해외 개인정보보호 동향 보고서

최신동향 보고서 2019년 11월 4주

KISA 한국인터넷진흥원

호주 OAIC의 '건강프라이버시 가이드라인' 주요 내용 분석

< 목 차 >

1. 배경

2. 주요 내용
(1) 가이드라인의 개요 및 특징
(2) 가이드라인의 핵심 내용

3. 시사점

1. 배경

▶ 호주의 개인정보보호 감독기구 OAIC(Office of Australian Information Commissioner)는 건강 관련 개인정보보호를 위한 종합 가이드라인(Guide to health privacy)을 발표(`19.9.6)

- OAIC에 따르면, 보건의료(헬스케어) 영역은 지난 3년 동안 접수된 개인정보 침해 신고의 비중이 가장 높은 분야 중 하나로 선정
- 2018년 2월 개인정보유출 통지 의무화 이후 유출 통지 사례가 가장 많은 분야로 꼽힐 만큼 개인정보보호에도 취약
- 따라서 보건의료분야 종사자들이 환자의 건강 관련 개인정보를 더 효과적으로 보호하기 위한 지침이 필요한 상황
- OAIC의 Angelene Falk 커미셔너는 호주 개인정보보호법(Privacy Act 1988)[1]의 적용을 받는 모든 보건의료 서비스 제공자들에게 적용되는 건강 정보보호 가이드라인을 개발하여 공개하고, 이를 통해 보건의료 분야의 개인정보보호 관행 개선을 촉구할 수 있을 것으로 기대

1 총 9장(part) 100개 조항(section) 및 1개 부칙(schedule)으로 구성되었으며, 호주 연방 정부기관 및 민간 기관이 취급하는 일반 개인정보의 수집, 이용 및 제공에 관해 규율

2. 주요 내용 및 분석

(1) 가이드라인의 개요 및 특징

▶ OAIC의 가이드라인은 보건의료 관련 종사자들이 개인정보보호 의무에 대해 정확하게 이해하고 실무 전반에 걸쳐 올바른 개인정보보호 수칙을 지킬 수 있도록 지원하는 종합 안내서로서 단계별 핵심 내용 제공

- 이 가이드라인에서 보건의료 서비스 제공자의 범주는 의사, 민간 병원, 의료 전문가부터 대체 의학 종사자, 약사, 사립학교, 보육센터, 운동시설과 체중감량 클리닉에 이르기까지 다양한 영역을 망라한 것이 특징
- 건강관련 개인정보를 처리할 수 있도록 법적 요구 사항을 충족하고, 개인 정보의 수집·이용·공개 등을 위한 동의를 획득하는 방법 등에 대해 실무적인 조언 제공
- 이를 위해 가이드라인은 ①보건의료 서비스 제공자의 개인정보보호 실천을 위해 요구되는 8가지 단계를 요약하고(가이드라인 제2장) ②보건의료 서비스 현장에서 준수해야 할 주제별 의무사항에 대해 설명(제3장~제9장)

(2) 가이드라인의 핵심 내용

▶ 보건의료 분야에서 개인정보보호 의무를 준수하고 더 안전한 개인정보보호 관리를 위해 수행해야 할 8가지 주요 단계를 다음과 같이 제시

- 1단계: 개인정보 관리 계획을 개발 및 구현하는 단계
- 2단계: 개인 정보 관리에 대한 명확한 책임 소재를 확립하는 단계
- 3단계: 보건의료 서비스 제공자가 처리하는 개인정보 유형에 대해 문서로 기록하는 단계
- 4단계: 개인정보보호 의무에 대해 이해하고 이를 충족하기 위한 프로세스를 구현하는 단계
- 5단계: 개인정보보호 의무에 대한 직원 교육을 진행하는 단계
- 6단계: 개인정보처리방침을 작성하는 단계
- 7단계: 보유한 정보를 보호하는 단계
- 8단계: 데이터 유출에 대한 대응 계획을 발전시키는 단계

▶ 보건의료 서비스 부문에서 개인정보보호 의무를 적용 및 시행하는 방법에 대해 다음과 같이 지침을 제시

- **(건강정보의 수집)** 건강정보 수집 사실을 고지하고 수집 동의를 확보하기 위해서는 다음 사항에 유의하도록 제안

- 건강정보는 정보수집이 합리적으로 반드시 필요한 경우에 한하여 정보주체의 동의 하에 수집 가능
- 건강정보는 합법적이고 공정한 수단을 통해서만 수집해야하며 일반적으로 환자를 통해 직접 정보를 수집할 것을 권고
- 건강정보 수집 시 환자에게 특정한 사안을 알려야 하는 경우, 이를 위한 합리적인 조치를 취할 것을 권고

• **(건강정보의 이용 및 공개)** 환자의 건강 정보를 이용 및 공개해야 하는 경우에 대해 다음과 같이 지침 제시

- 건강정보는 수집 목적으로만 이용 및 공개 가능
- 단, 정보주체의 동의를 획득하거나 특정한 상황에 처한 경우에는 수집 목적 이외의 다른 목적으로도 건강정보의 이용과 공개 가능

※ 특정한 상황이란 환자의 생명이 위협받는 위급한 상황이거나 합리적인 방법으로 동의를 획득할 수 없는 상황 등을 포함

• **(건강정보의 열람)** 정보주체가 자신의 건강정보에 대해 행사할 수 있는 권리를 설명하고, 정보주체의 요청사항에 대한 처리 방법 및 열람권을 거부할 수 있는 근거 등에 대한 지침 제시

- 정보주체는 예외가 적용되지 않는 한 자신의 건강정보에 대한 열람권을 행사할 수 있으며, 일반적으로 30일 이내에 환자의 열람권 요청에 대응하는 것이 원칙
- 정보주체가 요청한 방식이 비합리적이거나 실행 불가능하지 않은 한 요청된 방식 그대로 열람권을 지원
- 정보주체의 요청한 방식의 열람을 거부하거나 열람 자체를 거부하기 위해서는 다음과 같은 조건 필요
  a. 건강정보 처리자와 정보주체의 요구를 모두 충족시킬 수 있는 열람 방식을 제공하기 위해 합리적인 조치를 취할 것
  b. 열람 거부의 근거 및 열람 거부에 대한 불만을 제기할 수 있는 방법에 대해 명시한 서면 통지를 정보주체에게 제공할 것

• **(건강정보의 정정)** 건강정보의 정확성 확보를 위해 합리적인 조치를 취하고, 정보주체의 건강정보 수정 요청에 대응하며, 건강정보 정정 요구를 거부해야 할 경우 통지하도록 지침 제시

- 현재 보유 중인 건강정보의 정확성을 위해 합리적인 조치를 취해야하는 경우는 다음과 같음
  a. 정보주체가 정정 요청을 하는 경우
  b. 현재 보유 중인 건강정보가 정확하지 않다는 사실을 인지한 경우
- 일반적으로, 환자의 정정 요구를 접수한 후 30일 이내에 응답해야 하며, 정정 요구를 거부하는 경우 정보주체에게 통지 필요

- **(건강관리활동)** “건강관리활동(health management activities)”의 정의 및 건강관리활동에 필요한 건강정보를 수집·이용·공개하는 방법에 대한 지침 제시
  - '건강관리활동'에는 일반적인 건강관리 서비스를 위해 합리적으로 필요한 모든 활동이 포함될 수 있으며, 호주 개인정보보호법은 '건강관리활동'을 건강 관련 서비스를 위한 관리, 자금조달, 모니터링 업무를 포괄하는 것으로 정의
  - 건강정보 수집을 위해서는 원칙적으로 정보주체의 동의가 필요하지만, 건강관리활동에 필요한 경우 동의 없이 건강정보 수집 가능
  - 건강관리활동을 위해 건강정보를 이용 및 공개하는 경우에는 일반적인 건강정보 이용 및 공개 원칙에 따르되, 동의 없이 건강정보를 이용 및 공개하기 위해서는 비식별화 조치 필요
- **(동의 능력이 상실된 정보주체의 건강정보 공개)** 동의가 불가능한 정보주체의 건강정보를 공개할 수 있는 경우와 대상에 대한 지침 제시
  - 동의 능력이 없는 환자에게 적절한 치료를 제공하기 위해 필요한 경우에는 환자의 건강정보를 '책임자'에게 공개하는 것이 가능
  - 단, 적절한 치료나 간호 또는 구호의 목적으로 건강정보를 공개하는 경우에도 공개되는 정보의 양은 해당 목적을 달성하기 위해 필요한 수준으로만 제한
  - 정보주체가 동의 능력을 상실하기 전이나 의사소통이 불가능해지기 전 명시적으로 표시한 의사에 위배되지 않는 수준에서 건강정보를 공개
- **(유전자 정보의 이용 및 공개)** 유전자 정보의 이용 및 공개와 관련하여 구체적인 상황과 방식, 동의 요건 등에 대한 지침 제공
  - 환자의 건강이나 안전에 대한 심각한 위협을 줄이거나 예방하기 위해 필요하다고 판단되는 경우 정보주체의 동의 없이 유전자 정보의 이용 및 공개 가능
  - 유전자 정보의 이용 및 공개를 위해서는 OAIC의 승인을 받은 호주 개인정보보호법 섹션 95AA의 가이드라인[2]을 따르도록 권고
- **(연구와 통계처리)** 공중보건 또는 공공의 안전과 관련된 통계 분석이나 연구 목적의 건강정보 수집·이용·공개가 가능한 조건과 동의 관련 이슈에 대한 지침 제공
  - 호주 개인정보보호법에 의해 요구되거나, 책임 있는 의료기관의 규칙에 부합하거나, 호주 개인정보보호법 섹션 95AA의 가이드라인에 따르는 경우에는 정보주체의 동의 없이 건강정보의 수집·이용·공개 가능
  - 공중보건 또는 공공의 안전과 관련이 있는 연구 또는 통계 조사와 분석이 되기 위해서는 그 결과물이 공중보건 또는 공공 안전에 영향을 미치거나 정보를 제공해야 함

2 https://www.legislation.gov.au/Details/F2014L00244

3. 시사점

▶ 이 가이드라인은 OAIC가 의료 서비스 기관 등의 개인 건강정보보호 문제를 진지하고 심각하게 받아들이고 있음을 시사

- 보건의료 분야의 개인정보 침해 우려를 완화하기 위해 △건강정보에 대한 적절한 동의 획득 방법 △비식별 조치 등을 통한 안전한 이용 방법 △제3자에 대한 합법적인 건강정보 공개 방법 등을 제시
- 특히 보건의료 분야의 실무 단계별로 개인정보보호 의무에 대한 정확한 이해와 수행을 통해 개인정보 침해 가능성을 줄이고 건강정보 처리 관행에 대한 신뢰도를 높일 수 있을 것으로 기대
- OAIC의 이러한 접근 방식은 미국의 소비자기술협회(Consumer Technology Association, CTA)가 제시한 개인정보보호 가이드라인(GUIDING PRINCIPLES FOR THE PRIVACY OF PERSONAL HEALTH AND WELLNESS INFORMATION)과 마찬가지로 개인 건강정보 처리 기술의 안전성과 신뢰성 강화에 기여
- CTA의 가이드라인이 업계의 자율규제용 지침인 반면 OAIC는 개인정보보호 감독기구의 가이드라인이라는 점에서 차이가 있으나 △수집하는 개인 건강정보의 종류와 수집 이유에 대한 투명한 공개 △건강정보에 대한 정보주체의 자기결정권 강화 △효과적인 동의 관리와 건강정보의 이용을 위한 수단 제안이라는 측면에서 공통점을 가진 것으로 분석

Reference

1. Millsoakley.com, New Privacy Guide Released for Health Service Providers, 2019.10월
2. Healthcare IT News, "Consumer Technology Association publishes new health data privacy guidelines“, 2019.9.12.
3. OAIC, "Guide to health privacy", 2019.9.6.
4. OAIC, "New guide released to help health sector improve privacy practice", 2019.10.18

KISA 한국인터넷진흥원

발 행 일 2019년 11월
발 행 및 편 집 한국인터넷진흥원 개인정보보호본부 개인정보정책기획팀
주 소 전라남도 나주시 진흥길 9 빛가람동 (301-2) Tel 1544-5118