

# 의료기관 개인건강정보의 이차적 이용

김 장 한\*

- I. 문제의 제기
- II. 의료기관 개인정보의 헌법적 의미
- III. 의료 정보 이용 입법 예
- IV. 의료 정보의 이차적 이용과 관련된 몇 가지 문제 사례들
  - 1. “소득세법” 상의 연말정산 간소화 조치
  - 2. 혈액관리법상의 정보 제공 조항
  - 3. 연구, 교육 등 공공 목적에 이용하려 하지만 이를 허용하는 개별 법률 규정이 없는 경우
- V. 검 토
  - 1. 정보 수집의 문제
  - 2. 최소 침해 가능한 다른 방법은 없는가?
- VI. 결 론

## I. 문제의 제기

1. 현대사회에 있어서 정보는 대규모 데이터베이스를 통하여 정보은행이 되고 막대한 부가 가치를 창출할 수 있는 재료가 되었다. 정보의 이용을 통하여 우리 사회가 원하는 적절한 가치를 창출할 수 있다. 예컨대 시판 허가 되어 유통되는 약물의 부작용은 집적된 진료 정보를 이용하면 쉽게 찾아 낼 수 있다. 그러므로 공공의 이익을 위하여 의료 정보를 이용하고자하는 수요는 점차 증가하고 있다. 또한 인터넷을 통한 정보 교환이 수월해지면서 원치 않게 자신의 정보가 사고 팔리는 것들을 목격하게 된다. 정보가 디지

\* 논문접수: 2010. 2. 13. \* 심사개시: 2010. 5. 10. \* 게재확정: 2010. 6. 10.

\* 울산대학교 의과대학 인문사회의학교실 교수

털화되면 생성과 동시에 집적된다. 정보 수집 과정에서 개인 터미널에서 생성되는 정보들이 네트워크를 통하여 중앙 전산 장치에 집적됨으로써 별도로 정보를 가공하여 데이터베이스화 하는 작업을 수행하지 않아도 된다. 또한 집적된 대규모 정보의 관리와 전달이 매우 신속하게 진행되며, 그 과정에서 정보의 손실은 극소화된다. 또한 컴퓨터를 통하여 집적된 대규모 정보들이 매우 빠른 속도로 이동하게 된다. 그로 인하여 정보 보관 및 유통 과정에서 발생할 수 있는 정보 누설의 가능성에 대한 문제가 나타난다. 데이터베이스의 운용과 인터넷을 통한 접근하는 것이 가능해지면서, 정보의 불법 이전에 대한 상시적 보안 문제가 발생한다. 개인이 누구라도 마음만 먹으면 손쉽게 대규모의 정보를 수집하고 관리할 수 있게 되므로 우리가 과거에 생각할 수 없었던 큰 규모의 폐해와 다양한 형태의 부작용이 나타날 수 있다. 이러한 정보의 집중은 필연적으로 정보의 독점을 가져오게 된다. 정부는 개인 정보의 비밀을 보호하여야 한다는 이유로 사회단체나 개인에게 정보를 공개하지 않으면서, 공공기관들 상호간에는 자유롭게 정보를 수집하고 행정상의 목적을 위하여 그 정보를 교환한다면 정부가 ‘빅브라더(big brother)’가 되는 것이다. 모든 정보는 비밀로 보관되어야만 하는 것은 아니다. 연구 기관이 공공복리를 위하여 정보를 생성하고 수집한 이후에 이를 공공의 목적을 위하여 사용하지 아니하고 이를 기관의 이익을 위하여 비밀로 운영한다면 이것은 다른 측면의 사회악이 될 수 있다. 디지털 시대에서 발생할 수 있는 위험을 인정하면서도 개인 사생활의 비밀 보호와 정보의 이용 문제는 이익과 해악이 공존하는 이익 형량의 문제로 볼 수밖에 없다.

2. 진료 정보의 수집과 이용은 의사가 의료 기관에 내원한 환자를 치료하기 위한 가장 기본적인 과정이다. 이것을 병력의 청취(history taking)이라고 한다. 환자가 치료를 받기 위하여 의료 기관에 방문하였다면 자신의 병력에 대하여 의사에게 이야기 해주고, 의사는 치료를 위하여 이를 기록하는 것은 당연한 과정이다. 의료기관은 진료와 관련되어 환자들의 민감한

정보가 수집, 저장, 활용되는 곳이다. 의료정보에는 성명, 주소, 주민등록번호, 전화번호 등과 같은 개인 식별 정보와 환자의 진료, 검사 결과 등이 결합하여 존재하므로 의료기관의 개인 정보는 인터넷상의 개인정보보다는 개인의 프라이버시에 더 중요한 내용을 가지고 있다. 우리나라의 국민건강보험은 의료보험의 원활한 작동을 위하여 필요한 정보의 집적과 이동을 원활하게 하기 위하여 의료정보의 디지털화를 추진하고 있다. 대표적인 것이 전자의무기록(Electric Medical Record, EMR)인데, 이를 통하여 종이 없는 병원을 가능하게 된다. 현재 대형 병원들은 수집된 개인 정보를 디지털화하고 있으며, 컴퓨터를 이용하여 진료의 효율을 높이고 있다. 물론 우리나라 모든 병의원들이 전자의무기록을 전면적으로 채택하기는 어려움이 있을 것이다. 하지만 이러한 기술의 발달은 의료기관의 개인 프라이버시 보호 역할에 새로운 과제를 던져주고 있다. 인터넷을 포함한 전산망과 전산 장비에 대한 보안의무가 그것이다. 개인의 프라이버시(privacy)를 보호하기 위하여 기술적인 측면에서 보안(security)이 전제가 되어야 한다. 프라이버시 보호와 보안은 논리적으로 밀접한 관계가 있지만, 프라이버시 보호는 문서에 정보를 기록하는 방식과 전산 장치를 이용하여 전자적인 방식으로 정보를 기록하는 방식을 모두 포함하기 때문에, 정보를 담고 있는 전산 기기와 이를 둘러싼 물리적, 전자적 환경에 대한 안전성을 추구하는 보안과는 달리 정보의 내용을 어떻게 수집, 이용, 정정, 삭제 하여야 하는가에 관한 관리적 내용을 주된 관심사로 한다.

3. 사생활의 비밀 보호 및 자유권에 기하여 의료 정보를 보는 시각은 정보의 수집과 이용을 가능한 억제하여 개인의 사생활을 보호하려는 주의와 이왕에 모아진 정보를 적절한 통제 하에 가능한 이용하려는 주의로 구별할 수 있다<sup>1)</sup>. 보호주의의 입장은 환자의 동의를 정보 이용에 대한 기초적인 근거로 본다. 의료 정보에 대한 보호는 정보 주체인 환자의 동의에 의하여

---

1) 전자를 개인정보보호에 주안점을 둔 보호주의라 하고, 후자를 정보의 이용에 주안점을 둔 이용주의라 한다.

형법상의 업무상 비밀 누설죄의 구성요건을 조각한다. 환자의 질병과 관계 없는 공익적인 목적을 위하여 동의를 추정하는 것은 극히 조심하여야 하며, 자신의 일이라고 하여 질병과 관계없는 일에 정보를 사용하는 것 역시 그 동의를 추정하는 것은 매우 조심스러워야 한다. 또한 보험급여를 위한 것 이면, 이를 위해서만 사용하여야 하고, 수집 이후 일정한 기간이 지나면 폐기하여야 한다고 주장한다. 이용주의는 적절한 보안 장치를 통하여 개인에게 미치는 영향을 최소화하면서 정보를 이용할 것을 주장한다. 적절한 보안 장치로는 ① 익명화, ② 디지털화된 정보에 대한 하드웨어적 정보 보호 장치의 요구이다. 아직 우리나라는 의료기관의 개인정보에 관하여 보호와 보안의 내용을 모두 담고 있는 특별법이 제정되지 않고 있다. 기존의 보건 의료기본법, 의료법 등의 개별 행정법은 일반적으로 개인의 프라이버시 보호에 관한 접근을 하고 있으며, 그 내용은 문서를 위주로 한 것으로서 컴퓨터를 이용한 전자 정보에 적합하게 만들어 진 것은 아니다. 이러한 입법의 미비를 해결하기 위하여 정보통신망이용촉진및정보보호등에관한법률(이하 정통망법)은 의료기관을 정보통신서비스 제공자에 준하여 취급하고 있는데, 도리어 준용규정이 의료기관 실무와 맞지 않아서 혼란만 일으키고 있다. 진료 정보의 이차적 이용은 기록열람, 사본발부, 의료인의 신고의무 등과 관련되는데, 의료기관의 개인정보는 정보 주체의 헌법상의 기본권으로서 제10조에 근거를 둔 일반적 인격권과 제17조 사생활의 비밀과 자유와 관련된 자기정보통제권, 형법 제317조(업무상비밀누설)에 의한 처벌, 공공기관의개인정보보호에관한법률, 보건의료기본법, 의료법, 정통망법 등에 의하여 규율된다. 본 논문에서는 의료기관에서 이루어지는 진료 정보의 기록 열람과 같은 정보의 이차적 이용에서 개인의 프라이버시를 지키기 위하여 현재의 적용 가능한 규정은 무엇이며, 정보 주체의 자기 정보통제권을 어떠한 방법으로, 어느 정도까지 보호할 것인가라는 문제를 몇 가지 사례를 들어 논하고자 한다.

## II. 의료기관 개인정보의 헌법적 의미

1. 사생활 비밀의 불가침은 사생활의 비공개를 보호하는 권리로서 사생활에 대한 비밀을 침해하는 행위를 막고자 것이다. 헌법 제17조의 '사생활의 비밀과 자유' 규정에 의하면 '모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다.'라고 규정하고 있다. 영미법상의 프라이버시권(privacy right)과 내용적으로 유사하지만, 구체적인 권리의 내용은 기본권이 발달되어 오면서 조금씩 차이를 보이고 있다. 사생활의 자유의 구체적 내용은 ① 사생활의 비밀을 공개 당하지 아니할 권리, ② 사생활의 자유로운 형성과 전개를 방해 받지 아니할 권리, ③ 자신의 정보를 스스로 통제할 권리로 분류할 수 있다. 일반적으로 인격권, 프라이버시권 그리고 사생활의 자유권 순서로 그 범위가 좁아진다고 본다. 사생활의 자유에 대한 기본권 내용은 과거에는 홀로 있을 자유라는 소극적인 권리로서 기능하였다. 그러나 현대에는 자기 정보통제권을 포함함으로써 적극적인 권리로 변화되었다. 자기정보통제권은 일반적으로 헌법상의 기본권으로서 제10조 제1문에서 도출되는 일반적 인격권 및 제17조의 사생활의 비밀과 자유에 의하여 보장된다. 권리 주체에는 외국인을 포함한 자연인 포함되며, 죽은 자, 법인은 원칙적으로 포함되지 않는다고 본다. 그러나 죽은 자의 사생활 비밀 침해가 죽은 자와 관계있는 생존자의 권리를 침해할 경우에는 생존자에 대하여 문제가 된다.

2. 사생활의 자유를 보호하기 위한 가장 기초적 전제 조건은 정보의 주체가 사생활의 주체인 본인이 되어야 한다는 것이다. 특히 공공 기간이 개인의 동의를 얻지 아니하고 누군가의 정보를 모은다는 것은 그 자체가 불법으로 볼 여지가 있다. 판례로는 '자료 수집 및 관리가 본인들로부터 전혀 동의를 얻지 않은 채 극히 비밀리에 이루어 졌고, 합리적이고 분명한 목적하에 필요한 최소한도로 자료가 수집된 것이 아니라, 시간적 지속성을 가진 채 일반적으로 수집이 금지된 사상, 신조 등을 포함한 개인에 대한 포괄적인

수집이 있었고, …(서울지법 91가합49346)’라는 국군보안 사령부 민간인 사찰 사건이 있다. 개인정보법 제4조에 의하면 “공공기관의 장은 사상, 신조 등 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인 정보를 수집하여서는 아니 된다. 다만 정보 주체의 동의가 있거나 다른 법률에 수집 대상 개인 정보가 명시되어 있는 경우에는 그러하지 아니하다.”라고 규정하고 있다. 다른 법률에 수집 대상 개인 정보를 명시할 경우에 적법성이 담보되었다고 보는데, 의료 정보에 관한 입법으로는 암등록법 등을 들 수 있다.

3. 우리 헌법이 인정하고 있는 기본권 제한 원리인 헌법 제37조 제2항의 일반유보에 의하면 ‘국민의 모든 자유와 권리는 국가안전보장, 질서유지 또는 공공복리를 위하여 필요한 경우에 한하여 법률로써 이를 제한 할 수 있으며, 제한하는 경우에도 자유와 권리의 본질적인 내용을 침해할 수 없다.’고 하고 있다. 국가 안전보장이나 사회 질서를 위한 기본권의 제한으로서 국가 안보나 범죄의 방지를 위하여 테러리스트나 범죄자들에 대한 유전자 은행을 설립하여 운영하는 것들이 있다. 미국에서 2001.9.11 사건이 발생한 이후 이러한 분야에 대한 프라이버시권 보호의 주장은 많은 후퇴를 하여야 했다. 우리나라 연쇄 성범죄, 미성년자 대상 성범죄가 발생할 경우에 이러한 주장이 많이 나타나고 있다. 의료 정보와 관련된 개인정보 역시 공공복리의 사유에 의한 제한이 가장 가능하다. 공공복리의 개념은 여러 견해가 있지만, 일반적으로는 공동으로 사회생활을 영위하는 사회구성원 전체를 위한 공공적 이익을 의미한다. 공공복리는 원래 적극적인 복지 향상을 의미하기 때문에, 이를 적극적으로 해석한다면 그 범위를 제한하기가 어려워지기 때문에 기본권이 쉽게 그리고 광범위하게 침해받을 우려가 있다. 헌법상의 기본권 제한 원리는 과잉금지원칙이라고 하는데, 그 내용으로는 목적의 정당성, 방법의 적정성, 피해의 최소성 및 좁은 의미의 비례 원칙으로서 법의 균형성을 요구하고 있다. 또한 공공복리를 위하여 개인 신상 정보가 포함된 의료 정보를 이용하는 것은 좀 더 허용 요건을 엄격하게 볼 필요가 있다. 이론적으로 논의의 여지가 있겠지만, 경제적 자유권에 비하여

정치적, 문화적 자유권에 대한 제한에는 그 요건에 대하여 엄격한 증명을 필요로 한다는 “이중기준의 원칙”이 적용될 수 있을 것이다.

4. 사생활의 비밀을 이루는 개인 정보는 다양한 형태와 내용을 가진다. 성명, 생년월일, 졸업일자를 교육정보시스템(NEIS)에 보유하는 행위가 개인정보자기결정권을 침해한 것인지를 판단한 현재결정<sup>2)</sup> 내용 중에 “일반적으로 볼 때, 종교적 신조, 육체적, 정신적 결함, 성생활에 대한 정보와 같이 인간의 존엄성이나 인격의 내적 핵심, 내밀한 사적 영역에 근접하는 민감한 개인정보들에 대하여는 그 제한의 허용성이 엄격히 검증되어야 할 것이다. 반면 성명, 직명과 같이 인간이 공동체에서 어울려 살아가는 한 다른 사람들과의 사이에서 식별되고 전달되는 것이 필요한 기초 정보들도 있다. 이러한 정보들은 다른 위협스러운 정보에 접근하기 위한 식별자 역할을 하거나, 다른 개인 정보들과 결합함으로써 개인의 전체적, 부분적 인격상을 추출해 내는데 사용되지 않는 한 그 자체로 언제나 엄격한 보호의 대상이 된다고 하기 어렵다.”고 하고 있다.

5. 의료정보는 일반적으로 공개를 목적으로 생성되는 것이 아니고, 환자의 정신과 신체에 관련된 극히 개인적인 사항을 담고 있다는 점에서 현행법 상으로도 일반적인 개인 정보와는 다른 특별한 보호를 하고 있다. 특별한 보호는 기존 법률 규정을 살펴보면 알 수 있는데, 형법에 의하여 업무상 비밀누설죄(형법 제317조)를 처벌하고 있고, ‘의료인은 의료법 또는 다른 법령에서 특히 규정된 경우를 제외하고는 그 의료·조산 또는 간호에 있어서 지득한 타인의 비밀을 누설하거나 발표하지 못한다(의료법 제19조).’라고 하여 의료인이 직무상 취득한 의료 정보를 누설하는 것을 처벌하고 있다. 더 나아가 ‘의료기관은 의료법 제21조 제2항 단서 규정에 따라 환자 외의 자에 제공하는 의무기록 및 진료 기록 등에 유전정보를 포함시켜서는 아니 된다. 다만 해당 환자와 동일한 질병의 진단 및 치료를 목적으로 다른 의료

2) 현재 2005.7.21. 2003헌마282 등.

기관의 요청이 있고, 개인 정보의 보호에 관한 조치를 한 경우는 그러하지 아니하다(생명윤리법 제35조).’라고 하여 유전 정보에 대한 특별한 보호를 규정하고 있다.

### III. 의료 정보 이용 입법 예

1. 개인 정보 보호에 관한 기본 원칙 및 입법은 여러 국제 조직 및 각 나라 별로 다양하게 이루어져 왔다<sup>3)</sup>. 전 세계적인 개인정보보호에 관한 입법 모델은 정부 주도에 의한 일원적, 포괄적 입법모델인 유럽형과 이원적 부문별 입법모델인 미국형으로 구분되는데, 공공부문과 민간 부문을 구분하여 규율하고 있는데, 우리나라는 후자의 입장에서 규율하고 있다<sup>4)</sup>. 대표적으로 공공부분에 대하여는 ‘공공기관의 개인 정보 보호에 관한 법률’이 있다. 이 법은 공공기관의 컴퓨터에 의하여 처리되는 개인정보의 보호, 취급(제1조)하기 위하여 제정되었으며, 다른 법률과의 관계(제3조)에서 ‘②공공기관의 컴퓨터에 의하여 처리되는 개인정보 중 통계법에 의하여 수집되는 개인정보와 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보의 보호에 관하여는 이 법을 적용하지 아니한다.’라고 하여 공공기관에 대하여 일반적으로 적용된다. 이 법에서 예정하고 있는 예외 상황은 통계법에 의하여 수집되는 개인 정보와 국가안전보장과 관련된 정보 분석이 있다. 또한 암통계 사업이 의료 정보에 관하여 통계법의 적용을 받는 것도 이에 해당한다<sup>5)</sup>. 민간 부문에 대한 일반적인 개인정보 보호

3) 1980년대 OECD 가이드라인, 유럽이사회 협약, 1990년대 UN 가이드라인, EU 개인정보 보호지침 등과 각국의 입법 및 자율 규제 규범들.

4) 이인호, “미국의 개인정보보호법제 대한 분석과 시사”, 『법학논문집』, 제29집 제1호, 중앙대학교법학연구소, 2005, 제193~217면.

5) 정부는 암관리를 위하여 암관리법을 제정하고 이에 근거하여 여러 사업을 벌이고 있는데, 암등록통계사업(제8조)은 ‘① 보건복지부장관은 암 발생에 관한 자료를 지속적으로 체계적으로 수집·분석하여 통계를 산출하는 사업을 실시하여야 한다. 이 경우 통계자료



규정, 특히 의료 정보에 대하여는 건강정보보호및관리·운영에관한법률(2006.10. 24 입법 예고), ‘개인진료정보보호법안’(한나라당 정형근 의원안), ‘건강정보보호법안’(열린우리당 윤호중 의원안) 등에서 의료 정보에 대한 일반적인 사항을 규율하려는 시도가 있었고, 정보통신망이용촉진및정보보호등에관한법률에서 인터넷 등을 이용한 정보 이용을 규율하고 있다.

2. 의료 정보 이용 및 보호에 대한 미국의 민간 입법례로는 1966년에 제정된 미연방의 건강보험양도 및 책임에 관한 법률(The Health Insurance Portability and Accountability Act, HIPAA)이다. 전자건강기록(Electronic Health Record, EHR)에 대한 개인정보 보호를 규정한 연방 법률로서 본래 개인 및 단체 건강보험의 이전과 연속성을 개선할 목적으로 마련되었으나, 건강보험 관리 절차 간소화로 범위가 확대되었다. 관리 절차 간소화 부분에서는 트랜잭션 및 코드 집합, 식별자, 보안, 개인정보보호, 기간, 벌금 등을 규정하고 있으며, 개인 식별이 가능한 정보를 불법적으로 노출시킬 경우에는 건당 1만~2만5천 달러 벌금과 고의 범죄의 경우는 25만 달러 벌금이나 10년 이하의 징역을 처하도록 하고 있다. 제정 당시 이 법은 프라이버시에 대한 규정을 직접 담지는 못하였고, 위임 규정에 의하여 보건복지부 장관(Secretary of Health and Human Services)이 1999년 11월 3일 프라이버시 규칙(Privacy rule)을 공표하였다<sup>6)</sup>.

---

의 수집 및 통계의 작성 등에 관하여는 「통계법」을 준용하되, 통계의 산출을 위하여 처리되는 개인정보는 「공공기관의개인정보보호에관한법률」 제3조 제2항의 규정에 따라 동법이 적용되지 아니하는 개인정보로 본다.’라고 하고 있다.’

6) 2002년 부시 행정부가 개정. 45C.F.R. parts 160~164에 편입됨.

## IV. 의료 정보의 이차적 이용과 관련된 몇 가지 문제 사례들

### 1. “소득세법” 상의 연말정산 간소화 조치

2005년 소득세법(법률 제7837호) 개정에 의하여 소득세법 제165조 제1항(소득공제증빙서류의 제출 및 행정지도) “이 법 또는 「조세특례제한법」의 규정에 따른 소득공제 중 대통령령이 정하는 소득공제를 받기 위하여 필요한 증빙서류(이하 “소득공제증빙서류”라 한다)를 발급하는 자는 정보통신망의 활용 등 대통령령이 정하는 바에 따라 국세청장에게 소득공제증빙서류를 제출하여야 한다. 다만, 소득공제증빙서류를 발급받는 자가 서류의 제출을 거부하는 등 대통령령이 정하는 경우에는 그러하지 아니하다.” 제4항 “국세청장은 소득공제증빙서류를 발급하는 자에 대하여 소득공제증빙서류를 국세청장에게 제출하도록 지도할 수 있다.”를 도입하였고, 이 규정에 의하여 대통령령 제216조의3(소득공제 증빙서류의 제출 및 행정지도) 제1항 제3호 “법 제52조(특별 공제) 제1항 제3호 및 「조세특례제한법」 제122조의3에 따른 의료비. 다만, 제110조 제1항 제3호 내지 제5호의 의료비를 제외한다.”에 의하여 의료기관은 자료집중기관으로 지정된 국민건강보험공단에 수진자의 의료비 내역에 대하여 자료를 제출하여야 한다.

의료계는 2006년 12월26일 소득세법 165조에 대하여 위헌소원심판을 제기하였다. 헌법재판소는 2008. 10. 30일 헌법재판소 전원재판부 2006헌마 1409 결정 재판관 8(기각)대 1(각하)의 의견으로 기각 결정했다. 청구 이유 중에서 중요한 것은 환자의 동의 없이 의료기관으로 하여금 진료기록을 제출하도록 하는 것은 환자들인 청구인들의 개인정보자기결정권을 침해한다는 주장이었고, 이에 대한 헌법재판소의 기각 결정 요지는 “국세청장에게 제출되는 내용은, 환자의 민감한 정보가 아니고, 과세관청이 소득세 공제액을 산정하기 위한 필요최소한의 내용이며, 이 사건 법령조항으로 연계되는 납세자의 편의와 사회적 제비용의 절감을 위한 연말정산 간소화라는

공익이 이로 인하여 제한되는 의사들의 양심실현의 자유에 비하여 결코 적다고 할 수 없으므로, 이 사건 법령조항은 피해의 최소성 원칙과 법익의 균형성도 충족하고 있다. 따라서 이 사건 법령조항은 헌법에 위반되지 아니한다.”는 것이었다. 각하 의견으로는 “의료비에 관한 내용 중 ‘의료기관 등의 사업자등록번호, 환자의 성명·주민등록번호, 납부일자·납부금액’을 제출하도록 규정하고 있는 『연말정산 간소화를 위한 의료비 소득공제자료 제출요령』에 의하여 비로소 청구인들의 기본권이 직접 침해되거나 침해될 위험성이 있게 된다고 할 것이다.”라고 하고 있다.

현재 결정 당시 의료법(법률 제9135호)에 의하면 “환자, 환자 배우자 등이 신청하는 경우 또는 환자 치료를 위하여 의료기관이 요청하는 경우 외에 제3자의 기록 열람 등은 의료법이나 다른 법령에 따로 규정된 경우에 한하여 인정하였다(의료법 제21조 제1항 본문).” 다른 법령에 따로 규정된 경우가 과연 무엇인가에 대하여 견해의 대립이 있었다. 형사소송법에 의하여 영장을 받은 경우에 의료기관이 기록 열람을 하는 것은 인정되지만, 교통사고에서 보험 처리를 위하여, 수사상 필요에 의하여 경찰관집무집행법에 기하여 기록 열람을 요구하는 경우와 같이 다른 법령에 따로 규정한 경우를 확정하는 어려움이 있었다. 그 이후에 의료법이 개정되고 기록 열람이 가능한 법률을 한정적으로 열거하게 된다. 의료법(법률 제9906호)은 “환자가 아닌 다른 사람에게 환자에 관한 기록을 열람하게 하거나 그 사본을 내주는 등 내용을 확인할 수 있게 하여서는 아니 된다(제21조 제1항).”, “제1항에도 불구하고 의료인이나 의료기관 종사자는 다음 각 호의 어느 하나에 해당하면 그 기록을 열람하게 하거나 그 사본을 교부하는 등 그 내용을 확인할 수 있게 하여야 한다. 다만, 의사·치과의사 또는 한의사가 환자의 진료를 위하여 불가피하다고 인정한 경우에는 그러하지 아니하다(동법 제21조 제2항).”라고 하여 “1. 환자의 배우자, 직계 존속·비속 또는 배우자의 직계 존속이 환자 본인의 동의서와 친족관계임을 나타내는 증명서 등을 첨부하는 등 보건복지가족부령으로 정하는 요건을 갖추어 요청한 경우, 2. 환자가 지

정하는 대리인이 환자 본인의 동의서와 대리권이 있음을 증명하는 서류를 첨부하는 등 보건복지가족부령으로 정하는 요건을 갖추어 요청한 경우, 3. 환자가 사망하거나 의식이 없는 등 환자의 동의를 받을 수 없어 환자의 배우자, 직계 존속·비속 또는 배우자의 직계 존속이 친족관계임을 나타내는 증명서 등을 첨부하는 등 보건복지가족부령으로 정하는 요건을 갖추어 요청한 경우”를 인정하고 그 외 법률에 의한 기록열람 사유로서 “「국민건강보험법」, 「의료급여법」, 「형사소송법」, 「민사소송법」, 「산업재해보상보험법」, 「자동차손해배상보장법」, 「병역법」, 「학교안전사고 예방 및 보상에 관한 법률」, 「고엽제후유의증 환자지원 등에 관한 법률」에 한하여 제3자의 기록 열람 등을 인정하고 있다.

개정 이유를 살펴보면 다음과 같다.

환자에 관한 기록의 열람제한(법 제21조)

1) 환자의 기록정보는 가장 엄밀하게 보호되어야 할 개인정보임에도 현행 「의료법」은 환자진료기록의 열람·사본 교부 등 내용확인을 요구하는 자의 범위가 환자 본인 외에도 환자의 배우자, 직계 존속·비속으로 광범위하고, 「의료법」 외의 다른 법령에 의한 경우에도 가능하여 엄격히 보호되어야 할 환자의 진료관련 정보가 환자 본인의 동의 없이 누출될 우려가 있음.

2) 환자 본인이 아닌 경우 환자진료기록 열람을 엄격히 제한하고, 「형사소송법」·「민사소송법」 등 이 법에서 열거한 법률에 열람근거가 있는 경우에만 환자기록의 열람 및 사본 교부가 가능하도록 함.

## 2. 혈액관리법상의 정보 제공 조항

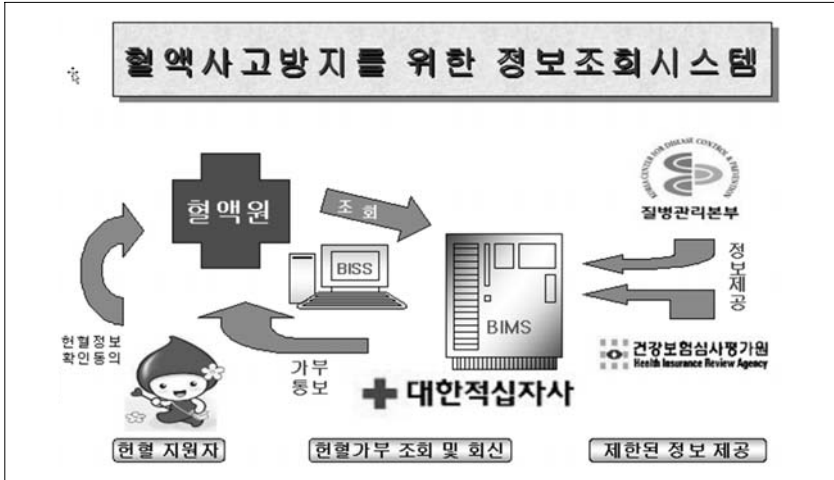
2006년 국정감사자료에 의하면, 대한적십자사가 건선치료약물인 ‘아시트레닌’을 처방받은 환자(약 25만 명)의 헌혈기록을 조회한 결과, 1,285명이 2,679회 헌혈하여 3,927 유니트의 혈액이 수혈용으로 출고된 사실이 확인되었다<sup>7)</sup>. 이에 따라 보건복지부는 건선치료제(제품명: Neotigason<sup>®</sup>) 투

여자에 대해 헌혈 및 임신 금지를 주지하여 줄 것을 의료 기관과 약국에 통보하였다. 아시트레틴 성분의 건선 치료제를 투여 받은 자가 헌혈한 혈액의 안전성이 문제가 제기되었는데, 주요 국가에서는 투약 후 일정기간(복용 중단 후 최소 2년간) 임신과 헌혈(복용 중단 후 1년 또는 3년)을 금지하고 있다는 이유였다. 하지만 임신초기 약물복용자에서는 태아기형이 발생한 사례보고가 있으나, 헌혈혈액을 통한 기형발생은 전 세계적으로 보고된 바는 없는 약물이다. 당시 대한적십자사는 2006.8.17.에 건선치료제를 처방받은 환자의 헌혈혈액재고를 출고금지, 분획용 혈장은 제조공정투입을 중지시켰다. 또한 헌혈금지약물에 대한 문진을 강화하도록 일선 혈액원에 지시하였으며, 현재 건선치료제를 처방받은 헌혈자에 대한 문진과정 중 오류가 있었는지에 대한 자체조사를 진행 중이라고 밝혔다. 혈액관리법 시행규칙이 '07.9.7. 개정되면서 헌혈금지약물 복용자가 채혈금지대상자로 지정되었지만(보건복지부령 제387호, 별표 3), 혈액관리법 개정 작업이 늦어지면서 개인의 진료 정보에 대하여 이를 확인할 수 있는 방법이 없었다<sup>8)</sup>. 2009년 혈액관리법(제9387호) 개정에 의하여 제7조 “(헌혈자의 신원확인·건강진단 등) ① 혈액원은 보건복지가족부령으로 정하는 바에 따라 채혈 전에 헌혈자에 대하여 신원확인 및 건강진단을 실시하여야 한다. ② 혈액원은 보건복지가족부령이 정하는 전염병환자 및 건강기준에 미달하는 자로부터 채혈하여서는 아니 된다. ③ 혈액원은 신원이 확실하지 아니하거나 신원확인에 필요한 요구에 응하지 아니하는 자로부터 채혈하여서는 아니 된다. ④ 보건복지가족부장관은 혈액제제의 안전성을 확보하기 위하여 필요하다고 인정하는 때에는 관계 중앙행정기관의 장 또는 공공기관의 장으로 하여금 전염병환자 또는 약물복용환자 등의 관련 정보를 혈액원 등에 제공하도록

7) 보건복지부, “헌혈금지약물에 대한 혈액관리강화대책 추진”, 보도자료, 2006, 9.6.

8) 2008년 혈액관리법(법률 제8852호) 제7조 “(헌혈자의 건강진단 등) ① 혈액원은 보건복지가족부령이 정하는 바에 의하여 채혈 전에 헌혈자에 대하여 건강진단을 실시하여야 한다. ② 혈액원은 보건복지가족부령이 정하는 전염병환자 및 건강기준에 미달하는 자로부터 채혈하여서는 아니 된다”.

〈그림 4-1〉 혈액관리법에 의한 정보조회시스템



요청할 수 있다. 이 경우 관계 중앙행정기관의 장 또는 공공기관의 장은 정당한 사유가 없는 한 이에 응하여야 한다. ⑤ 혈액원은 보건복지가족부령으로 정하는 바에 따라 헌혈자로부터 채혈하기 전에 채혈금지대상 여부 및 과거 헌혈경력과 그 검사결과를 조회하여야 한다. 다만, 천재지변, 긴급수혈 등 보건복지가족부령으로 정하는 경우에는 그러하지 아니하다. ⑥ 제4항 및 제5항에 따른 정보제공의 범위 및 조회 등에 관한 구체적인 사항은 보건복지가족부령으로 정한다.” 동 법률 시행규칙 제 6조 “(헌혈자의 건강진단 등) ⑥ 법 제7조제6항에 따른 혈액원 등이 제공받을 수 있는 정보의 범위는 다음 각 호와 같다. 1. 전염병환자 및 약물복용환자 등의 인적사항, 2. 진단명 또는 처방약물명, 3. 진단일 또는 처방일.”

### 3. 연구, 교육 등 공공 목적에 이용하려 하지만 이를 허용하는 개별 법률 규정이 없는 경우

연구, 교육 등 공공 목적에 이용하려 하지만 이를 허용하는 개별 법률 규

정이 없는 경우라면, 환자의 동의에 의하여 이를 이용하여야 한다. 현실적으로는 진료 정보를 이용한 연구에 사용하는데 대하여 포괄적 동의를 받는다든지, 동의를 받은 범위를 넘은 경우에 수집된 정보를 어떻게 이용할 것인지가 문제 된다.

첫째, 포괄적인 동의와 동의 철회권을 인정하는 방식이다. 포괄적 동의라 함은 예컨대 '앞으로의 암연구에 사용할 수 있다.'라는 식의 일반적인 용어를 사용하는 것이다. 유럽에서는 자신의 검체를 이용한 연구를 함에 있어서 정보 주체의 포괄적 동의(*general consent*), 독립적 윤리 위원회에 의한 정보사용 승인, 언제든지 제한 없이 동의를 철회할 수 있는 자유의 보장에 의하여 사용하는 것이 허용된다<sup>9)</sup>. 이에 반하여 미국은 인체 대상 연구에서 피험자에 대하여 연구에 대한 명시적인 연구만을 인정하고 있다. 그렇기 때문에 IRB, 또는 Privacy Board를 통하여 해당 연구를 수행하는데 있어서 동의를 받도록 하는 것이 불가능하고, 피험자에 대한 침해가 경미한 경우라면 이에 대한 동의 면제하여 주는 연방행정규칙(*Code Federal Regulation, CFR*)을 가지고 있다.

둘째는 '익명화, 암호화'이다. 익명화는 정보에서 개인을 파악할 수 있는 식별 표지를 제거하는 것을 의미한다. 익명화는 여러 단계로 구분될 수 있는데, 첫째 모든 개인 식별자를 제거하여서 정보의 주체를 더 이상 알 수 없는 단계에 이른 것을 *Unlinked (irreversibly) anonymized*라고 한다. 개인 식별자를 제거한 뒤 적당한 암호를 부여하여 익명화 이후 연구자가 개인 정보를 추적할 수 있는 가능성을 남겨 둔 경우는 두 가지로 구분되는데 하나는 *Linked (reversibly) anonymized*라고 하여 연결점은 존재하지만, 그 암호책을 관리하는 자가 따로 존재하여 연구자가 직접 접근할 수 없는 경우와 연구자가 접근할 가능성이 존재하는 경우로 구분할 수 있다. 유럽은 *Unlinked & Linked (reversibly) anonymized*로서 암호책을 관리하는

9) UK biobank 2003, Council of Europe Committee of Ministers 2006, European Society of Human Genetics, 2003.

자가 따로 존재하여 연구자가 직접 접근할 수 없는 경우를 익명화가 되었다고 보는 반면에, 미국은 Linked (reversibly) anonymized 모두를 익명화가 되지 않았다고 보며, 대신 Code화 되었다고 한다. 암호화된 정보를 사용하기 위해서는 개별 IRB의 승인이 필요하다. 익명화가 이루어지면 원칙적으로는 정보 주체를 확인할 수 없기 때문에 환자(개인)의 동의 없이 정보를 사용하는 것이 가능하다. 유전자 연구의 경우, 생명윤리 및 안전에 관한 법률[법률제9100호] (이하 생명윤리법)에 의하면 유전자은행은 수집한 모든 유전정보 등을 익명화하여 보관·관리하여야 하고, 개인정보 보호를 위한 정보관리 및 보안을 담당 책임자를 두어야 한다(제35조의2 제1, 2항). 이때, 성명, 주민등록번호 및 주소 등 개인 식별이 가능한 정보는 코드 또는 암호 등을 이용하여 익명화하여야 한다(동법 시행규칙 제2항 제2호). 생명윤리법은 코드화를 익명화로 인정하고 있다<sup>10)</sup>.

미국의 경우는 HIPAA (The Health Insurance Portability and Accountability Act; 건강보험양도및책임에관한법률)은 전자건강기록(EHR; Electric Health Record)에 대한 개인정보 보호규정(Privacy rule)은 Title 45 of CFR(the Code of Federal Regulation), Part 160 and subparts A and E of Part 164. 에 규정되어 있는데, 정보 주체의 승인 없이 개인건강정보를 사용할 수 있는 경우로서 여러 가지 경우가 열거되어 있는데, 그 중에서 연구의 경우에 IRB 또는 Privacy Board가 다음의 3가지 기준에 따라 정보 주체의 동의 내용을 변경하거나 동의 없이 사용하는 것을 인정하고 있다[45 CFR § 164.512(i)]. 또한 HIPAA & CFR에서 정보 주체

---

10) 익명화는 개념적으로 정보의 주체를 정보로부터 분리하는 방법이지만, 이것이 만능은 아니라고 보아야 한다. 첫째, 제한 익명화의 경우 암호에 대한 정보가 유출되면 익명화가 실패하게 된다. 둘째, 익명화 자체에 친숙하지 않는 정보들이 존재한다. 지역 사회가 폐쇄적이거나 유전 질병이 희귀한 경우 등의 경우, 가계도 분석이 가능한 경우는 익명화와 관계없이 특정 사실이 공표되는 것만으로 개인 식별이 가능할 수 있다. 정보에 대한 논의 과정에서 인종적 그룹(Ethnic group)에 대한 보호 문제는 서양의 경우 항상 거론되는 문제이다. DNA 검체의 경우, 유전자 분석을 하다면 언제든지 공여자를 파악할 수 있다는 측면에서 익명화의 한계로서 언급하는 견해도 있다.



의 승인 없이 제한된 데이터셋(limited data set)을 이용하는 것을 최소 위험이라고 하였어도, 개별 기관의 IRBs나 privacy board가 승인을 받을 것을 요구하는 것은 가능하다.

1) 프라이버시에 대한 최소 위험을 초과하지 않는 특정한 조건이 만족되는 경우(1) No more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements<sup>11)</sup>, 2) 동의 포기나 변경이 없다면 연구가 실질적으로 수행될 수 없는 경우(The re-search could not practicably be conducted without the alteration or waiver)<sup>12)</sup>, 3) 개인정보를 사용하지 않을 경우에는 연구가 실질적으로 수행 불가능한 경우(The research could not practicably be conducted without access to and use of the PHI).

아직 우리나라는 의료정보가 관련된 연구에 관한 이러한 일반적인 조항을 도입하고 있지는 않고 있다. 다만, 의학 연구에 있어서 기관내윤리위원회가 조직되어 의학 연구에 관한 의료 정보의 수집, 이용에 대하여 계획서를 승인하는 절차를 가지고 있는데, 생명윤리및안전에관한법률(이하 생명윤리법) 제9조 및 동 시행규칙 제2조에 의한 유전자연구 등 기관생명윤리

---

11) ① an adequate plan to protect the identifiers from improper use/disclosure; ② an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining identifiers or such retention is otherwise required by law; ③ adequate written assurances that PHI will not be reused/disclosed to any other person or entity, with certain exceptions.

12) ① Limited data set with a data use agreement; ② Preparatory to research; ③ For the research on decedents' information. / Limited Data Set: A limited data set is information that is minimally identified by including a few selected identifiers. It may only contain: the subject's dates of admission and/or discharge, their date of death (if applicable), their date of birth (which can only be used as necessary), and the subject's five digit zip code or any other geographic subdivision (e.g., state, city, county.) / Data Use Agreement - An agreement into which the covered entity enters with the intended recipient of a limited data set that establishes the ways in which the information in the limited data set may be used and how it will be protected. / The subject's street address cannot be included. Because a limited data set is not fully de-identified and could potentially be used to re-identify an individual, it is still subject to privacy protections.

심의위원회 등을 조직하여 연구계획서에 대한 승인 기능을 하는 것, 의약품임상시험관리기준(식품의약품안전청 고시 1999-67호)에 의하여 임상시험심사위원회(Institutional Review Board, IRB)를 조직하여 약물과 관련된 임상시험계획서를 심사하면서 개인 정보를 보호하는 것이 있다. 2010.1월에 발표된 “의료기관의 개인정보보호가이드라인(500병상 이상)”의 경우, 의료기관에 대하여 개인정보보호위원회를 설치하도록 하고, 연구에 관하여 IRBs와 통합적인 운영이 가능하도록 규정하고 있다<sup>13)</sup>. 민간부분에서 의료 정보에 대한 수집과 이용 문제는 입법에 의하여 위원회 설치 의무를 부과하고, 정부는 각종 위원회의 활동을 규율하는 간접적 방식으로 이루어지고 있다. 이에 반하여 공공부분의 경우, 개인정보법에 의하면 제20조 및 동 대통령령 제28조에서 개인정보보호심의위원회를 구성하는데, 그 기능이 제도 개선, 공공기관간의 의견조정, 개인 파일 기록 항목의 관보 게재 여부, 법령의 정비 개선에 그치고 있으며, 개인 정보가 포함된 의료 정보를 이용하는 경우는 입법에 의한 사유로 한정하고 있다<sup>14)</sup>.

## V. 결 토

1. 의료기관 개인정보의 이차적 이용은 공공 목적을 위하여 반드시 필요할 수 있다. 비록 의료법 제21조에서 기록 열람 사유를 한정적으로 열거하고 있지만, 개별 입법을 통하여, 연구, 교육 등의 목적을 위하여 기관내부

13) 의료기관 개인정보보호 가이드라인. III. 개인정보 보호 및 보안에 관한 관리적 지침. 1. 개인정보 보호 및 보안 관리 조직. 1.1. 개인정보보호위원회. 5. 연구에 관련되어 연구 계획서 심의와 함께 개인정보를 다루는 경우에 개인정보보호위원회는 그 권한을 병원 내의 연구윤리심의위원회에 위임할 수 있다.

14) 공공기관의 개인정보보호에 관한 법률[법률 제8871호] 제10조(처리정보의 이용 및 제공의 제한) ① 보유기관의 장은 다른 법률에 따라 보유기관 내부 또는 보유기관 외의 자에 대하여 이용하게 하거나 제공하는 경우를 제외하고는 당해 개인정보파일의 보유 목적 외의 목적으로 처리정보를 이용하게 하거나 제공하여서는 아니 된다.

개인정보보호위원회, 임상시험심사위원회의 승인을 거쳐서 이용할 수 있는 방법들이 현실적으로 열려 있다. 소득세법, 혈액관리법상의 정보 제공은 의료법의 제3자 기록 열람 범위를 확장한 것이다. 그렇다면 이차적 이용에 대하여 개인의 프라이버시를 보호하기 위한 가능한 기준을 정하여야 한다. 1980년 경제협력개발기구이사회의에서는 각국에서의 개인정보보호법 제정과 관련하여 채택한 “프라이버시 보호와 개인 데이터의 국제유통에 관한 가이드라인에 관한 이사회 권고(‘Guidelines on the Protection of Privacy and Transborder Flows of Personal Data’ OECD, Paris, 1980)”에 의한 “① 수집제한(Collection Limitation)<sup>15)</sup>, ② 데이터 질(Data Quality)<sup>16)</sup>, ③ 목적 명확화(Purpose Specification)<sup>17)</sup>, ④ 이용제한(Use Limitation)<sup>18)</sup>, ⑤ 안전보호(Security Safeguards)<sup>19)</sup>, ⑥ 공개(Openness)<sup>20)</sup>, ⑦ 개인참가(Individual Participation)<sup>21)</sup>, ⑧ 책임(Accountability)<sup>22)</sup>” 원칙들을

- 
- 15) There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
  - 16) Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
  - 17) The purposes for which personal data are collected should be specified not later than at the time of collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
  - 18) Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [Principle 3] except: (a) with the consent of the data subject; or (b) by the authority of law.
  - 19) Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
  - 20) There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
  - 21) An individual should have the right: - to obtain from the a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; to be given reasons if a request made under sub-paragraphs (a) and (b) is denied, and

고려할 필요가 있다.

그 중에서 제1의 원칙이 “수집 제한”이라는 것은 디지털 시대에 있어서 개인정보보호의 첫 출발점은 가능한 데이터화를 하지 않는 것에 있다는 것을 의미한다. 동의가 없거나 동의 추정이 어렵다면, 공공복리를 위한 기본권 제한의 문제가 되며, 입법에 의한 기본권 침해의 과잉금지원칙 위반을 따져야 한다, 이때 가장 중요한 것은 과연 이러한 데이터베이스를 만들어야 하는가에 대한 논의를 해야 한다는 것이다.

### 1. 정보 수집의 문제

1) 국세청은 소득세 신고의 편의성을 위하여 병원에서 진료한 내역을 컴퓨터를 통하여 국세청에 신고하는 방안을 고지한 바 있다. 이 경우 환자 정보에 대한 보호는 컴퓨터 상의 식별자(ID), 암호(PW)와 같은 전자적 보호장치로 충분하다고 하였다. 의료 기관은 환자의 개인 정보 보호를 위하여 이를 거부하였고, 많은 시민단체들은 이를 의약단체들이 밥그릇 지키기를 하는 것이라고 비난하였다. 진료 정보는 특히 민감한 개인정보이므로, 환자가 특정한 의원을 내원한 사실이 알려지는 것만으로도 많은 문제를 일으킬 수 있다. 의료비 공제에 일정한 액수 제한(의료비 공제는 총급여의 3%인 공제 한도를 초과하는 금액만 가능하며 500만원 한도; 2010년 기준)이 있다는 것을 고려하면, 세금 징수의 편의를 위하여 개인 의료정보를 수집하는 것에 대하여 모든 의료 행위자에 대한 데이터베이스를 만드는 것이 필요한 것인지는 의문이 있다.

2) 헌혈 금지 (또는 보류) 약물을 처방할 경우, 조제하는 경우에 본인의 임신 금지와 헌혈에 대한 주의 사항의 설명은 약을 처방한 의료 기관과 조

---

to be able to challenge such denial; and to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.  
22) A data controller should be accountable for complying with measures which give effect to the principles stated above.

제한 약사의 공동 책임으로 보아야 한다. 이러한 설명을 바탕으로 약을 복용한 자들이 스스로 헌혈을 하지 않도록 하고, 헌혈을 하는 경우에도 문진을 통하여 헌혈을 막는 것이 가장 바람직한 방법이 될 것이다. 그러나 환자들이 이러한 설명을 이해하지 못하거나 망각한 경우에는 헌혈시 문진을 통하여 이를 선별할 수 없게 된다. 이 문제를 해결하기 위하여 혈액관리법은 개정되었고, 그림 1)의 방식을 도입하게 되었다. 정보조회시스템의 당부를 논할 때 반드시 고려하여야 할 전제는 제시된 방안들이 현실적으로 타당한가를 따져보아야 한다는 것이다. 예컨대 정보 조회를 하지 말고 헌혈된 혈액을 사후에 검사하여 부적격 혈액으로 폐기하는 방식을 택하는 것이 적절하다는 주장을 한다면, ‘현재 기술 수준에서 헌혈 혈액으로부터 헌혈 금지 약물인 아시트레틴을 찾아낼 수 있는지? 기술적인 의미에서 이러한 것이 가능하다고 하여도 이를 실제로 시행하는 것이 경제적으로 가능한지?’에 대한 검토가 선행되어야 한다. 마찬가지로 정보조회시스템을 통하여 헌혈 금지 약물을 복용한 자의 헌혈을 막아야 한다고 주장하기 위해서는 이러한 약물을 투여한 환자로부터 유래한 혈액을 수혈한 경우에 발생할 수 있는 위험은 과연 어느 정도인지를 확정하는 것도 필요하다. 오염된 수혈의 결과가 수혈 받은 자의 건강 등에 매우 중대한 피해를 유발한다면 이러한 정보 조회가 정당화 될 수 있는 여지는 커질 것이다. 이 점은 간염, 에이즈와 같은 전염성 질환에 대한 정보 조회와 구별된다. 전염성 질병을 가지고 있는 자의 헌혈에 의한 질병 전염의 가능성은 매우 잘 알려져 있는데 비하여, 헌혈 금지 약물의 경우, 실질적으로 위해가 발생할 가능성에 대한 입증은 거의 입증되지 못하고 있다. 그렇다면 과연 이런 식으로 헌혈을 금지하는 것이 타당한 것인가라는 의문조차 발생시킨다. 헌혈 금지 약물은 제외 기준들(exclusion criteria)로 작동하며 부족한 혈액의 공급을 더 낮추는 장애물로 나타날 수도 있다.

## 2. 최소 침해 가능한 다른 방법은 없는가?

1) 현재의 정보 수집과 활용 방안에 의하면 독립된 데이터베이스를 생성하고 이를 이용하여 헌혈 현장에서 헌혈 부적격 여부를 확인하는 것이 가능해진다. 그러나 이러한 조치들이 반드시 필요한지에 대하여 의문을 제기할 수 있다. 현재의 체계를 유지한다면 개별 헌혈 현장에서 수많은 직원들이 ID와 PW를 가지고 개인 정보를 조회하는 상황이 발생한다. 이러한 상황은 헌혈을 원치 않는 많은 개인들의 정보가 함께 노출된다는 점을 의미한다. 물론 전산시스템에 접속한 사람들에 대한 기록을 자동으로 남기도록 함으로써 책임 소재를 차후에 추궁할 수 있다고 하지만, 현재 개인들이 느끼는 불안감을 제거하기는 어려울 것이다. 만약 헌혈 현장에서 헌혈 부적격 여부를 확인하는 것이 반드시 필요하지 않다면, 헌혈 이후에 혈액을 보관한 상태에서 제한된 범주의 사람들이 본부의 DB를 이용하여 혈액제제에 대하여 exclusion criteria를 적용하는 것은 불가능한지를 고려해보아야 한다. 이 방법이 가능하다면 비록 시간적으로는 약간의 지체가 있을 수 있지만, 개인 정보가 누출될 가능성을 줄일 수 있다는 장점이 있다. 더 나아가 헌혈을 자원한 사람이 헌혈 창구에서 거절당하는 문전 박대와 같은 상황은 연출되지 않을 것이다.

2) 만약 1)의 가정이 가능하다면, 더 나아가 독립된 DB를 운용하지 않고 심평원, 질병관리본부에 개별적으로 의뢰하는 것은 불가능한지를 살펴볼 필요가 있다. 실제로 우리가 필요로 하는 정보는 심평원과 질병관리본부의 DB에 보관된 것이다. 이 정보의 외부 전달은 현재는 ‘공공기관의 개인정보 보호에 관한 법률 제10조 제3항 2호에 의하여 ‘처리 정보 보유기관의 장은 처리 정보를 보유목적 외의 목적으로 이용하게 하거나 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 제20조에 따른 공공기관개인정보보호 심의기관위원회의 심의를 거친 경우… 제공 할 수 있다.’ 규정에 의하면 정보 제공의 조건으로 정보를 제공하지 않으면 다

른 법률에 정한 소관 업무를 수행할 수 없는 경우에만 일정한 절차에 따라 정보를 제공할 수 있다. 정보를 제공하지 않고서도 다른 법률에 정한 소관 업무를 수행할 수 있다면 정보를 제공하여서는 안 된다. 생각건대 보유하고 있는 정보가 외부의 다른 정보와 결합하여야만 새로운 정보 능력을 발휘하는 경우, 많은 DB로부터 정보를 얻어서 통합하여야 하기 때문에, 현실적으로 통합된 하나의 DB를 구성하는 것이 정보 이용을 위하여 반드시 필요한 경우 등과 같은 경우라면 외부로 정보를 제공하는 것이 정당화 될 수 있을 것이다. 예컨대 헌혈에 대한 제외 기준(exclusion criteria) 적용을 위하여 32개의 DB를 이용하여야 하고, 개별 DB가 전산화 정도가 차이가 있는 경우에는 하나의 DB를 구성할 필요성이 나타날 것이다<sup>23)</sup>. 하지만 이번 정보조회시스템은 심평원, 질병관리본부 자체 DB에 의하여 결정된 정보로 보아야 한다. 그러므로 현재의 상황이라면 굳이 외부로 정보를 제공할 필요는 없고, 혈액원에서 필요한 사항을 심평원, 질병관리본부에 의뢰하면 이를 검색하여 결과를 알려주는 시스템을 가지는 것으로 충분하다고 생각된다.

## VI. 결 론

의료기관 개인정보 이용에 대한 입법의 위헌성을 다루는데, 논의가 된 부분은 과잉금지원칙에 의한 필요성이다. 의료정보 관련 개인정보는 개인의 내밀한 사적 영역에 관여하는 민감한 정보로서 언제나 엄격한 보호의 대상이 되어야 한다. 그러므로 개인정보를 수집하여 DB화하여 모아야 한다고 판단하였다면, 개인의 프라이버시를 침해하는 정도가 좀 더 적은 방법

---

23) William Riley, Matthew Schwei, and Jeffrey McCullough. The United States' potential blood donor pool: estimating the prevalence of donor-exclusion factors on the pool of potential donors. TRANSFUSION Volume 47, July 2007, 1182.

은 없는지 고려하여야 한다. 그것이 최소 수집의 원칙이다. 이러한 최소 침해의 방안이 있는데도 이를 우선 고려하지 않는다면, 개인의 프라이버시보호는 사실상 유명무실해진다. 예컨대 국세청에 모든 의료비 사용 내역에 대한 DB를 확립하기보다는, 연말정산 간소화를 원하는 해당자들이 자신의 의료 정보가 국세청으로 수집되는 것에 대하여 동의하는지 확인하고, 희망한 자들에 대해서만, 의료비 자료를 받아서 DB를 하는 것을 일차적으로 논의하여야 한다. 건선치료제(제품명: Neotigason<sup>®</sup>) 투여자에 대해 헌혈 금지를 위한 정보조회시스템 구축의 경우에는 다음과 같은 점을 고려하여야 한다. ① 현재 기술로 헌혈된 혈액을 검사하여 혈액에서 아시트레틴을 밝혀낼 수 있는지를 먼저 고려하여야 한다. 이것은 특정 질환을 가진 자가 헌혈하는 것에 대하여 항원이나 항체를 찾고자 하는 것과 마찬가지로 원리이다. 이러한 검출 방법이 경제적으로 가능한지도 분석하여야 한다. ② 과연 이러한 약물을 투여한 환자로부터 유래한 혈액을 수혈한 경우에 발생할 수 있는 위험은 과연 어느 정도인지를 정확하게 밝혀내는 것도 필요하다. 그다음에 혈액관리법에 의한 정보보호에 있어서도, 심평원과 질병관리본부에 개별 DB를 구축하고, 혈액원이 필요한 정보를 의뢰하는 방식을 먼저 선택하여야 한다. 혈액원에서 DB를 가지고 헌혈을 할 수 없는 배제군에 대한 리스트를 만들고, 헌혈 장소에서 터미널을 설치하여 그 정보를 조회하는 것은 헌혈자의 프라이버시 침해에 대한 엄격한 보호를 하였다고 보기 어렵다고 본다. 개별 입법이 없는 경우에 연구, 교육 등의 목적을 위하여 기관내부 개인정보보호위원회, 임상시험심사위원회의 승인을 거쳐서 이용할 수 있는 방법 역시 마찬가지로 그 사용에 대한 심사를 엄격하게 하여야 한다. 공공부문의 의료정보 보호 역시 민간 부문과 동일한 정도의 절차적인 권리를 인정하여야 한다. 형식적인 위원회나 제한적 열거주의로는 개인정보 보호를 하는데 한계가 있을 것으로 판단된다. 자기 정보 열람청구권, 자기 정보 정정청구권, 자기 정보 사용중지, 삭제청구권을 포함하는 자기 정보 관리통제권의 보장을 단순하게 보유기관의 장에게 맡기는 것(예컨대 개인정보법



제14조)보다는 인권에 대한 구체화된 결정은 내부윤리위원회에 위임하는 것이 필요하다.

**주제어** : 의료기관, 개인건강정보, 프라이버시 보호, 보안, 이차적 이용

[참 고 문 헌]

1. 국내문헌

김장한·김신효·박명화·박종현·방지언. 『의료기관 개인정보보호 가이드라인』, 울산대학교 산학협력단, 2010.

보건복지부, “헌혈금지약물에 대한 혈액관리강화대책 추진”, 보도자료, 2006, 9.6.

「의약품임상시험관리기준」, 식품의약품안전청 고시 1999-67호.

이인호, “미국의 개인정보보호법제 대한 분석과 시사”. 『법학논문집』, 제29집 제1호, 중앙대학교법학연구소, 2005.

2. 외국문헌

Guidelines on the Protection of Privacy and Transborder Flows of Personal Data' OECD, Paris, 1980.

The Health Insurance Portability and Accountability Act. Title 45 of CFR (the Code of Federal Regulation), Part 160 and subparts A and E of Part 164.

William Riley, Matthew Schwei, Jeffrey McCullough. The United States' potential blood donor pool: estimating the prevalence of donor-exclusion factors on the pool of potential donors. TRANSFUSION 2007; 47:1182.

## The Protecton of Privacy on Secondary Use of Personal Health Information

Jang Han Kim

*University of Ulsan College of Medicine Department of Medical Humanities and Social Science*

### =ABSTRACT=

Along with the development of digital technologies, the information obtained during the medical procedures was working as a source of valuable assets. Especially, the secondary use of personal health information gives the ordeal to privacy protection problems. In Korea, the usage of personal medical information is basically regulated by the several laws in view of general and administrative Act like Medicine Act, Public institutions' personal information protection Act, Information-Network Act etc. There is no specific health information protection Act. Health information exchange program for the blood donor referral related with teratogenic drugs and contagious disease and medical treatment reporting system for income tax convenience are the two examples of recently occurred secondary use of health information in Korea. Basically the secondary use of protected health information is depend on the risk-benefit analysis. But to accomplish the minimal invasion to privacy, we need to consider collection limitation principle first. If the expected results were attained with alternative method which is less privacy invasive, we could consider the present method is unconstitutional due to the violation of proportionality rule.

Keyword : Medical institution, Protected health information, Privacy protection, Security, Secondary use