

빅데이터 시대, 건강정보와 정보인권

장여경
(진보네트워크센터
정책활동가)

정보인권

개인정보 자기결정권 (헌재 2005. 5. 26. 99헌마513 등)

개인정보자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리이다. 즉 정보주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리를 말한다.

개인정보자기결정권의 보호대상이 되는 개인정보는 개인의 신체, 신념, 사회적 지위, 신분 등과 같이 개인의 인격주체성을 특징짓는 사항으로서 그 개인의 동일성을 식별할 수 있게 하는 일체의 정보라고 할 수 있고, 반드시 개인의 내밀한 영역이나 사사(私事)의 영역에 속하는 정보에 국한되지 않고 공적 생활에서 형성되었거나 이미 공개된 개인정보까지 포함한다. 또한 그러한 개인정보를 대상으로 한 조사·수집·보관·처리·이용 등의 행위는 모두 원칙적으로 개인정보자기결정권에 대한 제한에 해당한다.

개인정보 보호 원칙

개인정보보호법 제3조

- ① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.
- ② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.
- ③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.
- ④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다.
- ⑤ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다.
- ⑥ 개인정보처리자는 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.
- ⑦ 개인정보처리자는 개인정보의 익명처리가 가능한 경우에는 익명에 의하여 처리될 수 있도록 하여야 한다.
- ⑧ 개인정보처리자는 이 법 및 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.

개인정보

살아있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보 ※ 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함

만약 이 단서만 가린다면? => 비식별화 논쟁

※ 유럽 : “Personal data” as

“information relating to an identified or identifiable natural person”

- “identifiable” person is “one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.”
- In determining whether a person is identifiable, “account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person.”

건강정보

개인정보보호법 제23조(민감정보의 처리 제한)

개인정보처리자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 "민감정보"라 한다)를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.

1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 민감정보의 처리를 요구하거나 허용하는 경우
(의료법 상 “정당한 사유”로 발급하는 전자처방전, 전자의무기록)

빅데이터

단지 big 한 data 만은 아닙니다

- 공개된 정보
“비식별화 처리된 공개된 정보, 이용내역정보, 생성 정보는 이용자 동의 없이 제3자 제공이 가능하다.”(방송통신위원회 빅데이터 가이드라인 제10조)
- 생성중인 정보
“비식별화 조치를 취한 후 이용내역정보를 수집·이용할 수 있다.”(빅데이터 가이드라인 제5조 제1항)
※ “이용내역정보”란 이용자가 정보통신서비스를 이용하는 과정에서 자동으로 발생하는 서비스 이용기록, 인터넷 접속정보, 거래기록 등의 정보
- 새로운 정보의 생성 (빅데이터 가이드라인 제6조)
※ “목적외” 이용

빅데이터

개인정보 상업화

- “인류발전의 5번째 원동력...데이터”
- “빅데이터는 '21세기 원유'... 정보가 바로 돈이다”
- “빅데이터가 가진 잠재력과 파급효과를 분석한 다수의 글로벌 전문기관의 보고서에서 빅데이터의 혜택이 가장 큰 핵심 적용분야로서 보건의료분야를 제시하고 있다. 예를 들어, 맥킨지에 의하면 미국의 의료부문은 빅데이터 활용으로 연간 약 3,300억 달러(약 350조원)의 직·간접적 비용절감효과를 기대할 수 있다고 분석하고 있다. 이러한 수치는 미국 정부 의료예산의 약 8%에 해당하는 엄청난 규모다.” (한국정보화진흥원 부원장)

빅데이터와 정보인권

유럽연합 제29조 작업반

- 데이터 수집, 추적, 프로파일링의 가파른 증가 규모에 대한 우려 : 수집된 데이터들의 다양성과 상세함, 데이터들이 종종 다른 많은 출처의 데이터들과 결합
- 정보 보안에 대한 우려 : 양적 팽창에 비해 뒤쳐지는 것으로 보여지는 보호 수준
- 투명성에 대한 우려 : 충분한 정보가 제공되지 않는다면 개인(소비자나 이용자)은 자신이 이해하지 못하고 통제할 수 없는 결정에 종속될 수 밖에 없음
- 부정확성, 차별, 배제, 경제적 불균형에 대한 우려 : 알고리즘은 연관성에 주목하여 통계적인 추론을 산출하는데, 이것이 마케팅이나 다른 의사결정에 부당하고 차별적인 영향을 미칠수 있음. 현존하는 편견이나 스테레오 타입을 영속시키고, 사회적 배제와 계층화 문제를 악화시킬 수 있음. 구직 기회, 은행 대출, 건강보험 선택사항 등.
- 정부 감시의 강화 가능성

빅데이터와 정보인권

유럽연합 GDPR(개인정보보호규정) 연내 제정 임박

- 빅데이터에 대한 ‘프로파일링’ 과정에서 정보주체의 권리 보호
 - ※ 프로파일링 : 개인을 평가하거나 개인의 업무실적, 경제적 상태, 위치, 건강, 개인 선호, 신용 상태나 개인의 행동을 분석 또는 예측하기 위해 이루어지는 개인정보의 자동화된 처리를 말함

빅데이터 처리에서도 개인정보인 경우 정보주체의 동의권 보장

빅데이터 처리를 하려면 더이상 개인정보가 아니도록 철저히 익명화

그러나 처리 과정 중에 재식별되거나 사생활 침해가 발생할 위험성이 있으므로 목적 부합성에 대해 지속적으로 평가

빅데이터와 건강정보

공공의료

국민건강보험의 시행을 위한 의료정보의 조사, 복지혜택의 부여를 위한 소득 등의 조사, 전염병의 예방을 위한 질병조사, 사회생활지표의 작성을 위한 통계조사 등 (권건보)

보건의료분야 공공 빅데이터 현황

- 이연희 (한국보건사회연구원 책임전문원) “보건복지포럼 (2015. 9.)”

구분	보유기관	내용	공개여부
건강보험 표본 코호트 DB ¹⁾	국민건강 보험공단	<ul style="list-style-type: none"> - 자격DB: 건강보험가입자 및 의료급여수급권자의 성, 연령대, 지역, 사회경제적 변수, 장애, 사망관련 등 - 진료DB: 요양급여 청구자료로서 진료, 상병, 처방 관련 변수 - 건강검진DB: 검진 주요결과 및 문진에 의한 생활습관 및 행태관련 자료 - 요양기관DB: 요양기관 종별, 설립구분, 지역, 시설, 장비, 인력관련 자료 	제한적 공 개
환자 데이터셋 ²⁾	건강보험 심사평가원	- 건강보험 청구자료를 기초로 진료개시일 기준 1년 간 진료 받은 환자 대상의 표본 데이터	제한적 공 개
한국인체 자원 ³⁾	질병관리 본부	- 공여자로부터 기증받은 인체유래물(DNA, 조직, 혈액, 뇨 등)과 임상(진단명, 수술명, 병리조직검사결과, 혈액검사 등), 역학(성별, 생년월일, 음주력, 흡연력 등) 및 유전(SNP, CNV, Exome 등)정보	제한적 공 개
지역보건 의료정보	사회보장 정보원	- 전국 보건기관(보건의료원, 보건소/지소, 보건진료소)의 보건사업 및 행정업무, 전자 의무기록 및 진료관련(진료내역 및 검진결과 등) 정보	미공개
지역사회 건강조사	질병관리 본부	- 지역 보건의료계 획수립 및 보건사업 평가 활용 지표로서, 건강행태, 건강검진 및 예방접종, 질병이환, 의료이용, 사고 및 중독, 활동제한 및 삶의 질, 보건기관 이용, 사회 물리적 환경, 심정지, 교육 및 경제활동 등	공 개
국민건강 영양조사	질병관리 본부	<ul style="list-style-type: none"> - 국민의 건강 및 영양 상태에 관한 현황 및 추이 파악 - 신체계측, 비만, 고혈압 등 검진조사, 흡연, 음주, 비만 및 체중조절, 신체활동 등 건강설문조사, 식품 및 영양소 섭취현황, 식생활행태, 식이보충제 등 영양조사 	공 개
한국의료 패널	한국보건 사회연구원	<ul style="list-style-type: none"> - 개인의 건강수준, 의료이용 및 의료비 지출 요인, 건강행태, 의료욕구, 보건의료서비스 수요행태 변화분석 - 사회경제적 특성, 의약품 구매, 경제활동, 건강수준, 의약품 복용행태, 민간의료보험, 건강기능식품, 건강행태 등 	공 개

빅데이터와 건강정보

보건복지관련 공공 데이터 활용 서비스 (법령/동의/익명화)

보건의료 공공 빅데이터 활용 가능한 R&D 사업 예시

- 유전체 의료 빅데이터 마이닝을 통한 개인별 질환 발생예측 기술 개발
 - 지역별 일차의료지표 산출을 통한 지역주민의 건강 및 질병 감시 및 예보시스템 개발
 - 건강보험 · 진료비의 허위·부당청구 및 의료서비스 오남용 감시 및 관리 시스템 개발
 - 의료보장성 강화를 위한 건강보험 재정규모 감시 및 예측 시스템 개발
 - 건강보험 수가 적합성 및 부과 형평성 분석시스템 개발
 - 보건의료 빅데이터 시계열 분석 기반 복합만성질환 예측 기술
 - 진단/처방의 신뢰도 향상을 위한 보건의료 빅데이터 기반 진단결정 지원시스템 개발
 - 빅데이터 기반 적정 의료기관 이용모형 개발
-

서비스	주요내용	데이터 종류
국민건강 알람서비스	4단계 건강위험 예보 발령, 개인건강기록 시스템을 통한 맞춤형 건강정보 제공	진료내역, 의약품 처방, 건강검진 정보 등 (국민건강보험공단)
건강검진 진료정보	검진결과 맞춤형건강서비스	건강검진 정보, 의료기관 이용 내역 등 (국민건강보험공단)
뇌졸중위험예측 프로그램	뇌졸중과 관련된 고혈압, 콜레스테롤, 생활습관, 가족 력, 환경요인 등을 기초로 10년 이내에 뇌졸중에 걸릴 위험도 평가	건강검진정보, 문진정보 등 (국민건강보험공단)
대사증후군 맞춤정보	대사증후군 요소와 관련한 건강상태 및 위험요인별 맞춤형 처방정보 제공	건강검진정보, 문진정보 등 (국민건강보험공단)
운전면허 발급 간소화 서비스	국가건강검진정보 중 운전면허 적성검사에 필요한 시력·청력 정보 공동이용	국가건강검진정보 (국민건강보험공단)
갑상선암 의사에 게 꼭 물어보세요	갑상선암 정보, 종합병원 전문의와 1:1 맞춤형 상담	병원정보 (건강보험심사평가원)
병원 약국찾기	위치기반 서비스와 연동하여 내 주변의 병원, 약국, 응급의료기관 위치정보 제공	전국 응급의료정보 (국립중앙의료원)
MediMap	서울 소재 병원 규모별, 카테고리별 병원 위치, 연락처 정보 제공	전국병원정보 (공공데이터활용지원센터)
처방약 토탈 검색	약국 위치, 개폐정보	약국정보 (국립중앙의료원)
4th-Life	요양병원 정보 제공	-
울은 서비스	식단 재료의 합리적 구매기준을 위한 식단정보, 가격 정보, 성분정보	식단정보, 가격정보, 성분정보 (식품의약품안전처)
대전당직병원	대전지역 당직병원 응급실정보, 전화번호, 주소, 병원 등급 등 정보 제공	당직의료기관정보 (대전광역시)
헬스온스토리	상황인식기술 통한 사용자 맞춤형 건강정보 자동제공	보건기상지수정보 (기상청)

빅데이터와 건강정보

타겟마케팅과 민감정보 [결과적] 생성

미국 할인매장업계 2위인 '타겟'은 지난 2012년 고객으로부터 거센 항의를 받았다. 타겟이 고등학생인 딸에게 유아용품 할인쿠폰을 보냈기 때문이다.

타겟이 고등학생에게 유아용품 할인쿠폰을 보낸 것은 빅데이터를 활용했기 때문이다. 여성이 임신하면 초기에는 영양제, 중기에는 로션, 말기에는 유아용품을 주로 구매한다는 통계분석 결과가 바탕이 됐다. 여고생이 영양제를 구입한 후 얼마 지나지 않아 로션을 구매하자 타겟 측은 출산시점이 머지않았다는 판단 아래 유아용품 할인쿠폰을 보낸 것이다.

알고 보니 이 여고생은 진짜로 임신 중이었다. 부모조차 몰랐던 딸의 임신사실을 유통업체가 빅데이터를 기반으로 한 구매행태분석 기반의 예측시스템을 통해 '먼저' 알았던 것.

월스트리트 저널에서는 개인의료정보가 의료서비스 영역 뿐 아니라 신용카드정보, 쇼핑정보 등 개인의 일상적인 생활정보에서도 정교한 데이터 알고리즘에 의해 원치 않게 수집·이용되고 있음에 우려를 나타내기도

빅데이터와 건강정보

보건의료 관련산업 혁신

- 김현곤 (한국정보화진흥원 부원장) “보건복지포럼 (2015. 9.) 권두언”

빅데이터분석기술은 질병의 정확한 현재 실태, 발생 원인, 최적의 해결책, 예상되는 위험징후와 미래가
능성 분석 등을 가능하게 해주는 지능화기술이다. 데이터 분석·처리기술이 고도화됨에 따라 이제는 원
하는 거의 모든 전수데이터를 빠른 시간내에 분석하고 처리할 수 있는 것이 손쉽게 가능해지고 있다. **게**
다가 대한민국은 이미 전 국민의 건강과 질병, 진료기록 등에 관한 10년 이상의 데이터가 거의 완벽하게
디지털화되어 축적되어 있다. 최적의 보건의료, 보건복지 대안 모색을 지원하는 빅데이터분석환경이 이
미 완비되어 있는 셈이다 ... 먼저 평생에 걸쳐 개인맞춤형 건강의료서비스가 가능하다. 자신의 질병과
진료기록을 가지고 있고 전 국민의 관련질병과 진료기록을 분석하면 개개인에게 최적의 건강의료서비
스를 제공할 수 있다. 여기에 유전자분석까지 융합된다면 그 효과는 더욱 커진다. 4대 만성질환처럼 국
가차원에서도 비용이 많이 소요되고 개인차원에서도 극복하기 힘든 핵심질환 등에 대해서도 데이터분
석을 통한 과학적인 예방이 가능해진다. 따라서 매년 수조원 이상의 예산절감도 가능해질 것이다. 빅데
이터 분석활용이 확산됨에 따라 병원과 약국 등 보건의료분야의 경쟁력도 높아지고 보건의료 관련산업
의 혁신적인 성장도 가능하다.

빅데이터와 건강정보 (유럽 GDPR 의 예)

특별한 범주의 개인정보 [민감정보] 처리

원칙적으로 인종, 출신 민족, 정치적 견해, 종교 및 신념, 노동조합 가입 여부, 유전자, 건강, 성생활, 형사 판결 또는 보안 처분 등을 포함하는 개인정보의 처리는 금지된다. 다만, (a) 정보주체가 ... 동의하는 경우 (b) 회원국 법률에 의해 승인받는 경우 ... (h) 건강을 위해 그리고 제81조에서 규정한 조건 및 안전 장치에 따라 건강과 관련된 정보를 처리하는 경우 예외

잊힐 권리 및 삭제권

개인정보의 보유가 필요한 다음의 경우를 제외하고, 개인정보처리자는 개인정보를 지체 없이 삭제하여야 한다. 즉, (1) 제80조에 따라 표현의 자유에 대한 권리를 행사하는 경우, (2) 제81조에 따라 공공보건 부문에서 공익을 위한 경우, (3) 제83조에 따라 역사, 통계, 과학 연구 목적으로 필요한 경우, (4) 유럽연합 또는 개인정보처리자가 속한 회원국의 법률에 의해 개인정보를 보관해야 하는 법적 의무를 준수해야 하는 경우, (5) 제4항에 따라 개인정보의 처리를 제한하여야 하는 경우에는 예외적으로 개인정보를 보유할 수 있다.

빅데이터와 건강정보 (유럽 GDPR 의 예)

건강 관련 정보 특칙

GDPR 범위 내에서 그리고 제9조 (2)항에 따라, 건강과 관련된 개인정보의 처리는 정보주체의 정당한 이익과 다음 사항을 보호하기 위한 적절하고도 구체적인 기준을 제공해주는 유럽연합 또는 회원국 법률에 기초하여야 한다. 즉, (a) 업무상 비밀 의무를 준수해야 하는 건강 전문가 나 회원국 법률 또는 국내 관련 기관에서 제정한 규정을 준수해야 하는 다른 사람이 정보를 처리하는 경우로써, 예방 의학 또는 직업병 의학, 의학 진단, 치료, 처치, 건강 서비스의 관리 등을 위한 목적, (b) 국가들 사이에서의 건강 위협에 대한 보호나 의약품 및 의료용품의 품질이나 안전에 대한 높은 품질 보증 등과 같은 공공 건강 분야에서의 공공의 이익, (c) 사회적 보호, 특히 건강 보험 시스템에서의 혜택과 서비스에 대한 분쟁을 해결하는데 사용하는 절차의 비용 효율성 등의 분야와 관련된 공공의 이익과 같은 목적을 위하여는 구체적인 기준을 법률에 규정하여야 한다. 진단법 개선 및 유사한 종류의 질병 사이에서의 구별, 치료를 위한 연구 준비 등과 같은 역사, 통계, 과학 연구 목적에 필요한 건강 관련 개인정보의 처리는 제83조에서 규정된 조건과 안전 장치 등을 준수하며 이루어져야 한다.

빅데이터와 건강정보 (미국의 예)

HIPAA (Health Insurance Portability and Accountability Act,
건강보험 이전과 책임에 관한 법)
Privacy Rule

- 보호를 받는 의료정보(PHI) : 개인을 식별할 수 있는(individually identifiable) 정보' 혹은 '개인을 식별할 수 있는 합리적인 근거가 있는(reasonable basis) 정보
- 보호대상 제외 : 비식별화된 의료정보(de-identified health information)는 전면적 규율면제로 누구나 자유롭게 이용 및 제공할 수 있음을 명시

익명화와 비식별화

현행 개인정보보호법 (제18조 제2항)

개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다.

4. 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우

‘비식별화’ 법령화 시도

- 2014. 12. 23. 방송통신위원회, 빅데이터 가이드라인 제정
- 2014. 12. 행정자치부-정보화진흥원, 비식별화 안내서 발간
- 2015. 6. 3. 금융위원회, 금융회사와 핀테크 기업의 동반성장 토대를 구축하기 위한 ‘빅데이터 활성화 방안’을 발표 - 신용정보법 시행령 개정 계획
- 국회에도 유사한 내용의 법안 다수 발의

익명화와 비식별화

비식별화

- “비식별화”란 데이터 값 삭제, 가명처리, 총계처리, 범주화, 데이터 마스킹 등을 통해 개인정보의 일부 또는 전부를 삭제하거나 대체함으로써 다른 정보와 쉽게 결합하여도 특정 개인을 식별할 수 없도록 하는 조치를 말한다.(방통위 빅데이터 가이드라인)
- 비식별화(de-identification) : 정보의 일부 또는 전부를 삭제·대체 하거나 다른 정보와 쉽게 결합하지 못하도록 하여3) 특정 개인을 알아볼 수 없도록 하는 일련의 조치(행자부 비식별화 안내서)

익명화

- 익명화(Anonymization) : 비식별화 조치의 궁극적인 상태로, 개인에 대한 재식별이 더 이상 불가능한 상태 (행자부)
- the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable (유럽)

익명화와 비식별화

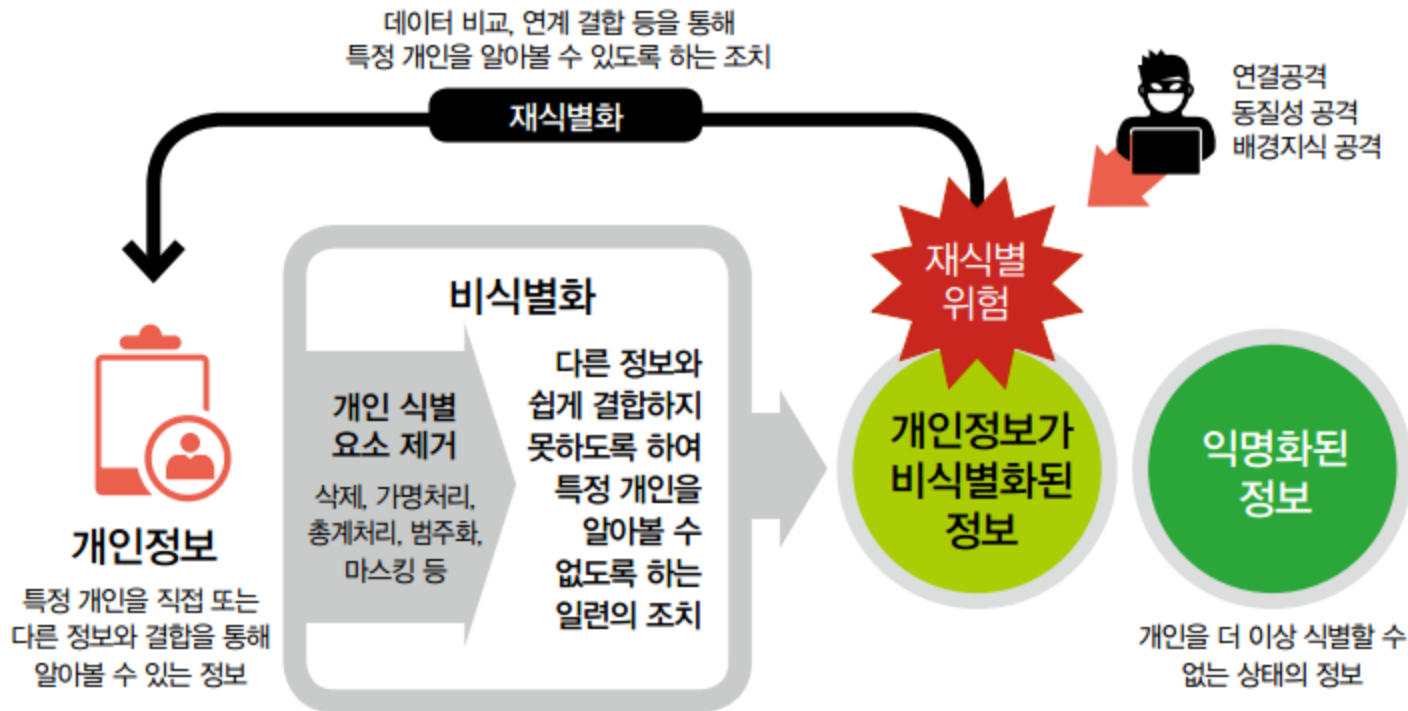
재식별화

- 재식별화(re-identification) : 비식별화한 개인정보를 다른 정보 또는 데이터와 비교, 연계, 결합 등을 통해 특정 개인을 알아볼 수 있도록 하는 일련의 조치 (행자부)
- 특히 악의적이고 목적의식이 뚜렷한 경우, 다양한 데이터를 결합해 자신들의 목적에 적합한 개인을 식별하고자 할 가능성이 높음 / 최근 정부의 공공정보 개방·공유 정책 등에 따라 공개적으로 수집할 수 있는 데이터의 증가로, 재식별 의도가 있는 이용자들은 이미 공개된 정보조각들을 보유하고 있을 가능성이 높음

한국적 특수성

- 인터넷 서비스에서 본인확인이 널리 이루어지고 있음
- 빅데이터에서 서로 다른 개인을 연결하는 키값으로 (이미 널리 유출된) 주민번호가 활용됨

익명화와 비식별화



익명화와 비식별화

‘비식별화’ 법령화의 주요내용 : 개인정보의 수집, 제공 등 처리 과정에서 요구되는 정보주체의 동의/법적 규제 절차를 생략하거나 우회

정보통신서비스 제공자가 개인정보가 포함된 공개된 정보를 비식별화 조치한 경우에는 이용자의 동의 없이 수집·이용할 수 있다. 다만, 이용자의 동의를 받거나 법령상 허용하는 경우에는 비식별화 조치를 취하지 아니하고 수집·이용할 수 있다. (빅데이터 가이드라인 제4조)

한국보건사회연구원

“민감정보와 같은 개인정보를 제3자에게 제공하려면 정보주체의 동의를 받아야 하는데 엄청난 수의 정보주체에게 동의를 받는 것은 상당한 시간과 노력 외에도 정보 제공 시마다 반복적으로 동의를 받는 것이 사실상 불가능하다 ... 암호화·익명화 기술이 뒷받침된다면 정보주체는 개인정보의 안전한 사용이라는 신뢰를 바탕으로 개인정보의 공익적 활용을 묵인할 수 있을 것”

“정보접근 및 정보처리에 대한 통제를 강하게 하면 정보활용을 활성화 할 수 없기 때문에 빅데이터의 ‘활용과 보호의 균형’ 마련되어야”

재식별화의 위험성 - 데이터 연계

뉴질랜드 통계청

- 데이터 연계가 새로운 통계를 생성하거나 기존 통계의 질을 향상시킬 수 있는 경우에만 수행한다.
- 데이터를 연계해서 경비를 줄이거나 질을 높이거나 규제를 줄이는 등의 가치가 있는 경우에만 데이터 연계를 고려한다.
- 데이터연계의 이득이 개인정보보호의 위험에 비하여 월등히 높은지를 고려한다.
- 원자료의 순수성을 해치지 않는 범위에서 데이터 연계를 고려한다.
- 데이터 제공자가 데이터 연계를 반대하는 경우 연계하지 않는다.
- 데이터 연계는 반드시 데이터를 제공한 모든 기관은 동의를 얻는다.
- 연계된 데이터는 공식 통계나 관련 연구에만 사용한다.
- 필요 이상으로 데이터나 변수를 연계하지 않는다.
- 연계 데이터는 다른 데이터와는 따로 관리한다.
- 이름이나 주소 등의 개인식별자는 데이터 연계 시에만 사용하고 파기한다.
- 연계된 데이터에는 외부기관에서 사용하고 있는 개인식별자(예: 아이디 등)등을 포함하지 않는다.
- 데이터 연계는 공개적으로 진행한다.

보건 의료 정보의 연계요건은?

재식별화의 위험성 - 데이터 연계

- ◎ 미국 매사추세츠 주의 단차료 병원 출입 기록을 요약
- 공개 정보에서 이름, 주소, 자 관련 100여개의 속성정보
※ 준식별정보에 해당하는 정보
- ◎ 또한 매사추세츠 주에서는 부를 공개(판매)하고 있었음
- ◎ 일련의 연구자가 투표자 식별을 시도하였으며, 그 결과
- ◎ 즉, 매사추세츠 주가 공개한 의료정보를 재식별 가능



IMS 헬스코리아 사건



IMS 헬스코리아 사건

검찰 기소 보도자료 (2015. 7. 23.)

- **의료법·약사법상 환자정보의 외부유출 금지**

- 의료인, 약사한약사는 업무상 알게 된 환자의 비밀을 누설하여서는 아니되며 (의료법 제19조, 약사법 제87조), 의료인이나 의료기관 종사자는 환자 기록을 제3자에게 열람하게 하거나 내용을 확인할 수 있게 해서는 아니됨(의료법 제21조)
- 누구든지 정당한 사유 없이 전자처방전에 저장된 개인정보를 탐지하거나 누출·변조·훼손해서는 아니되며(의료법 제18조 제3항), 병원이 약국에 전자처방전을 발송하려면 환자의 발송 요구가 있어야 함(의료법시행규칙 제12조)
- 결국, 환자정보의 업무 수탁자라 할지라도 병원·약국 밖으로 환자정보를 전송하여 저장하는 행위는 수탁범위를 초과하는 것으로서 금지된다고 할 것임

IMS 헬스코리아 사건

형사재판 쟁점

- **IMS**헬스는 약정원과 지누스측에 환자 주민등록번호를 알파벳 형식으로 암호화하는 방식을 개발해 제공한 만큼 민감정보[개인정보]가 아님을 주장 “수집된 환자진료 및 처방정보는 각기 다른 개인을 구분할 정도는 되지만 개개인을 식별할 수 있는 민감정보는 아니다.”
- 약학정보원 번호를 맡고 있는 태평양 측은 “서울대 법과대 고학수 교수의 법리적 의견에 따르면, 주민번호를 일방향 암호화 방식으로 암호화한 경우나 양방향으로 암호화해 복호화가 불가능하도록 수행하는 경우, 암호화된 식별정보는 그 자체로서 고유식별정보로서 가치를 상실한다”는 의견
- 이미 건강보험심사평가원에서 환자의 이름, 피보험자, 성명, 주민등록번호 등의 정보가 전송되고 있으며, **PM2000**에는 이를 암호화한 정보를 **IMS**측에 제공한 것이라고 반박
- 지누스의 변호를 맡고 있는 화우 측 역시 “**IMS**에 전달한 통계정보는 개인 식별이 불가능한 비식별 정보이다”라고 주장하면서 “검찰은 [2011년] 개인정보보호법이 시행되기 이전에 적법하게 처리된 개인정보까지 소급해 적용하고 있다”고 지적

빅데이터 시대 건강정보 보호의 쟁점

개인정보보호법 관련

익명화와 개인이력연구의 경계: '주민등록번호' 쟁점

개인정보 상업화와 건강정보의 보호: '비식별화' 쟁점

의료관련법률

공공의료와 개인정보 자기결정권의 조화

권력관계 속에서 '동의' 요건의 한계

더욱 민감한 정보의 보호

생체정보와 유전체 정보의 보호 한도

차별 목적과 결과적 차별의 방지