목차

1. 개인정보의 정의

- **개인정보란?**

살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보를 말한다(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함)

(1)**개인에 관한 정보**: 법률상의 개인정보는 '자연인(自然人)에 관한 정보'만 해당하며 법인(法人)이나 단체의 정보는 법률에 따라 보호되는 개인정보의 범위에서 제외

(2)**생존하는 개인에 관한 정보**: 법률상의 개인정보는 '생존하는' 자연인에 관한 정보만 해당하므로 이미 사망하였거나 민법에 의한 실종신고 등 관계 법령에 의해 사망한 것으로 간주되는 자에 관한 정보는 법률상의 개인 정보가 아님

(3)**생존하는 특정 개인을 알아볼 수 있는 정보**: 법률상의 개인정보에 해당되기 위해서는 그 정보로 '특정 개인을 알아볼(식별할)' 수 있어야 하며, 해당 정보만으로는 특정 개인을 식별할 수 없다 하더라도 '다른 정보와 쉽게 결합'하여 식별 가능하다면 개인정보에 해당

2. 개인정보의 종류

•일반정보: 이름, 전화번호, 주소, 생년월일, 출생지, 성별 등

•고유식별정보: 주민등록번호, 운전면허번호, 여권번호, 외국인 등록번호

•민감정보: 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 유전정보, 범죄경력정보

(1)환자 개인정보-이름 나이 등 -> 일반정보

(2)검사 정보 데이터 – 검사내내 수집되는 환자가 비명시/명시적으로 검사자에게 전달하는 정보 -> 민감정보

(3)영상데이터/(화면+ 음성 녹음), 위치정보 -> 민감정보

● 국내의 경우('공공정보 개방·공유에 따른 개인정보 보호 지침')은 공공부문에 적용되는 지침으로 개인식별 가능한 요소를 정하여 삭제하고 주기적인 모니터링으로 재식별 가능성을 완화해야 한다.

● 데이터 수집·분석: 법령 근거 또는 정보주체 동의에 의해 수집·이용하고, 개인 식별 가능한 정보는 삭제 또는 비식별화 후 분석(빅데이터 등) - 비식별화 해야 할 개인정보의 범위는 '그 자체로 개인식별이 가능한 정보'를 열거하여 우선 삭제 또는 비식별화를 권고하고 있음

※ '그 자체로 개인을 식별할 수 있는 정보'

① 쉽게 개인을 식별할 수 있는 정보(이름, 전화번호, 주소, 생년월일, 사진 등),

② 고유식별정보(주민등록번호, 운전면허번호 등),

③ 생체정보(지문, 홍채, DNA 정보 등)

④ 기관, 단체 등의 이용자 계정(등록번호, 계좌번호, 이메일 주소 등)

- 재식별의 경우, 데이터를 제공받은 자가 보유하고 있거나 공개되어 있는 정보와 결합하였을 때 재식별 가능성에 대해 사후 모니터링 수행 권고

3. 합법적 개인정보 수집 및 처리 절차

(1) 보유 개인정보의 수집·이용 목적이 있어야 함

● 빅데이터 분석 전 보유 데이터에 개인정보가 포함되어 있는 경우 정보주체의 동의가 있거나 법률상 구체적 근거가 있을 때에만 수집·이용목적 범위 내에서 분석 가능.

단, 정보주체의 동의가 없거나 법률상 구체적 근 거가 없는 경우 비식별화 조치 필요

(2) 수집시 고지의무

● 국가별 개인정보 수집시 고지의무 사항

한국	EU	미국	일본
수집이용 목적 수집하는 개인정보 항목 보유 및 이용기간 동의거부권 및 동의 거부시 불이익	처리자와 대리인의 신원 처리목적 수령인 또는 그범주 (제공시) 동의의 강제성 여부 및 거부시 불이익 정보접근권 및 정정 요구권	포괄적 고지의무 규정 없음	이용목적

(***한국과 EU 가 까다로운 규정을 가지고 있는 것을 알 수 있음)

(3) 정보 출처 및 수집 주체에 따른 절차

● (**정보주체로부터 직접 수집한 경우**) 수집 당시 사용된 근거 법령, 동의 내용에 명시되어 있는 수집·이용 목적이 있어야 함

- 단, 고유식별정보와 민감정보는 법령상 구체적 근거가 있거나 정보주체의 별도 동의를 얻어야 수집・이용 가능함

● (제 3 자로부터 제공받은 경우) 제 3 자로부터 제공받을 당시 사용된 근거 법령 또는 동의 내용에 명시되어 있는 개인정보를 제공받은 자의 개인정보 이용 목적에 부합되어야 함

- 개인정보의 제공은 제 3 자에게 그 개인정보에 대한 지배 관리권 등이 이전되는 결과를 초래하므로 개인정보 수집·이용 관련 규정보다 더욱 엄격한 요건이 적용됨.

● (인터넷 등 공개된 출처에서 수집한 경우) 공개 목적이 명확한 경우에는 해당 정보의 공개목적에 따라 분석 가능

* 예시: 정보주체가 별도 이용 목적을 제한하여 공개한 경우 공개한 목적 내에서 분석 가능 - 공개 목적이 불명확한 경우: 공개된 정황에 비추어 사회통념에 위배되지 않는 범위

* 단, 비식별화하여 수집·이용하는 것을 우선으로 하여야 함

(4) 제 3 자 제공

●(개인정보를 제 3 자에게 제공할 경우)

유저 정보를 다른 회사 또는 연구기관에게 제공하려고 할 때는 다음과 같은 동의를 받고 **비식별화**를 한다.

개인정보 처음 수집했을 때와 마찬가지로 제 3 자에게 **다음 5 가지 내용**을 고지하고 동의를 받아야만 한다 (동의한다는 문구 추가, 웹사이트에 개인정보 제 3 차 제공 동의 체크 박스 등)

※제 3 자 제공 시 동의 위반 시 과태료 가 아닌 5 년 이하의 징역 또는 5 천만원 이하의 벌금

①개인정보를 제공받는 자

②개인정보를 제공받는 자의 개인정보 이용 목적

③제공하는 개인정보의 항목

④ 개인정보 보유 및 이용기간

⑤동의 거부 권리 및 동의거부시 불이익 내용

(5) 개인정보 비식별화

●비식별화란?

보유 개인정보의 분석을 위한 동의 등이 곤란한 경우 정보에 포함되어 있는 개인정보의 일부 또는 전부를 삭제하거나 다른 정보 로 대체함으로써 다른 정보와 결합하여도 특정 개인을 식별하기 어렵도록 하는 일련의 조치 - 원칙적으로 그 자체로 개인을 식별할 수 있는 정보는 삭제(또는 개인을 식별할 수 있는 정보의 삭제처리 대신 다른 정보로 대체한다.

●비식별화 처리 기법

처리 기법	주요 내용

① 가명처리 (pseudonymization)	개인정보 중 주요 식별요소를 다른 값으로 대체하여 개인식별을 곤란하게 함 (예) 홍길동, 35 세, 서울 거주, 한국대 재학 → 임꺽정, 30 대 서울 거주, 국제대 재학 * 다른 값으로 대체하는 일정한 규칙이 노출되어 역으로 개인을 쉽게 식별할 수 있어서는 안된다.
② 총계처리 (Aggregation)	데이터의 총합 값을 보임으로서 개별 데이터의 값을 보이지 않도록 함 (예) 임꺽정 180cm, 홍길동 170cm, 이콩쥐 160cm, 김팥쥐 150cm → 물리학과 학생 키 합 : 660cm, 평균키 165cm * 단, 특정 속성을 지닌 개인으로 구성된 단체의 속성 정보를 공개하는 것은 그 집단에 속한 개인의 정보를 공개하는 것과 마찬가지 결과가 나타나므로 그러한 정보는 비식별화 처리로 볼 수 없음 (예> 에이즈 환자 집단임을 공개하면서 특정인물 '갑'이 그 집단에 속함을 알 수 있도록 표시하는 것은 '갑'이 에이즈 환자임을 공개하는 것과 마찬가지임)
③ 데이터 값 삭제 (Data Reduction)	데이터 공유·개방 목적에 따라 데이터 세트에 구성된 값 중에 필요 없는 값 또는 개인식별에 중요한 값을 삭제 (예) 홍길동, 35 세, 서울 거주, 한국대 졸업 → 35 세, 서울 거주 (예) 주민등록번호 901206-1234567 → 90 년대 생, 남자 (예) 개인과 관련된 날짜 정보(자격 취득일자, 합격일 등)는 연단위로 처리 (예) 연예인·정치인 등의 가족 정보(관계정보), 판례 및 보도 등에 따라 공개되어 있는 사건과 관련되어 있음을 알 수 있는 정보
④ 범주화 (Data Suppression)	데이터의 값을 범주의 값으로 변환하여 명확한 값을 감춤 (예) 홍길동, 35 세 → 홍씨, 30-40 세
⑤ 데이터 마스킹 (data masking)	공개된 정보 등과 결합하여 개인을 식별하는 데 기여할 확률이 높은 주요 개인식별자가 보이지 않도록 처리하여 개인을 식별하지 못하도록 함 (예) 홍길동, 35 세, 서울 거주, 한국대 재학 → 홍**, 35 세, 서울 거주, **대학 재학 * 남아 있는 정보 그 자체로 개인을 식별할 수 없어야 하며 인터넷 등에 공개 되어있는 정보 등과 결합하였을 경우에도 개인을 식별할 수 없어야 한다.

●개인식별요소 제거를 위한 참고 알고리즘 (가명처리)

▶ 시계열 데이터 마이닝 (k-익명화)

동일한 속성 값을 가지는 데이터를 k 개 이상으로 유지하여 데이터를 공개하는 방법으로서 지정된 속성이 가질 수 있는 값을 k 개 이상으로 유지하여 프라이버시 누출을 방지

▶ 부분그래프 익명화

소셜 네트워크 데이터의 구조적 특성 중 하나인 부분 그래프에 의한 프라이버시 노출을 방지하기 위한 익명화 기법으로 익명화를 위해서 그래프 수정을 통해 특정 부분 그래프가 전체 그래프에서 k 개 이상 존재하게 만드는 기법

▶ 차수 익명화

k-차수 익명화를 만족하는 그래프는 각 정점에 대해 해당 정점과 같은 차수를 가진 정점이 최소 k-1 개 이상 존재하는 그래프로 원본 그래프를 k-차수 익명화 그래프로 만들기 위해 간선을 추가/삭제함

▶ 부분 그래프 + 차수 익명화

부분 그래프와 차수를 동시에 배경 지식으로 가지고 있을 때, 프라이버시 노출을 막기 위한 익명화 기법

▶ 매크로 기법- 셀 값 감추기 방법 (suppression)

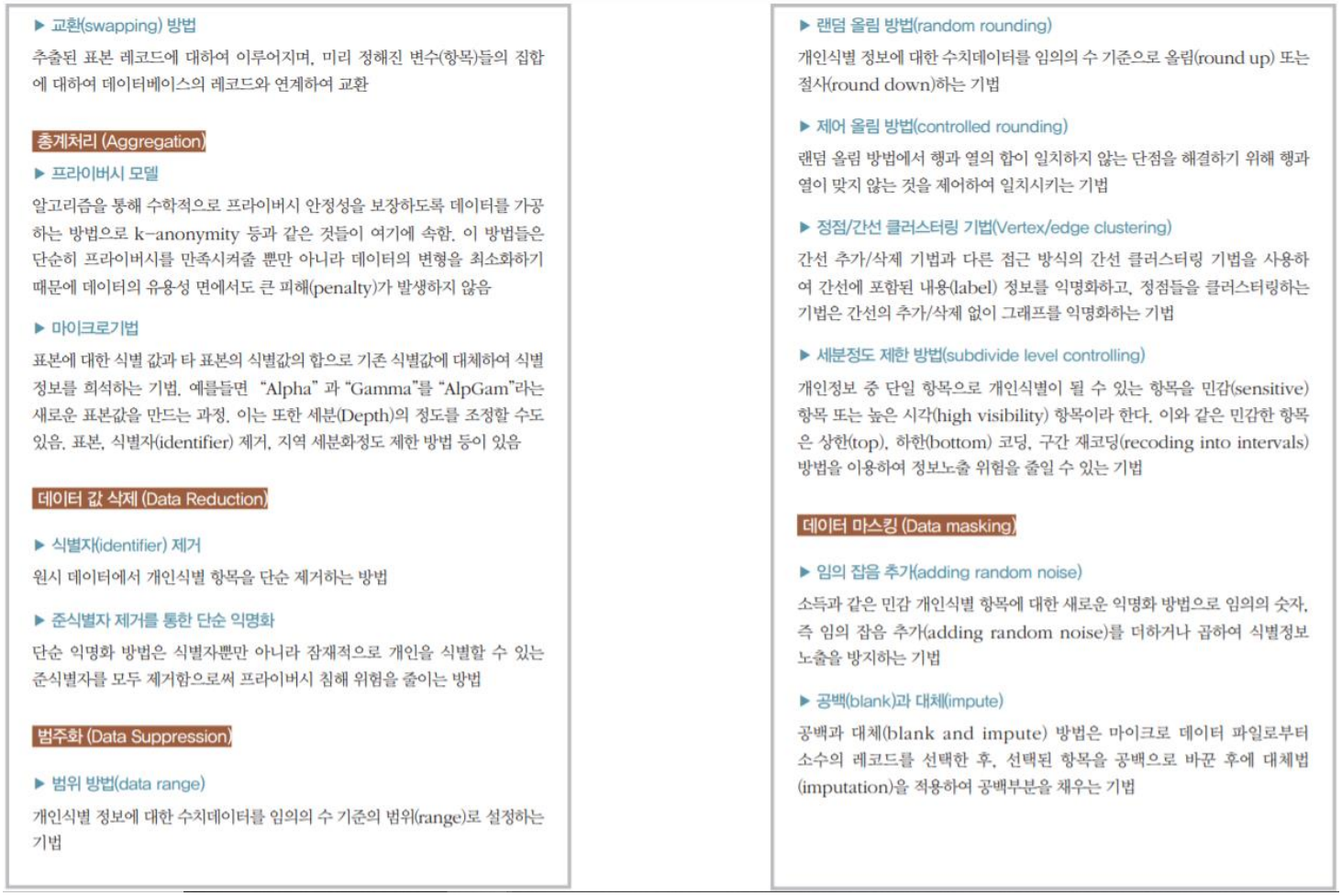
민감 식별항목의 셀 값 노출방지를 위한 대표적인 방법으로 민감한 셀의 행과 열의 주변 값도 동시에 감추는 기법(suppression)이다. 여기서 부수적으로 감추어지는 셀을 보조 셀 감추기(complementary suppression)라 하며, 이 셀은 인위적으로 선정

▶ 휴리스틱 익명화 (heuristic anonymization)

준식별자에 해당하는 값들을 몇 가지 정해진 규칙 혹은 사람의 판단에 따라 가공하여 자세한 개인 정보를 숨기는 방법

	개념	활용가능 범위
개인정보	특정 **개인에 관한 정보**, 개인을 **알아볼 수 있게 하는 정보**	**사전적**이고 **구체적인** **동의**를 받은 범위 內 활용 가능
가명정보	**추가정보**의 사용없이는 **특정 개인을 알아볼 수 없게 조치**한 정보	다음 목적에 **동의 없이** 활용 가능 (EU GDPR 반영) ① 통계작성 (상업적 목적 포함) ② 연구 (산업적 연구 포함) ③ 공익적 기록보존 목적 등
익명정보	**더 이상 개인을 알아볼 수 없게** (복원 불가능할 정도로) **조치**한 정보	개인정보가 아니기 때문에 **제한없이** **자유롭게 활용**

<비식별화기법 상세내용>



(5) 개인정보 보관 및 파기 방법

● (비식별화 했을 경우 사후검토의 개념) 시간의 경과에 따라 데이터 분석기술의 진화 및 관련 공개정보가 누적되어 재식별 위험이 증가할 수 있으므로 비식별화 기법 및 재식별 가능성에 관한 주기적 모니터링 실시

- 재식별이 되는 경우 추가 비식별화 등의 보완 조치 및 향후의 비식별화 처리 기법 개선 시 반영

● 생성되거나 재식별화된 개인정보의 관리 철저

- 빅데이터 분석 등의 과정에서 불필요한 개인정보가 새로 생성되거나 비식별화 처리된 정보가 재식별화된 경우에는 지체없이(통상 5 일이내) 그 개인정보를 삭제하거나 비식별화 처리

개인정보의 파기와 보관

⦿ 법 제21조 1항

· 개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니한다.

⦿ 방송통신위원회 〈개인정보의 기술적, 관리적 보호조치 기준〉

· 최소 6개월 이상 보존, 관리

⦿ 금융감독원 〈전자금융감독규정 해설서〉

· 금융기관 또는 전자금융업자의 통신망에 접속 시 접속일시, 출발지 및 목적지 IP, 접속포트(Port)를 포함하여 접속내역을 1년 이상 기록, 보관

⦿ 전자금융거래와 관련된 접속기록

· 전자금융거래법 시행령 제12조에 의거하여 5년간 기록/보존

개인정보의 파기와 보관

⦿ 정보시스템 가동기록 · 전산기기의 가동, 업무처리와 관련하여 주전산기 또는 서버에 접속한 일시, 접속자 및 접근을 확인할 수 있는 접근 기록과 전산자료를 사용한 일시, 사용자 및 자료의 내용 등을 확인할 수 있는 접근 기록 등을 자동기록 되도록 하고 일정기간 이상(최소 1년) 보관

· 예 : 시스템 로그, 콘솔로그 등

⦿ 법 제21조 2항 · 개인정보처리자가 개인정보를 파기할 때에는 복구 또는 재생되지 아니하도록 조치하여야 한다.

4. 심리 검사 개인정보 관련 소송/위반 사례

(1) 심리센터 상담사례

A 씨는 2014 년 11 월 B 씨 등이 운영하는 심리상담센터를 방문해 심리상담을 받았다. B 씨는 휴대폰으로 상담내용을 녹음해 음성파일을 녹취록 형태로 보관했다. 녹취한 내용에는 A 씨의 나이와 가족관계, 학력뿐 아니라 성장기, 유학과정의 경험담, 스스로에 대한 가치관, 현재 직종과 근무 회사의 성격, 직장 상사와의 관계, 연애 성향과 이성관, 역사와 종교관, 각종 고민거리 등 내밀한 신상정보가 포함돼 있었다.

비밀엄수 의무·상담자 신뢰보호 관련 소송

이듬해 4 월 센터는 유료 세미나의 사례분석 자료로 활용하기 위해 다수의 세미나 참석자에게 A 씨의 상담내용이 담긴 녹취록을 메일로 발송했는데, 이 녹취록에는 성(姓)이 생략된 A 씨의 이름이 남아 있었고 최소 2 명에게는 익명화되지 않은 녹취록이 전송됐다. 이 센터에서 전문가 과정을 이수한 D 씨는 A 씨의 상담내용이 포함된 자료를 이용해 책자로 만들어 시중에 판매하기도 했다. 2017 년 7 월 자신의 상담내용이 녹취록으로 만들어져 세미나 자료로 배포되거나 책자로 유통되고 있다는 사실을 알게 된 A 씨는 소송을 냈다.

재판부는 "B 씨는 센터를 실질적으로 운영하며 업무를 목적으로 A 씨의 개인정보에 해당하는 상담내용을 스스로 또는 타인을 통해 수집·저장·편집·제공 등 처리한 사람이고, C 씨는 센터 대표이므로 개인정보보호법 제 2 조 5 호가 정한 개인정보처리자에 해당하고, A 씨가 B 씨에게 털어놓은 상담내용은 그의 사생활을 현저히 침해할 우려가 있는 **민감정보**로서 법이 보호하는 개인정보에 해당한다"고 밝혔다.

이어 "B 씨는 A 씨의 동의 없이 이러한 정보를 수집해 여러 사람에게 유출했고, 센터에서 전문가 과정을 이수한 D 씨가 A 씨의 상담 내용이 포함된 자료를 이용해 만든 책 머리말에 발간사를 쓰기도 한 점을 보면, D 씨가 독단으로 A 씨의 정보를 유출했다고 보이지 않는다" 며 "B 씨와 C 씨는 법에 위반해 A 씨의 개인정보를 수집·이용하고 그 유출을 초래한 개인정보처리자로서 개인정보보호법 제 39 조 1 항에 따라 정보주체인 A 씨가 입은 정신적 손해를 배상할 책임이 있다"고 설명했다.

그러면서 "A 씨가 민감정보 유출로 상당한 정신적 충격을 받았을 것으로 보인다" 며 "상담자의 비밀 엄수의무와 내담자의 신뢰보호에 대한 몰각의 정도가 심각할 뿐 아니라 제 3 자에게 전파된 개인정보에 대한 식별가능성의 정도, 책자 배포로 이어진 2 차 유출 경위 등 제반사정에 비춰 위자료를 1000 만원으로 정한다"고 판시했다.

==>(판결) 서울중앙지법, 상담센터 운영자에1000만원 지급 판결

(2) 약학정보원 환자정보 유출사례

2013년 12월 11일 서울중앙지방검찰청은 개인정보관리법 위반행위와 관련해 약학정보원을 압수수색했다.약학정보원은 2007년부터 2012년까지 약 5년 간 약국 보험청구 프로그램인 'PM2000'을 이용해 환자들의 질환, 의약품 청구 내역 등의 정보를 무단으로 수집, 다국적 의약정보제공기업인 IMS헬스코리아에 제공했다는 혐의를 받고 있다.

약학정보원의 처방전 전산처리 시스템은 전국 49%의 약국에 설치돼 있고 지금까지의 수사결과 약학정보원은 매년 약 3억원을 받고 환자처방정보 300만 건을 유출한 것으로 파악되고 있다.이에 19일 보건복지부와 행정안전부는 뒤늦게 개인의료정보취급에 관한 가이드라인을 발표했다. 대한의사협회는 23일 약학정보원과 그 정보를 사들인 IMS헬스코리아를 상대로 집단 손해배상청구소송을 제기할 것이라는 입장을 밝혔다.

이와 같은 개인정보의 침해는 과거에도 문제가 된 바 있다. 2003년 건강보험공단이 가입자의 개인정보 4000여 건을 업무목적 외로 열람해 그 일부를 보험회사에 유출한 사례가 있다.

(3) 다양한 개인정보 유출/분쟁조정사건 사례

① 심리상담센터가 피상담자의 허락 없이 심리상담 내용이 담긴 녹취록(민감정보)을 세미나 자료 등으로 사용했다면 배상책임 존재(서울중앙지법 2019나31794 판결: 위자료 1000만원),

② 경품행사로 대량 수집한 고객 개인정보(고유식별정보)를 보험사에 팔아넘긴 혐의로 기소된 홈플러스에 벌금형이 확정(대법원 2018도13694 판결: 벌금 7500만원),

③ 시장점유율을 유지하기 위해 고객정보를 무단으로 이용해 선불폰(요금을 미리 내고 쓰는 휴대전화) 요금을 임의로 충전한 SK텔레콤에 벌금형이 확정(대법원 2016 판결 : SK텔레콤 벌금 500만원, 전·현직 팀장급 직원 2명에게는 징역 2년에 집행유예 3년),

④ 수백 명의 개인정보를 불법으로 구매해 인터넷 게시글의 추천 수를 조작한 혐의로 재판에 넘겨진 30대 남성에게 징역형(인천지법 2017 판결 : 징역 1년, 집행유예 2년, 80시간 사회봉사 명령),

⑤ 법률사무소에서 사무장으로 일하는 동생의 부탁을 받고 다른 사람의 수배내역(민감정보) 등을 몰래 알아봐 준 혐의로 기소된 전직 경찰관에게 징역형이 선고(인천지법 2017 판결 : 징역 4월, 집행유예 1년),

⑥ 개인정보 불법 수집 여부를 둘러싸고 의사와 환자들이 약학정보원 등을 상대로 소송을 냈지만 1심에서 패소(서울중앙지법 2014 판결 : 약학정보원이 식별성이 완전히 제거되지 않은 정보를 정보주체의 동의 없이 한국IMS헬스에 제공한 것은 개인정보보호법 위반이나, 해당 정보가 약학정보원과 한국IMS헬스에 제공된 이외에 다른 곳으로 유출되거나 제3자가 열람했을 가능성이 있다고 보기는 어려움),

⑦ 직원이 개인적으로 사용하기 위해 사내 전산망에서 다른 직원의 전화번호와 주소 등 개인정보를 조회하고 사용했다면 회사도 손해배상 책임(서울중앙지법 2016가단5038590 판결 : 각 50만원 위자료, 개인정보의 처리 업무 위탁자인 회사는 정보주체의 개인정보가 유출되지 않도록 수탁자를 교육하고 처리 현황을 점검하는 등 감독해야),

⑧구글은 제3자에게 제공한 가입자의 개인정보와 서비스이용내역 현황을 가입자에게 공개할 의무가 존재(서울고법 2015 판결 : 미국 본사인 구글 인코퍼레이티드, 구글 한국지사인 구글코리아는 이용자의 개인정보, 서비스이용내역을 제3자에게 제공한 현황을 공개하라, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제30조 2항),

⑨개인정보 유출로 피해를 본 롯데카드 이용자들에게 카드사가 10만원씩을 배상해야(서울남부지법 2014 판결 : 각 10만원씩 위자료),

⑩ 온라인에서 할인쿠폰 이벤트 등으로 수집한 고객 정보(주로 일반정보)를 보험사에 넘긴 개인정보수집업체에 대한 방송통신위원회의 제재는 정당하다(대법원 2014 판결),

⑪ 휴대전화 번호 뒷자리 숫자 4개도 개인정보에 해당하기 때문에 무단으로 유출하면 처벌(대전지법 논산지원 2013고단17 판결 : 경찰관 서모씨와 서씨에게서 김씨의 전화번호를 받은 도박 참가자 윤모씨에게 각각 징역 6월, 4월에 집행유예 1년을 선고),

⑫ 13년 전 중학교 때 받은 인성심리 검사내용이 계속 보관 관리 → 손해배상금 50만원 지급

5. 개인정보보호 법제체계 정리

[개인정보 보호법]을 비롯한 우리의 개인정보보호법제는 기본적으로 개인정보에 해당하는 경우에는 수집 단계에서부터 엄격한 처리 기준을 설정하여, 개인정보보호 관련법에서 규정하는 요건을 충족하는 경우에만 합법적인 처리가 가능하다. 수집 단계에서 합법적 처리 요건을 갖추었다고 하더라도 이를 수집 목적 외로 처리하거나 제 3 자에게 제공하는 경우에는 각 단계별로 별도의 기준을 충족한 때에 적법한 처리로 인정된다. 즉, 개인정보에 관한 일반법인 [개인정보 보호법]에 따르면, 수집단계에서는 (1) 정보 주체의 동의를 받는 경우, (2) 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우, (3) 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우, (4) 정보 주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우 (5) 정보주체 또는 그 법정 대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제 3 자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우 (6) 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우(이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한함) 에 합법적인 처리로 인정된다. 개인정보를 제공하는 경우에도 동의를 받거나 위수집시 적법 처리 기준 중 (2,3,5)에 따라 개인정보를 수집한 목적 범위에서 개인정보를 제공하는 경우에 적법한 제공으로 인정된다.
개인정보를 목적 외로 이용하거나 제공하는 것은 원칙적으로 금지 되지만 정보주체 또는 제 3 자의 이익을 부당하게 침해하는 우려가 없는 때에 한하여 (1) 정보주체로부터 별도의 동의를 받은 경우, (2) 다른 법률에 특별한 규정이 있는 경우, (3) 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제 2 자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우 (4) 통계작성, 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우 (5) 개인정보를 목적 외의 용도로 이용하거나 이를 제 3 자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우, (6) 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우, (7) 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우, (8) 법원의 재판업무 수행을 위하여 필요한 경우,

(9) 형 및 감호, 보호처분의 집행을 위하여 필요한 경우에만 허용된다. 이외에도 여러 처리 기준이 존재하지만, 기본적으로는 법에 규정된 사항 외에는 정보주체의 동의를 요한다. 합법적 처리는 법에 규정된 경우 혹은 동의를 받은 목적 범위 내에서만 원칙적으로 처리 가능하다.

출처: 인공지능과 법 (한국인공지능법학회)

6. 개인정보 및 빅데이터를 활용한 성공적인 헬스케어 비즈니스 사례

스마트헬스케어 베스트 3

서비스명	회사명(대표)	비즈니스 모델	투자유치(투자사)
라파엘 스마트 글러브	네오펙트 (반호영)	뇌졸중 등 환자 재활훈련 콘텐츠 · 의료기기	140억원 이상 2018년 코스닥 상장
희귀질환 스크리닝	쓰리빌리언 (금창원)	AI 유전자 분석 7800여 종 희귀질환 진단	144억원 이상 (산업은행, 신한캐피탈 등)
MOAAH	휴먼스케이프 (장민후)	개인 건강데이터 신약개발 등 활용 블록체인 커뮤니티	85억원 이상 (KB증권, 한국투자파트너스 등)

▶스마트헬스케어 베스트3 (출처: https://www.mk.co.kr/news/business/view/2020/02/108789/)

지난 2018년 기술특례로 코스닥에 상장한 네오펙트는 뇌졸중 등 신경계·근골격계 질환 환자의 재활을 돕는 스마트 기기 '라파엘 스마트 글러브'로 유명한 회사다. 2017년과 2018년 세계최대 가전전시회 CES에서 라파엘 스마트 글러브, 라파엘 스마트 페그보드로 연이어 혁신상을 수상했고, 올해 CES에서도 하지 재활 훈련기기 '스마트 밸런스'로 혁신상을 받으며 3관왕에 올랐다. 간단한 게임을 즐기며 재활훈련을 할 수 있는 혁신적인 솔루션으로 CNN 등 글로벌 미디어의 주목을 받고 있다.

진단조차 하기 힘든 희귀질환을 유전자 검사 한 번으로 찾아준다는 스타트업도 있다. 쓰리빌리언은 AI 기술로 약 7800여 종의 희귀질환을 진단해주는 솔루션을 개발했다. 기존에 5년 이상 걸리던 진단 기간을 20~40시간으로 줄였고, 미국 대학병원을 기준으로 1000만원이 넘던 진단비용도 10분의 1 수준으로 낮췄다. 최종 진단은 물론 의사가 내리지만, 유전자를 읽고 해석하는 과정과 증상을 보고 질병을 판단하는 모든 과정에 AI가 활용된다.

국내 암호화폐 거래소에도 상장되어 있는 코인(HUM)을 발행한 휴먼스케이프는 개인 건강데이터를 신약개발과 임상시험 등에 활용하는 블록체인 커뮤니티 앱 '모아(MOAAH)'를 운영하고 있다. 내 건강 데이터를 블록체인으로 수집해 제약사, 연구기관 등에 제공하고

HUM 토큰으로 보상하는 방식이다. 환자는 데이터를 제공한 보상을 받고, 희귀난치질환 치료법 개발에 기여할 수 있다. 이 회사는 GC녹십자지놈, 싸이퍼롬, 서울대 의대 정보의학실 등과 협력해 희귀질환자 데이터 플랫폼을 구축했고, 서울성모병원 스마트병원과 암환자 데이터를 연구하고 있다.

△네오펙트의 스마트 글러브

【23andMe, 美 FDA로부터 개인 유전정보 분석 테스트 허가】

https://www.bioin.or.kr/board.do?num=250894&cmd=view&bid=issue

○ 美 FDA는 희귀유전 질환인 블룸 증후군(Bloom syndrome)의 보인자 여부 테스트를 허가 (2015.1.9)

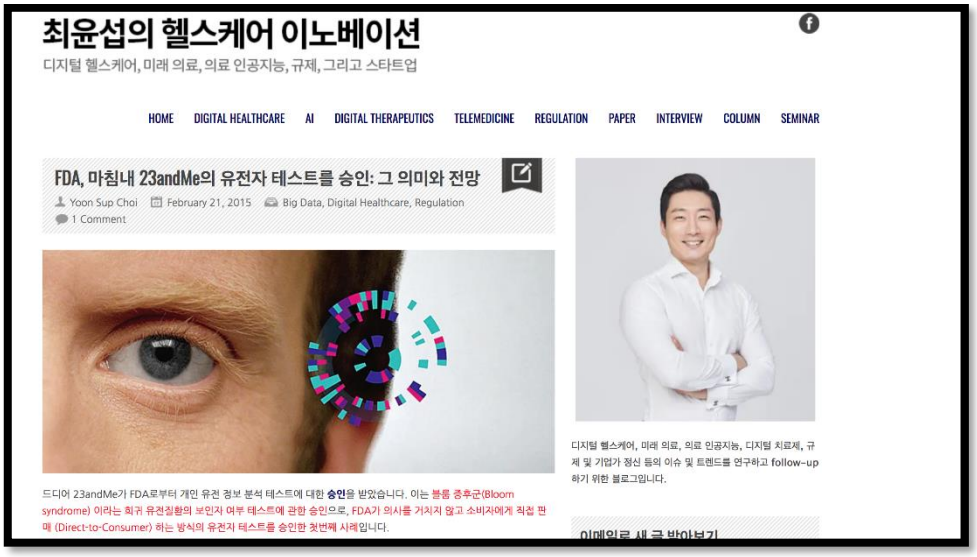
○ 이는 FDA가 의사를 거치지 않고 소비자에게 직접 판매하는 방식의 유전자 테스트를 승인한 첫 번째 사례

- 체외진단학 및 방사선 보건국 책임자인 알베르토 구티에레즈(Alberto Gutierrez)는 "FDA는 소비자가 자신의 유전정보를 접근하는데 있어서 의사를 거쳐야 할 필요가 없다고 믿는다"고 언급

○ 23앤미는 블룸 증후군 보인자 상태 검출이 정확하다는 것을 보여주기 위해 두 개의 독립적인 연구를 수행하였고 동등한 결과를 증명

출처: US FDA, 'FDA permits marketing of first direct-to-consumer genetic carrier test for Bloom syndrome', 2015.1.19

http://www.yoonsupchoi.com/2015/02/21/fda_approved_dtc_test_of_23andme/v



7. 최근 데이터 활성화 법과 제도의 동향 (데이터3법 통과)

>> 데이터 3법 주요 내용 및 향후 과제

데이터 3법의 통과

데이터 3법 주요 내용

개인정보 보호법	• 개인정보 중 가명 정보는 통계작성, 연구 등 목적으로 사용 가능 • 기업간의 정보를 보안시설을 갖춘 전문기관을 통해 결합할 수 있고, 전문기관 승인 거쳐 반출 허용
정보 통신망법	• 정보통신망법상 개인정보 보호 사항을 개인정보법으로 이관해 규제하고 감독 추세를 방송통신위원회에서 개인정보보호 위원회로 변경
신용 정보법	• 가명 정보의 안전한 이용 위해 보안 장치 의무화, 부정한 복적으로 이용 시 징벌적 과징금 부과 • 정보 활용 동의서 등급제, 프로파일링, 대응권 등 새로운 개인정보 자기결정권 도입

향후 과제

- **세부 법안들의 규정화**
  가명화된 개인정보를 통계작성, 연구목적, 공익적 기록보전 용도 등으로만 활용할 수 있음. 상용화 분야의 활용에는 아직 제약 이 남아 있는 실정
- **의료법을 넘어 설 수 있을까?**
  의료법과 국민건강보험법에서 별도로 보호하고 있어 이번 개인정보법 개정안과 법체계가 충돌할 우려
- **개인정보 유출에 대한 우려**
  익명 처리를 해도 개인 정보를 드러내는 '재식별화'의 가능성이 제기

Source: 국회 각 상임위원회, 언론보도 종합, 삼정KPMG 경제연구원 재구성

(시사점) 데이터 3법 통과: 의료 데이터, 개방을 넘어 활용으로

- 결국은 정부의 적극적인 드라이브가 핵심, 의료데이터의 활용에 있어서는 **정부의 역할**이 매우 중요하다.
- 정밀의료를 실현하기 위해서는 **1명의 유전자, 진료기록, 라이프로그(life log)**를 연결하는 것이 중요한데, 각 정보는 각기 다른 기관을 통해서 수집되기 때문에 정부 주도하에 통합하지 않는 이상 민간기관에서 통합하기는 어려움이 있다.

- 미국의 경우 헬스케어 관련 규제를 완화함과 동시에 정부차원에서 헬스케어

서비스를 제공하기 위해 대규모 프로젝트를 지속적으로 진행하고 있다. 헬스케어 진입장벽을 완화하기 위해 사전인증제도를 도입하고, 소프트웨어 자체를 의료기기로 분류하는 규정 등은 테크기업이 헬스케어 산업에 진입하는데 장벽을 크게 낮춘 것으로 보인다.

- **일본 정부는 차세대의료기반법을 제정하여 건강정보를 '필요배려 개인정보'**로

분류하고 데이터를 활용도를 적극적으로 높인 반면, **한국에서는 여전히 의료 데이터를 '민감정보'로 분류하여 보호 중심**의 관리 체제를 유지하고 있는 실정이다.

- **2020년 1월 데이터3법의 통과는 빅데이터를 활용하기 위한 작은 첫발을** 내딘 것임

그러나 여전히 세부 법안들의 규정화해야 하며, 의료법과의 충돌을 피하기 위한 정확한 가이드라인이 필요한 상황이다. 또한 데이터3법 통과로 인한 데이터 활용의 발판을 바탕으로 헬스케어 데이터가 정밀의료에 효과적으로 적용되기 위해서는 정부 주도의 대규모 프로젝트를 지속적으로 발굴해 기업들이 헬스케어 산업에 진입 할 수 있는 장벽을 낮춰야 한다

- **기업들도 정부 정책과 발맞춘 기술적 대비가 필요함.**

가까운 미래에 의료 데이터 개방이 예고된바, 기업들 또한 의료 빅데이터의 완벽한 활용을 위한 준비가 필요하다. 아무리 많은 데이터들을 보유하고 있다고 해도, 그것을 정확하게 활용하지 못한다면 무용지물이 되기 때문이다.

출처: https://assets.kpmg/content/dam/kpmg/kr/pdf/2020/kr-issue-monitor_healthcare-big-data-20200317.pdf

8. 앞으로의 개인정보보안 연구과제

1. 병원에서 웹 애플리케이션에서 입력한 정보를 전송할 때 저장되는 데이터의 서버를 구축해야 한다.

2. 데이터가 저장되는 서버에서 데이터베이스 접근을 어떻게 할 것인지 (i.e. 인트라넷으로 연동되는 DB 암호화 모델설계 및 문서관리를 어떻게 할 것인지 정해야 한다

3. 심리검사 DB 구축(리버스 엔지니어링을 통해)을 위한 심리검사 오픈 API 찾기

- https://openpsychometrics.org/_rawdata/

PSEMO 개인정보정리와 관련된 시스템에 필수적인 단계들 정리

- **세모 데이터 분류**

(1)환자 개인정보-이름 나이 등 -> 일반정보
(2)검사 정보 데이터 – 검사내내 수집되는 환자가 비명시/명시적으로 검사자에게 전달하는 정보 -> 민감정보
(3)영상데이터/(화면+ 음성 녹음), 위치정보 -> 민감정보

- **수집-보관-이용-파기 4 단계 메뉴얼**

1. **수집 주체에 따른 절차**
*정보주체[전문가] 로부터 직접 수집한 경우: 수집 당시 사용된 근거 법령, 동의 내용에 명시되어 있는 수집·이용 목적이 표기된 동의서 작성
수집시 표기할 항목: 수집하려는 개인정보의 항목

수집이용 목적
수집하는 개인정보 항목
보유 및 이용기간
동의거부권 및 동의 거부시 불이익

예) 수집이용 목적: 병원과의 일정 매칭서비스를 위해, 검사 전반의 업무에 필요한 개인정보를 수집하고 이용하고자 함
수집하는 개인정보 항목: 검사자 이름, 나이, 라이센스, 주소
보유 및 이용기간: 동의일로부터 수집・이용 목적 달성시까지 보유 후 파기
동의거부권 및 동의 거부시 불이익: 임상심리전문가는 개인정보 수집·이용에 관한 동의를 거부할 수 있습니다. 다만, 필수적으로 수집하는 정보에 관하여 동의를 거부할 경우 해당 조건에 맞는 검사가 불가능할 수 있으며, 선택적으로 수집하는 정보에 관하여 동의를 거부할 경우 해당 항목이 매칭 절차에 고려될 수 있습니다.

*정보주체[병원] 로부터 직접 수집한 경우 수집 당시 사용된 근거 법령, 동의 내용에 명시되어 있는 수집·이용 목적이 표기된 동의서 작성
수집시 표기할 항목

수집이용 목적
수집하는 개인정보 항목
보유 및 이용기간

동의거부권 및 동의 거부시 불이익

예) 수집이용 목적: 전문가와의 일정 매칭서비스를 위해
수집하는 개인정보 항목: 엔드유저(검사내담자)의 증상과 특징, 지역정보
보유 및 이용기간: 동의일로부터 수집・이용 목적 달성까지 보유 후 파기
동의거부권 및 동의 거부 시 불이익: 병원은 개인정보 수집·이용에 관한 동의를 거부할 수 있습니다. 다만, 필수적으로 수집하는 정보에 관하여 동의를 거부할 경우 해당 조건에 맞는 검사가 불가능할 수 있으며, 선택적으로 수집하는 정보에 관하여 동의를 거부할 경우 해당 항목이 매칭 절차에 고려될 수 있다.

- 단, 고유식별정보와 민감정보는 법령상 구체적 근거가 있거나 정보주체의 별도 동의를 얻어야 수집・이용 가능함

*__동의없이 개인정보 수집・이용이 가능한 경우__

1. 정보통신서비스 제공에 관한 계약 이행을 위해 필요한 개인정보로서 경제적 및 기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우 -> PSEMO가 보안 전문기관승인을 거칠 때 사용될 개인정보는 동의가 필요하지 않다.
2. 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우 매칭서비스로 정산하게 될 경우 사용할 개인정보(성명, 카드번호 등)은 동의가 필요 하지 않다.

2. 보관 -(비식별화 저장, 세션관리, 주기적인 점검 및 검토)

웹애플리케이션 이용시 유저 개인정보 보관

- 접속기록 월 1 회 이상 점검

시스템에 전자적으로 자동 기록되도록 설계 및 구현해야 한다.
계정(ID) - 시스템에 접속한 자를 식별할 수 있도록 부여된 정보
접속일시 (년월일시분초) - 접속한 시점 또는 업무를 수행한 시점
접속지(IP 주소)- 접속한 취급자의 컴퓨터/모바일 기기 등의 주소
정보주체정보 - 개인정보취급자가 누구의 개인정보를 처리하였는지 알 수 있는 이름, ID 등
수행업무 (저장, 수정, 삭제 다운로드 등) 취급자가 시스템에서 처리한 정보주체에 관한 수행업무 내용을 알 수 있는 정보

예시

번호	계정정보	접속일자	접속시간	접속지정보	수행업무	정보주체
1001	k123	2019-02-01	10:05:14	192.168.***	다운로드	ab1234

- 접속기록은 생성되는 시기에 따라 아래 기간동안 보관해야 한다.

모든 개인정보처리시스템 - 1 년이상
5 만명 이상 개인정보 처리 또는 고유식별정보 및 민감정보 처리시스템 2 년이상
-개인정보처리시스템에 보관된 접속기록을 최소 월 1 회 이상 점검하여 비정상 행위를 탐지하고 적절한 대응 조치를 해야 한다.
아래와 같은 사항등을 사전에 계획하고 시행한다.
1.점검주체
2.점검 시기
3.점검 항목 및 내용 (개인정보 처리 및 대량의 개인정보 다운로드 등 비정상 행위 탐지, 접속기록의 위 변조 여부 등)
4. 점검 후속조치(개선조치, 결과보고등)

- 접속기록을 안전하게 보관

접속기록이 위조.변조 및 도난, 분실되지 않도록 아래와 같은 방법 등으로 안전하게 보관해야한다.

1. 접속기록을 상시 백업하여 별도의 보조저장매체, 저장장치 등에 보관
2. CD_ROM, DVD_R WROM 과 같은 덮어쓰기 바지 매체 사용
3. 접속기록을 수정가능한 매체 (하드디스크)에 백업하는 경우에는 위조.변조 여부를 확인할수있는 정보를 별도의 장비에 보관하기

- 안전한 보안설계를 위해 아키텍처 설계시 다음을 충족시켜야 한다.

세션 간 데이터가 공유되지 않도록 설계해야 한다.
세션과 세션 ID 가 안전하게 관리되도록 해야 한다

-세션 ID 는 안전한 서버에서 생성해서 사용되도록 한다. 세션 ID 는 최소 128 비트의 길이로 생성되어야 하며, 안전한 난 수 알고리즘을 적용하여 예측이 불가능한 값이 사용되도록 한다. URL Rewrite 기능을 사용하는 경우 세션 ID 가 URL 에 노출될 수 있으므로, URL Rewrite 기능을 사용하지 않도록 설계한다. 로그인 성공 시 로그인 전에 할당받은 세션 ID 는 파기하고 새로운 값으로 재할당하여 세션 ID 고정 공격에 대응하도록 한다. 장기간 접속되어 있는 경우 세션 ID 의 노출 위험이 커지므로, 일정시간 주기적으로 세션 ID 를 재할당하도록 한다.

- 비식별화 했을 경우 시간의 경과에 따라 데이터 분석기술의 진화 및 관련 공개정보가 누적되어 재식별 위험이 증가할 수 있으므로 비식별화 기법 및 재식별 가능성에 관한 주기적 모니터링 실시

- 재식별이 되는 경우 추가 비식별화 등의 보완 조치 및 향후의 비식별화 처리 기법 개선 시 반영시 생성되거나 재식별화된 개인정보의 관리 철저

- 빅데이터 분석 등의 과정에서 불필요한 개인정보가 새로 생성되거나 비식별화 처리된 정보가 재식별화된 경우에는 지체없이(통상 5 일이내) 그 개인정보를 삭제하거나 비식별화 처리

검사결과에 대한 데이터 (전체가 개인정보-민감정보로 해당된다고 간주함)
-검사 결과(보고서) 가 PDF 로 웹사이트에 업로드 되는 경우
노출사례/타인의 개인정보 접근 및 해킹에 대한 조치

수집된 개인정보를 빅데이터 분석 및 이용 시 가명처리와 총계처리로 특정개인 데이터 비식별화

(1) 가명처리: 개인정보 중 주요 식별요소를 다른 값으로 대체하여 개인식별을 곤란하게 함 (이름 수정, 나이 범주화, 라이선스 명칭 세모팀 구성원들만 식별 가능하도록 특정 코드를 만들어서 바꾸기 예) 임상자격증 1급: 1e, 임상자격증 2급: 1k 등

(예) 홍길동, 35세, 서울 거주, 한국대 재학 → 임꺽정, 30대 서울 거주, 국제대 재학 * 다른 값으로 대체하는 일정한 규칙이 노출되어 역으로 개인을 쉽게 식별할 수 있어서는 안된다.

(2) 총계처리 데이터의 총합 값을 보임으로서 개별 데이터의 값을 보이지 않도록 함

(예) 임기현 180cm, 홍길동 170cm, 이*현 160cm, 김*동 150cm → 물리학과 학생 키 합 : 660cm, 평균키 165cm * 단, 특정 속성을 지닌 개인으로 구성된 단체의 속성 정보를 공개하는 것은 그 집단에 속한 개인의 정보를 공개하는 것과 마찬가지 결과가 나타나므로 그러한 정보는 비식별화 처리로 볼 수 없음 (예> 에이즈 환자 집단임을 공개하면서 특정인물 '갑'이 그 집단에 속함을 알 수 있도록 표시하는 것은 '갑'이 에이즈 환자임을 공개하는 것과 마찬가지임)

*데이터 제3법으로 인해 개인정보 중 가명 정보는 통계작성, 연구 등 목적으로 사용이 완전히 가능하게 되었다. 다만, 가명정보의 안전한 이용을 위해 보안 장치를 의무화해야 한다.

이에따라 세모는 보안시설을 갖춘 전문기관을 통해 결합할 수 있고, 전문기관 승인 거쳐 반출 허용 가능하다.

비식별화 이후 주기적인 검토 (보관)

(1) 비식별화 했을 경우 시간의 경과에 따라 데이터 분석기술의 진화 및 관련 공개정보가 누적되어 재식별 위험이 증가할 수 있으므로 비식별화 기법 및 재식별 가능성에 관한 주기적 모니터링 실시

- 재식별이 되는 경우 추가 비식별화 등의 보완 조치 및 향후의 비식별화 처리 기법 개선 시 반영

(2) 생성되거나 재식별화된 개인정보의 관리 철저

- 빅데이터 분석 등의 과정에서 불필요한 개인정보가 새로 생성되거나 비식별화 처리된 정보가 재식별화된 경우에는 지체없이(통상 5 일이내) 그 개인정보를 삭제하거나 비식별화 처리

3. 이용

(개인정보를 연구에 활용하는 경우) 개인의료정보를 임상자료 연구에 활용하기 위해서는 성명, 주소, 전화번호, 팩스번호, 메일주소, 각종의 번호, 지문 등의 생체정보, 얼굴 전체의 사진 및 유사한 것 등 18 개의 민감건강정보(Protected Health Information;PHI)를 익명화해야 한다.

4. 파기

보유기간이 경과한 개인정보는 종료일로부터 지체 없이 파기한다

서비스 가입 해지, 폐지 또는 종료 등 개인정보파일이 불필요하게 되었을 때에는 개인정보의 처리가 불필요한 것으로 인정되는 날로부터 지체 없이 그 개인정보파일을 파기한다

개인정보를 파기할 때에는 다시 복원하거나 재생할 수 없는 형태로 완벽하게 파기해야 한다. 하드디스크, CD/DVD, USB 메모리 등의 매체에 전자기적으로 기록된 개인정보는 다시 재생시킬 수 없는 기술적 방법으로 삭제하거나 물리적인 방법으로 매체를 파괴하여 복구할 수 없도록 해야 하며, 종이와 같이 출력물의 형태로 되어 있는 경우에는 물리적으로 분쇄하거나 소각하는 방법으로 해당 개인정보를 완전히 파기해야 한다.

법령상 의무보관 개인정보의 보존방법

법령에 따라 개인정보를 파기하지 않고 보존하는 경우에는 개인정보가 포함된 게시물 비공개 처리 개인정보가 포함된 게시물 삭제 처리

5. 검색엔진 자동저장 내용 삭제 요청

01. 검색 검색포털에서 노출된 페이지의 URL 또는 노출된 값 검색

02. 삭제 신청 검색포털 별 웹마스터 도구 또는 고객센터를 통해 삭제 신청 및 삭제

03. 삭제 확인 재검색을 통해 원본 페이지 및 캐쉬 페이지 삭제 여부 확인