

코로나19 관련 개인 건강정보 활용 및 침해 사례

수시 보고서

2020년 12월

코로나19 관련 개인 건강정보 활용 및 침해 사례

< 목 차 >

1. 개요 및 배경
2. 코로나19 대응을 위한 개인 건강정보 활용 사례
 - (1) 공공 대응 사례
 - (2) 민간 기업 대응 사례
3. 코로나19 대응 과정에서 발생 가능한 개인정보 침해 이슈 및 사례
 - (1) 정보 연동을 통한 개인정보 침해
 - (2) 건강정보에 근거한 차별과 불평등
 - (3) 개인정보 유출
4. 시사점

1. 개요 및 배경

- ▶ 2020년 전 세계적인 코로나19 확산과 함께 각국 정부와 민간 부문의 일선 대응 과정에서 개인 건강 데이터의 수집 및 처리가 불가피해지고 있으나 감염병 확산 통제 목적을 위해 개인정보보호 가치가 유보될 수는 없는 상황
 - 이는 △코로나19의 신속한 종식을 위해 개인 건강 관련 데이터(이하 건강정보)의 효과적인 이용이 필요하다는 사실과 △개인 건강정보의 익명성을 유지하고 개인정보 오남용을 방지해야 한다는 사실 사이의 균형을 요구
 - 실제로 방역을 위한 적극적인 대응 과정에서 개인 건강정보 처리의 투명성과 비례성 원칙이 지켜지지 않아 시민의 기본권을 침해할 수 있다는 논란을 야기한 사례들도 등장
 - 이와 관련, 본 고에서는 코로나19 확산 방지라는 공중 보건의 대의(大義)를 위해 개인 건강정보를 수집 및 처리하는 과정에서 발생한 개인정보보호 관련 이슈에 대해 검토

2020년 12월

2. 코로나19 대응을 위한 개인 건강정보 활용 사례

(1) 공공 대응 사례

- ▶ 영국 NHS(National Health Service) 산하의 NHSX는 코로나19 방역 대응을 위해 "Covid-19 데이터스토어(Covid-19 datastore)" 구축
 - ‘Covid-19 datastore’의 주요 목적은 장관과 정부기관 담당자들에게 공중보건 현황 및 건강 서비스와 관련한 실시간 정보를 제공하는 것으로, 바이러스의 확산을 모니터링하고 환자가 서비스와 지원을 받을 수 있도록 정확한 현황 파악 자료 제시
 - 영국의 보건 사회복지부 장관(The Secretary of State for Health and Social Care)은 이를 지원하기 위해, 기밀 데이터의 수집 및 배포에 대한 내용을 규율하는 환자정보 통제규정(Control of Patient Information (COPI) Regulations 2015)에 따른 통지 발표
 - COVID-19에 대한 대응을 위해 수집 및 처리되는 데이터는 COPI 통지에 따라 여러 출처에서 확보되며, 응급 치료, 입원 및 외래 환자 활동 데이터 세트 등에서 집계된 데이터 등을 포함
- ▶ 프랑스는 2020년 5월 13일부터 코로나19 진단 결과를 기록하는 정부 주도의 ‘SI-DEP’ 시스템을 도입하여 병원과 임상 시험실 및 병원에서 수행한 코로나19 관련 테스트 결과 데이터를 국가 차원에서 체계적으로 기록 및 관리
 - 이 시스템에는 진단 대상자의 수와 연령대, 일일 및 주간 단위의 양성 판정자 수, 국제선 도착 시 공항에서 수행된 검사에 따른 코로나19 양성률 등의 내용을 기록
 - ‘SI-DEP’ 시스템의 활용과 관련, 프랑스의 개인정보보호 감독기구 CNIL은 데이터 이용의 안전성 확보를 위해 △해당 시스템의 데이터베이스를 사용할 조사관 및 기타 개인(분석 시험실 직원, 의사 및 기타 건강 전문가, 약사, 연구원 등)에 대한 적절한 교육 △데이터 오남용 탐지 및 처벌을 위한 추적 시스템 구축 등을 요구
- ▶ 미 보건복지부는 다양한 지역 기반 검진 장소(community-based testing sites, CBTS)가 운영되는 가운데, CBTS에서 이루어지는 환자 건강정보의 수집 및 보호에 대한 규제 완화
 - 보건복지부 민권사무소(Office of Civil Rights, OCR)는 CBTS를 HIPAA(Health Insurance Portability and Accountability Act)의 엄격한 보안 및 개인정보보호 규칙 적용 대상에서 제외

2020년 12월

- 단, CBTS의 검진 서비스 제공자가 기존의 전자건강기록시스템을 CBTS에 연동시킨 후 데이터보호 위반사항이 발생하는 경우 CBTS 이용 과정에서 데이터가 수집된 모든 정보주체에게도 해당 내용을 통지하도록 책임 부과
- ▶ 중국은 코로나19 유행 초기부터 약물 치료 목적 등을 이유로 시민들의 개인정보를 대대적으로 수집해왔으며, 이를 이용해 바이러스가 가장 널리 퍼진 지역들을 파악해왔다는 의혹 제기
- 예컨대 무인 항공기를 사용하여 거리의 군중을 스캔하고 높은 체온으로 코로나19 감염 가능성이 있는 것으로 의심되는 사람들을 식별하여 지상에 있는 감시자들에게 신호를 보내는 등 인권침해 논란의 여지가 큰 생체정보 모니터링까지 실시한 것으로 관측
- 특히 시민들이 인지하지 못하는 상황에서 드론을 통한 생체정보 수집이 이루어지고, 해당 정보의 보관 기간이나 용도 등에 대한 투명성이 확보되지 않은 것이 문제점으로 지적
- 한편, 영국과 프랑스 경찰 당국도 코로나19 확산 방지 활동을 위해 드론을 활용하는 과정에서 개인정보 침해에 대한 우려를 야기한 바 있으나 이들 국가의 경우 사회적 거리두기 위반을 모니터링하기 위한 영상촬영에 국한했던 반면 중국은 체열 감지를 통한 생체 및 건강정보를 수집했다는 점에서 차별화
- ▶ 해외 이동 과정에서 정확한 보건 정보 확인을 위해 여행자의 보건 기록을 쉽고 빠르게 체크할 수 있는 솔루션에 대한 수요가 확대됨에 따라 세계경제포럼이 지원한 비영리단체 The Commons Project Foundation은 현재 다수의 항공사와 함께 여행자 보건 기록 확인 솔루션 CommonPass 테스트 진행
 - 여행자가 각 국가별 상이한 보건 관련 요구사항을 준수했는지 확인할 수 있는 바코드를 생성하는 모바일 앱 CommonPass는 국제기구 및 항공, 보건 분야 표준 기구의 지침에 따라 여행자의 건강 정보를 수집하고 저장하는 프레임워크 구축
 - United Airlines, Lufthansa, Swiss International Air Lines, JetBlue와 Virgin Atlantic 등의 항공사가 CommonPass 이니셔티브에 참여
 - 2020년 10월 United Airlines의 Newark-London 항공편, Cathay Pacific의 Hong Kong-Singapore 항공편을 대상으로 시범 운영
 - CommonPass의 목표는 국가마다 다른 다양한 보건 입국 요건 지원을 위해 관련 정보를 쉽고 안전하게 공유할 수 있는 방안을 제시하는 것

2020년 12월

- ▶ 이 밖에 많은 국가들이 코로나 바이러스 확산 방지 과정에서 원격 의료의 잠재력에 대해 논의하고 확진자 접촉 추적 앱과 원격 진료, 코로나19 대응을 위한 개인 건강정보와 디지털 도구 활용을 수용
 - 유럽에서는 크로아티아, 폴란드, 핀란드, 스페인은 코로나19 확산 초기부터 시민들이 건강 상태를 평가하고 대응 방법을 조언 받을 수 있는 코로나19 셀프 진단 앱을 활용
 - 싱가포르, 홍콩, 호주, 뉴질랜드 등 아시아 국가들과 브라질 등 중남미 국가 등 세계 전역에서 이 같은 관리 앱을 도입
- ▶ 한편, 코로나19 관련 데이터 사용자들의 건강 데이터 보호를 위해 입법부 차원에서 법안이 발의된 사례도 등장
 - 미국 민주당 의원들이 발의한 공중보건 위급상황 시 개인정보보호법(The Public Health Emergency Privacy Act) 법안과 미 공화당의 코로나19 소비자 데이터보호법(The COVID-19 Consumer Data Protection Act) 법안이 대표적인 사례
 - 이에 따르면, 코로나19 사태와 같은 공중보건 위기 중 수집되는 건강 데이터에 대해 수집 대상·수집 주체·이용 목적 등을 엄격하게 제한
 - 건강 데이터를 수집하는 경우 △소정의 보안 기준을 충족하고 △위급 상황이 종료된 후에는 데이터를 삭제하며 △공중보건 활동을 위해 수집된 데이터를 상업 광고·고용·보험 등 목적 이외의 용도로 이용할 수 없도록 규제

(2) 민간 기업 대응 사례

- ▶ 영국 정부의 코로나19 대응 조치의 일환으로 진행 중인 데이터 마이닝(data-mining) 업무와 관련해 여러 기술 기업이 참여하여 환자의 개인 건강정보 처리
 - 이 프로젝트를 추진한 영국 NHS(National Health Service)의 디지털 전환 담당 사업부 NHSX는 기술 기업들과 도급 계약을 체결
 - 원칙적으로 해당 기술 기업들은 데이터를 통제할 수 없고, NHS 시스템을 통해서만 데이터에 접근 가능하며, 자체 목적을 위한 데이터의 이용과 공유도 불가능하다는 것이 NHS의 설명

- 접근이 허용된 데이터는 총계화 되거나 익명화 처리된 데이터로 한정되었음에도 불구하고 이 프로젝트를 수행하는 과정에서 전례 없이 방대한 규모의 개인 건강정보가 처리되고 개인정보보호나 데이터 윤리에 대한 고려가 충분히 이루어지지 않은 채 과업이 수행되고 있다는 비판 제기
- ▶ Google의 ‘Project Baseline’은 일반인 대상의 자가진단 온라인 서비스를 표방하며 웹사이트를 통해 코로나19 테스트를 원하는 사람들의 건강정보를 Google이 수집한 다른 데이터와 연결
 - Google 계열사인 의료서비스 전문 업체 Verily가 코로나19 자가진단과 관련한 정보를 제공하는 웹사이트 ‘Project Baseline’ 서비스를 캘리포니아 일부 지역 주민들을 대상으로 서비스 운영
 - Project Baseline은 당초 다양한 배경을 가진 인구집단의 건강 관련 데이터를 취합하여 질환 위험 요인을 규명하고 의료서비스 접근을 개선할 수 있는 헬스케어 기술 개발 과제로 2017년 출범한 바 있으며, 2020년에는 코로나 19 확산 대응을 위해 개인별 건강 데이터를 활용한 자가진단 지원
 - 다양한 진단 결과 데이터는 물론 전자건강기록 및 건강보험 청구에 관한 데이터도 폭넓게 취합하는 Project Baseline은 유전 정보 수집 등에 한정되었던 기존의 건강 데이터 프로젝트에 비해 훨씬 더 방대한 임상 정보를 수집할 수 있다는 점에 주목
- ▶ Apple은 자사가 운영해온 코로나19 추적 앱과 웹 사이트의 업데이트를 통해 사용자가 미국 질병통제예방센터(U.S. Centers for Disease Control and Prevention)와 개인정보를 공유할 수 있도록 개편
 - 사용자는 자신의 연령, 건강상태, 증상, 코로나19에 대한 노출 가능성 등을 익명으로 공유할 수 있으며, 질병통제예방센터에 제공된 데이터는 코로나19 방역을 위한 자료로 활용 가능
 - Apple에 따르면 데이터는 개인정보보호를 위해 비식별 상태로 제공되며 총계 처리된 데이터를 기반으로 코로나19와 관련된 잠재적 위험 요소와 감염 노출 가능성 등에 대한 최신 정보를 제공할 수 있도록 지원
 - 그러나 Apple과 같이 방대한 사용자 기반을 보유한 거대 기술기업이 민감한 개인 건강 데이터를 다량으로 수집하고 이를 공공기관과 공유하는 과정에서 개인정보 침해 가능성이

2020년 12월

가중될 수 있다는 우려도 제기

3. 코로나19 대응 과정에서 발생 가능한 개인정보 침해 이슈 및 사례

(1) 정보 연동을 통한 개인정보 침해

- ▶ 코로나19 백신의 출시가 임박한 것으로 기대되는 가운데, 백신 접종 과정에서 오류 가능성을 통제하기 위해 백신 접종 자료를 생체 인식 정보와 연동할 경우 개인정보 침해 우려가 증폭될 것으로 우려
 - 예컨대 백신 투여 후 홍채 또는 지문을 스캔하고 두 기록을 연결하여 저장함으로써, 향후 해당 정보주체의 예방 접종 여부를 확인할 수 있는 방식 채택 가능
 - 이 경우 중복 접종에 따른 사고 가능성을 낮추고 신속하고 포괄적인 예방 접종 캠페인을 기대할 수 있으나, 전문가들은 개인정보보호 및 데이터 보호 측면에서 적지 않은 문제점이 노출될 것이라고 경고
 - 이와 관련, 민권단체 European Digital Rights의 Ella Jakubowska 이사는 신속한 접종을 위해 사전 동의 원칙 등이 무시될 수 있다는 점을 지적
 - 또한 정부가 생체인식 정보를 사용하여 대량 감시 시스템을 설정하거나 민간 기업이 생체 인식 데이터 저장소를 활용하여 고객 프로파일링과 표적광고에 나설 가능성에 대한 우려 제기
- ▶ 코로나19 방역 과정에서 수집된 개인 건강정보가 쿠키 및 온라인 추적 기술과 결합할 경우 당초 취지와 무관하게 표적광고나 마케팅 목적으로 개인정보가 이용될 가능성도 제기
 - 사용자가 코로나19 관련 정보 사이트에 로그인한 상태에서 "질병 또는 건강 상태에 대한 세부 사항"을 검색하는 경우 명시적인 사용자 프로필을 통해 Google과 Facebook 등의 사업자들과 데이터가 공유 가능
 - 고유한 식별자에 근거한 사용자 프로파일링도 진행될 수 있으며, 그러한 데이터의 저장 및 처리에 대한 합법적인 근거가 없다는 점도 문제로 지적
 - 실제로 건강 보험 웹 사이트들이 광고 및 사용자 타겟팅을 목적으로 Google 소유의 DoubleClick이 설정한 쿠키를 포함하여 다양한 쿠키를 사용 중이라는 점에 비춰볼 때 코로나19 대응 과정에서 수집된 개인 건강 기록이 주요 기술기업들의 추적 대상이 될 수 있다는 우려 심화

(2) 건강정보에 근거한 차별과 불평등

- ▶ 코로나19 방역 과정에서 사업장 안전을 위한 고용주의 피고용인 건강정보 처리 문제가 부각되면서 고용 맥락에서 개인정보의 오남용 가능성도 간과할 수 없는 상황
 - 코로나19 확산 방지를 위한 피고용인 건강데이터 처리의 법적 근거와 관련하여, 고용주의 해당 데이터 처리는 고용주의 법적 의무 수행에 필요한 것으로 정당화
 - 사업장에서의 건강 및 안전과 관련된 고용주의 의무 또는 질병 통제 등 공익에 관한 의무를 이행하기 위해 피고용인의 개인 데이터 처리가 필요한 경우로 인정¹
 - 이와 관련, EDPB(European Data Protection Board)는 2020년 3월 19일 코로나19 확산 기간 중 개인정보 처리에 대한 공식 성명(Statement on the processing of personal data in the context of the COVID-19 outbreak)을 통해 고용주는 국내법이 허용하는 범위 내에서만 건강정보를 요구해야 한다는 점을 지적
 - 예컨대 연락처, 출석기록, CCTV 영상, 직원 건강 신고서, 공공 및 민간 시설의 로그북에서 얻은 데이터를 코로나19의 예방 및 통제 이외에 직접 마케팅, 고객 프로파일링, 기타 다양한 목적을 위해 재사용할 수 없다는 점을 강조
 - 고용주는 법적 의무에 따라 필요한 경우에만 건강 데이터에 접근하여 처리하고 코로나19 감염과 관련한 건강정보를 익명화하며 직원들을 대상으로 코로나19 감염 사례를 알리고 보호조치를 취해야하지만 필요 이상의 정보를 전달하지 않도록 제한
 - 그러나 고용주가 코로나19 감염 직원을 식별하고 감염을 이유로 인사상의 불이익이나 차별에 나설 가능성을 배제할 수 없는 상황

(3) 개인정보 유출

- ▶ 코로나19 상황에서 개인 건강정보 침해 이슈가 가장 직접적으로 나타나는 데이터 유출 사고도 이미 여러 지역에서 발생
 - 영국, 뉴질랜드, 브라질², 인도 등 세계 각지에서 코로나19 검진 결과 및 환자 관리와 관련한 데이터 유출 사태가 발생함에 따라 코로나19 관련 건강정보의 처리에 앞서 적절한 보안 조치가 필요하다는 경각심 제기

¹ https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf

² 브라질의 사례는 <2020년 하반기 해외 개인정보 유출 사례> 보고서 참조 요망

2020년 12월

- ▶ 영국에서는 2020년 2월 27일부터 2020년 8월 말까지 코로나19 양성 반응을 보인 웨일즈 주민 전체의 개인 건강정보가 유출되는 개인정보 침해 사고 발생
 - 이 사고는 2020년 8월 30일 Public Health Wales의 직원이 비즈니스 인텔리전스 소프트웨어 플랫폼에 데이터를 업로드 하는 과정에서 실수로 발생
 - Public Health Wales에 따르면, 이 직원은 내부용 서버가 공용 서버에 해당 데이터를 게시했으며 이에 따라 코로나 바이러스 양성 반응을 보인 1만 8,105명의 개인 데이터가 외부에 공개
 - 이 사고로 유출된 데이터에는 개인의 이니셜, 성별, 생년월일, 지역 관할 구역이 포함되어 있으며, 요양원 등 시설 입소자들의 경우 해당 시설의 명칭도 함께 공개
- ▶ 뉴질랜드에서는 코로나19 확진 환자의 세부 개인정보가 유출되는 사고가 발생하여 원인 규명 등을 위한 정부기관의 조사가 진행 중
 - 뉴질랜드에서 진행 중인 코로나 19 대응 사례와 관련하여, 해당 환자의 이름과 생년월일 등 기밀 정보로 분류된 세부 개인정보가 유출되었으며, 여기에는 오클랜드의 30세 여성부터 캔터베리의 70세 남성까지 총 18건의 확진 사례 포함
 - 해당 개인정보 유출 사실은 언론매체인 Weekend Herald가 취재를 통해 해당 데이터를 포함한 스프레드 시트 문서를 확인하고 보도해 알려졌으며, 이 문서에는 코로나19 확진자의 양성 반응 당시 머물렀던 지역과 격리를 위해 이동한 지역에 대한 정보도 포함
 - 실제로 여러 정부 기관 및 기타 시설에서 해당 정보에 접근할 수 있었던 것으로 알려졌으며, 민감한 개인 건강정보가 어디에서 공개되었는지는 확실하게 파악되지 않은 상황에서 뉴질랜드 보건복지위원회(The State Service Commission)가 조사에 착수
- ▶ 인도에서는 정부 서버에 안전하지 않은 상태로 저장된 8만 건 이상의 코로나19 환자의 의료 기록에 액세스했다는 해커들의 주장 제기
 - 자칭 ‘Kerala Cyber Warriors’라는 이름의 이 해커 그룹은 델리 주 보건부(Delhi State Health Mission) 웹사이트에 10분 이내에 접속하여 환자의 이름, 주소, 전화 번호, 코로나19 테스트 결과, 여권 세부 정보 등 건강 관련 데이터가 포함된 민감정보에 접근할 수 있었다고 발표
 - 이 사고는 웹 사이트의 보안 취약점을 이용해 이루어졌으며, 해커들은 해당 사이트에서

2020년 12월

여러 개의 백도어를 발견한 것은 물론 데이터 유출 후에도 웹 사이트 관리자들이 해킹 사실을 인지하지 못했다고 밝혀 파문을 야기

- Kerala Cyber Warriors는 델리의 의료 서비스 방식에 불만을 품고 개인 건강정보 관리 과정의 보안 결점을 드러내기 위해 보건부를 표적으로 삼은 것으로 알려졌으며, 이번 사례를 통해 코로나19 관련 건강정보의 유출 및 개인정보 침해 가능성에 경종

4. 시사점

- ▶ 개인의 건강정보는 가장 대표적인 민감정보이지만 코로나19의 전 세계적 확산이라는 비상상황에서 실용적인 활용 방안이 요구되며 이 과정에서 개인정보보호의 원칙과 정보주체의 기본 권리를 희생하지 않을 수 있는 균형잡힌 접근방식에 대한 고민 확산
- 전세계 주요국의 정책 당국과 개인정보보호 감독기구는 기본적인 데이터 보호 및 개인정보 보호 원칙에 대한 존중을 바탕으로 방역 일선의 요구사항을 수용하는 방식으로 대응하고 있으나, 개인정보 침해 우려를 불식하기 위해 특히 다음과 같은 노력 필요
 - 준비단계에서는 코로나19 관련 개인의 건강정보 수집 과정에서 △데이터 처리 기술에 개인정보보호 기능이 어떻게 내재되어 있는지 점검하고 △개인정보 수집 및 이용이 비례성의 원칙에 따라 계획되어 있는지 확인 필요
 - 건강정보 수집단계에서는 개인정보 수집 사실을 알리고, 명확하고 이해하기 쉬운 표현으로 개인정보보호 동의 내용을 설명하며 개인정보처리와 관련된 통지 사항 개발
 - 건강정보 처리단계에서는 비례성과 최소수집의 원칙을 준수하는 것은 물론 수집된 모든 개인 데이터는 기존 정부 지침에 의해 허용된 기간 동안만 보유하고 이후 모든 개인 데이터는 안전한 방식으로 폐기되도록 확인
- 건강정보와 같이 민감한 데이터일수록 개인정보의 추가적인 결합 및 데이터 누적에 따른 개인정보 침해 위험이 높아질 수 있다는 점에 주목하여, △데이터 활용과 데이터 보호 사이의 상충관계를 조율하는 과정에서 개인정보보호 감독기구와 면밀하게 협조하고 △투명성과 비례성의 원칙을 준수하며 △코로나19 위기 종식 즉시 개인건강정보에 대한 이용 관행을 정상화하는 것이 필요

2020년 12월

Reference

1. Bird&Bird, "Guidance available on processing personal data from Finnish Ombudsman on COVID-19", 2020.7.8
2. Consumer Reports, "New Privacy Bills Aim to Protect Health Data During the Pandemic", 2020.5.14.
3. Data.gouv, "Données relatives aux résultats des tests virologiques COVID-19 SI-DEP", 2020.10.1
4. Euractiv, "EU stands by its data privacy rules in response to COVID-19" 2020.4.28.
5. Health IT Secuirities, "Sens. Propose Bill to Regulate Privacy of COVID-19 Contact Tracing Apps", 2020.6.3.
6. ICO, "Combatting COVID-19 through data: some considerations for privacy", 2020.4.17.
7. EDPB, "Statement on the processing of personal data in the context of the COVID-19 outbreak" 2020.3.19.
8. EDPB, "Twenty-fourth Plenary session: EDPB doubles down on COVID-19 guidance in newly adopted letters", 2020.4.24.
9. NextGov, "HHS Relaxes Data Security and Privacy Enforcement For COVID-19 Test Sites", 2020.5.18
10. Public Technology, "Personal data of all Welsh coronavirus cases compromised in breach", 2020.9.15
11. Tech Crunch, "Apple adds anonymous symptom and health info sharing to its COVID-19 app and website", 2020.6.9.
12. The Daily Swig, "Indian government hack exposes 80,000 coronavirus patients' data", 2020.6.29
13. The Guardian, "Documents seen by Guardian show tech firms using information to build 'Covid-19 datastore'", 2020.4.12.



발 행 일 2020년 12월

발 행 및 편 집 한국인터넷진흥원 개인정보보호본부 개인정보정책기획팀

주 소 전라남도 나주시 진흥길 9 빛가람동 (301-2) Tel 1433-25

▶ 본 동향보고서의 내용은 한국인터넷진흥원의 공식적인 입장과는 다를 수 있습니다.

▶ 해외 개인정보보호 동향보고서의 내용은 무단 전재할 수 없으며, 인용할 경우 그 출처를 반드시 명시하여야 합니다.