바이러스, 랜섬웨어 방지)
	운영체제 및 백신프로그램은 자동 업데이트 설정
	Exchange Online Protection(MS 스팸방지기술) 적용

BAYADA Data Protection_회사(1)

BAYADA Home Health Care

01 업무연속성계획(Business Continuity Planning) 수립

재난(감염병 등) 발생으로 갑작스러운 위기 상황에서도 조직이 제공하는 모든 업무 영역에 대한 연속성을 유지하기 위한 계획
Email, SharePoint, CRM 등의 개인정보 데이터 손실 등의 피해를 방지한다.

02 전 직원 대상 개인정보보호 교육 실시

개인정보의 수집・유출・오용・남용으로부터 사생활의 비밀 등을 보호함으로써 권리와 이익을 증진하고, 나아가 개인의 존엄과 가치를 구현하기 위하여 개인정보 처리에 관한 사항을 교육한다.

03 외부메일 필터링 적용(보안정책)

메일 보안을 강화하여 스팸 메일 주소 및 악성 도메인의 외부 메일을 자동 격리한다.
메일 첨부파일 바이러스, 악성코드 탐지(MS EOP 적용)

*MS EOP(Exchange Online Protection) : 스팸, 맬웨어 및 기타 이메일 위협으로부터 보호하는 클라우드 기반 필터링 서비스

BAYADA Data Protection_회사(2)

BAYADA Home Health Care

04 고객 정보, 전송 트래픽 암호화 처리(보안정책)

SSL/TLS 동적 암호화를 적용하여 사용자와 Server 간에 전송되는 데이터를 보호한다.

05 보안 사고 대응 계획 및 통보 절차 수립

데이터 침해사고에 신속하게 대응하기 위한 준비와 대응절차를 기술하여 침해사고로부터의 피해를 최소화하고 후속 보안 대책을 세울 수 있도록 하는데 그 목적이 있음. 적절하지 못한 사고대응은 지속적인 해킹사고를 야기하게 되며, 이에 따른 고비용을 초래하게 된다.

06 안티바이러스 기술 적용(EDR, Endpoint Detection and Response 소프트웨어 사용)

백신프로그램 알약을 사용하여 실시간 분석 및 AI 기반 자동화를 사용하여 사이버 위협으로부터 조직의 데이터를 보호한다.

BAYADA Data Protection_IT(Data Privacy)

사진출처: The CyberArk Blog » Data Privacy Day: Data Protection Lessons from the 2010s

01 접속 계정(ID) 발급, 엑세스 권한 관리(SharePoint, Outlook)

IT 내부적인 절차에 따라 접속 계정(ID)의 발급, 데이터 접근 권한 부여 등의 프로세스 진행한다.

02 CRM 접속 권한 IP 리스트 관리, Password 변경(연2회)

KT Firewall을 통하여 접속 허가 IP 리스트 관리, CRM 접속 계정의 Password 변경을 진행한다.

BAYADA Data Protection_IT(Data Security)

사진출처: loginradius Blog - 9 Data Security Best Practices For your Business

01 System 오류 또는 보안사고 발생시, 복구하며 근본 원인 분석하여 보고함

IT 내부적인 절차에 따라 해당 업체에 연락 하고 사고 보고서 등의 문서를 받아 내용을 정리하고 기록 및 보고한다.

02 월간 유지보수 리포트를 검수

매월 CRM 월간 유지보수 리포트를 검수하여 시스템 점검, 보안 이슈 등의 내용을 확인한다.

03 녹취 파일(Call Center), 백업자료(SharePoint) 관리

Call Center 녹취 파일 이중화 관리, SharePoint 자료 백업 및 모니터링을 통하여 업무의 안정화 추구한다.

BAYADA Data Protection_직원(1)

BAYADA Home Health Care

01 메일, MS365 프로그램 / SharePoint 로그인 및 사용

내부적인 보안정책에 따라 직원은 로그인 및 개인정보 데이터를 사용함. 보안은 SSL/TLS 암호화 처리됨. 또한 발급된 MS365 ID의 Password를 주기적으로 변경하여 피싱 사고 등을 방지한다.

02 꼭 필요한 경우에만 SharePoint 內 개인정보 포함된 문서열람

개인정보를 처리하는 직원은, 동의를 받은 범위로만 활용하며 별도로 정보를 수집하는 행위 등을 지양한다.

사진출처: Microsoft

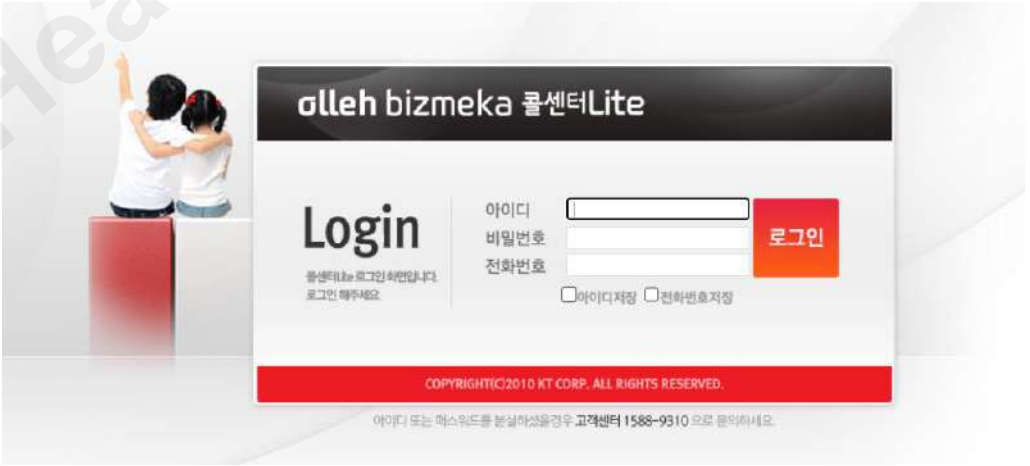
BAYADA Data Protection_직원(2)

03 환자 및 고객의 개인정보 동의서 확인 및 보관

담당하고 있는 환자 또는 보호자의 개인정보, 민감정보 (진료기록 등) 업무상 필요한 경우, 개인 정보 동의절차를 수행한다.(명시적인 서면 또는 녹취 등)

04 업무상 필요한 경우에만 CRM 개인정보 데이터 사용

CRM은 환자등록, 상담이력 등록(방문, 전화, 문자), 환자 검색, 과거 상담 이력 열람, 투약 예약 알림 문자 발송 등의 목적으로만 인가된 사용자에 한하여 사용한다.



사진출처: KT

BAYADA Data Protection_직원(3)

BAYADA Home Health Care

05 노트북 PC 잠금 설정

노트북 PC의 보안 및 해킹 방지를 위해 비밀번호를 설정하고 사용하지 않을 때는 잠금 설정하여 데이터 보안을 유지한다.

06 개인정보가 포함된 종이문서는 시건장치 사용

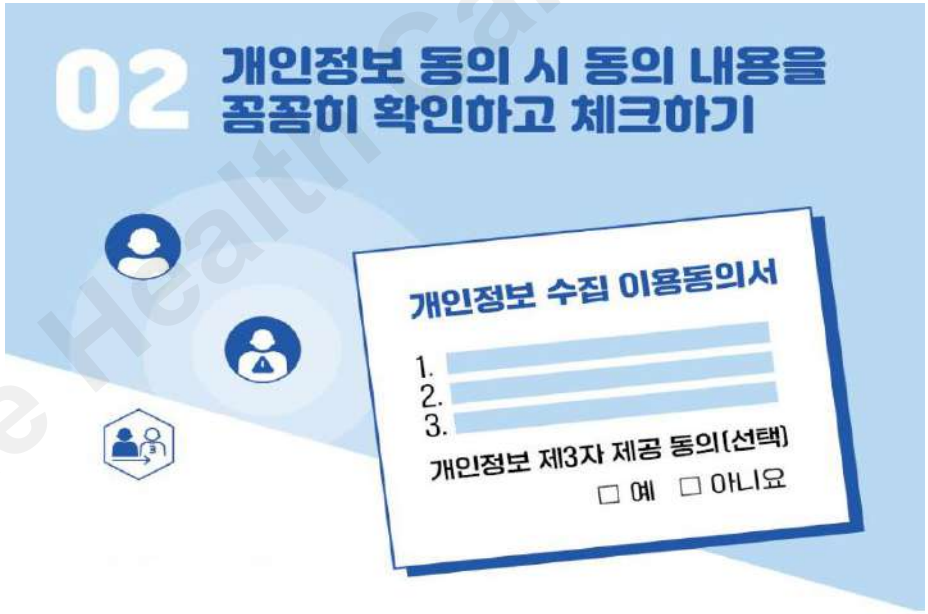
유실방지를 위하여 시건장치에 보관, 대장 작성 및 주기적인 점검을 진행한다.

07 개인정보 삭제 정책 준수

담당 업무의 지침에 따라 Drop Out(D/O) / Withdrawal 환자의 경우, 월단위로 명단을 정리하여 보안이 강화된 보관장소에 저장하고, CRM 내의 해당 환자의 개인정보/민감정보를 삭제한다.

사진출처: 중소기업기술정보지흥원 웹진 > 중소기업 R&D 보안 캠페인 EP.03 관리적 보안 강화하기

Data Protection 실천수칙_Data Privacy(1)



알파벳 대문자, 소문자, 특수문자, 숫자를 3가지 이상 조합하여 8자리 이상으로 설정한다.

과도한 개인정보를 수집하지는 않는지 확인하고, 제3자 제공 등 선택사항은 꼭 필요한 경우에만 동의한다.

출처: 한국인터넷진흥원공식네이버 포스트

Data Protection 실천수칙_Data Privacy(2)

사진이나 동영상을 업로드 할 때, 이름이나 주소, 연락처 등 개인정보가 노출되지 않았는지 확인한다.

다른 기기에서 로그인할 때 한번 더 본인확인을 하도록 설정한다.

출처: 한국인터넷진흥원공식네이버 포스트

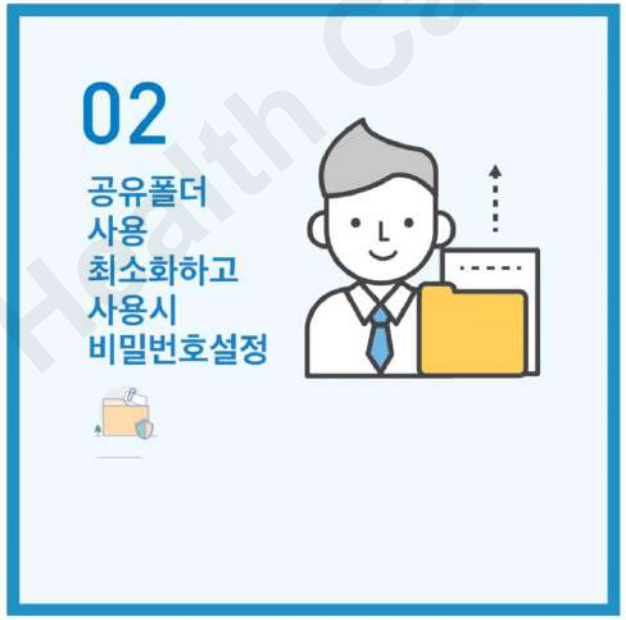
Data Protection 실천수칙_Data Privacy(3)

택배 송장 카드, 영수증에 남아있는 주소, 연락처, 카드정보 등이 고스란히 버려져 범죄에 악용되지 않도록 주의한다.

출처: 한국인터넷진흥원공식네이버 포스트

Data Protection 실천수칙_Data Security(1)

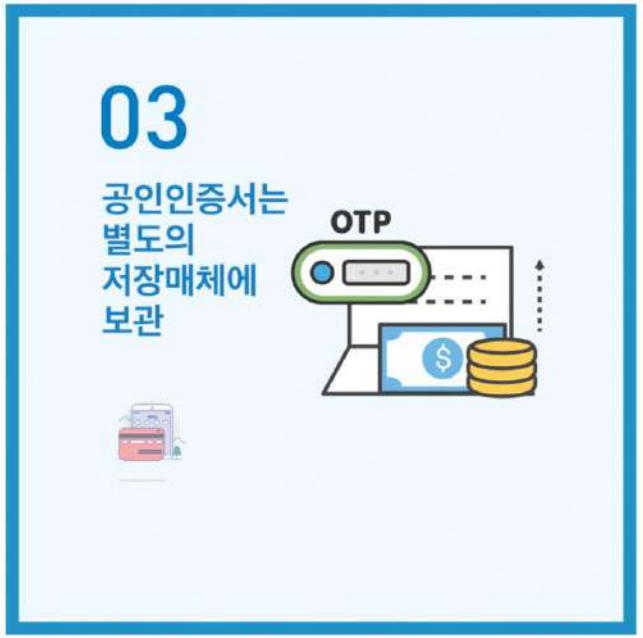
정품 OS는 보안 업데이트를 꾸준히 지원해준다. 정품이 아닌 OS로 임의로 변경하게 되면 보안 위험에 빠지기 쉽다.



중요한 정보의 경우 USB 같은 외장하드에 저장하는 것이 안전하다. 공유 폴더를 사용해야 할 때는 비밀번호를 만들어 사용한다.

출처: 한국인터넷진흥원공식네이버 포스트

Data Protection 실천수칙_Data Security(2)



공인인증서는 '나'를 인증할 수 있는 중요한 문서이다. 보안이 안전한 저장매체(보안토큰, USIM 등)에 보관해야 한다.

모르는 사람에게서 온 이벤트 당첨문자, 택배 미수령 문자 등은 링크를 누르지 말고 바로 삭제해야 한다.

출처: 한국인터넷진흥원공식네이버 포스트

Data Protection 실천수칙_Data Security(3)

BAYADA Home Health Care

백신 프로그램은 PC와 스마트폰 속 악성 코드 및 프로그램을 검사하고 찾아서 제거 하는 프로그램이다. 안전한 사용을 위해 정기적으로 검사를 실시한다.

비밀번호는 주기적으로 바꿔주는 것이 좋다. 이때, 비밀번호에 이름, 생일, 전화번호 등을 사용하지 않도록 주의한다.

출처: 한국인터넷진흥원공식네이버 포스트

Data Protection 실천수칙_Data Security(4)

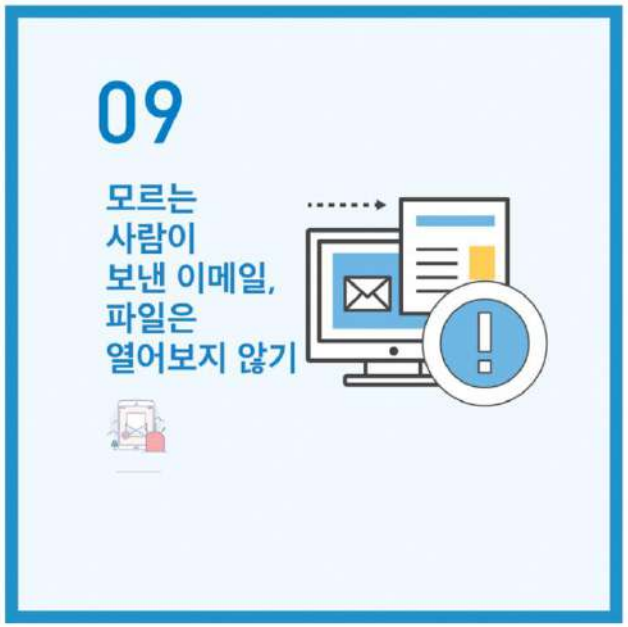
BAYADA Home Health Care

의심스러운 웹사이트에서 로그인/회원가입을 하게 될 경우 입력한 개인정보가 바로 유출될 수 있다. 유명 웹사이트를 똑같이 만들어 로그인하게 만드는 피싱 사이트도 조심해야 한다.

옛날 버전의 윈도우는 최신 바이러스에 취약하다. 자동 보안 업데이트를 설정해두면 늘 최신 버전의 윈도우를 유지할 수 있다.

출처: 한국인터넷진흥원공식네이버 포스트

Data Protection 실천수칙_Data Security(5)



클릭하게 되면 자동으로 결제가 되는 피싱 사기일 수 있다. 의심스럽다면 바로 삭제하도록 한다.

출처: 한국인터넷진흥원공식네이버 포스트