# 우리나라 상급종합병원의 개인정보 처리방침 운영실태

*The Status of Privacy Policy on Tertiary Hospitals in Korea*

**정영철** 한국보건사회연구원 연구위원

개인정보 처리방침은 개인정보처리자에게는 개인정보 보호 수준향상을 위한 첫걸음이자, 개인정보 주체에게는 자신의 개인정보 처리를 확인하여 정보불평등을 해소할 수 있는 기전이다. 우리나라 43개 상급종합병원의 개인정보 처리방침 내용을 분석해본 결과, 공개율은 만족할만한 수준이었으나 충분성, 정확성 등 질적수준은 미흡하게 나타났다. 향후 질적 수준을 계량적으로 측정할 수 있는 기준에 대한 진일보된 연구를 기대하며, 본 연구에서 제시한 각 항목별 예시를 기반으로 보다 정확하고 충분한 개인정보 처리방침을 수립하고 공개하여 의료기관 개인정보 보호 수준향상에 일조하고자 한다.

## 1. 서론

우리나라는 정보통신기술(ICT: Information & Communication Technology)의 발전정도를 평가하는 국제전기통신연합(ITU: International Telecommuincation Union)의 ICT 발전지수에 있어 2010년부터 4년연속 1위를 차지할만큼[1] 정보화강국이다. 그러나 정보화로 인한 생산성 및 효율성 향상, 시공간을 초월한 관계형성 등과 같은 순기능 뿐 아니라 해킹, 프라이버시 침해, 개인정보 오남용 등과 같은 역기능으로 인한 사회문제가 빈발하면서 우리나라에서도 정보주체의 사생활 보호 및 개인정보에 대한 권익을 보장하기 위해 마침내 2011년 3월 「개인정보 보호법」이 제정되었다.

정보보호 및 개인정보 보호 분야에 대한 글로벌 지수로는 세계경제포럼(WEF: World Economic Forum)이 매년 발표하는 세계 ICT보고서(Global Information Technology Report) 중 네트워크 준비지수(NRI: Networked Readiness Index)의 하나인 '보안서버 보급률'이 유일하다 하겠다. 「개인정보 보호법」 시행이전인 2010년 우리나라 보안서버 보급률은 인구 백만명당 696대로 14위[2]를 차지한 반면, 2013년 우리나라의 보안서버 보급률은 인구 백만명당 2,752대로 148개국 중 3위[3]를 차지하여 정보화수준

1) ITSTAT 포털(itstat.go.kr), 국제 ICT 발전지수 중 'ITU ICT 발전지수'. [인용 2014.5.11.].
2) 방송통신위원회 · 한국인터넷진흥원(2012). **2011 경제발전경험 모듈화사업: 한국의 정보보호활동과 시사점**, pp.131.
3) World Ecomonic Forum(2014). Global Information Technology Report 2014.

에 맞추어 정보보호 및 개인정보 보호 분야에서도 현격한 발전의 모습을 보이고 있다.

정보보호와 개인정보 보호는 상황에 따라 같은 의미로 사용되기도 하지만 '정보보호'는 관리와 책임, 그리고 상대해야 할 주체가 모두 조직의 내부에 있는 반면, '개인정보 보호'는 외부 고객도 조직이 상대해야 할 주체에 포함되는 만큼[4] 개인정보 보호를 위해 필요로 하는 제반 활동이 더해질 수 있다. 그 중 하나가 "개인정보 처리방침"을 수립하고 공개하는 것이다. 개인정보 처리방침은 개인정보처리자에게는 개인정보 보호에 관한 경각심을 불러일으키고[5], 개인정보 주체에게는 개인정보처리자가 자신의 개인정보를 어떻게 처리하고 있는 지 확인할 수 있는 기전으로 개인정보 보호법에 의해 이를 수립 및 공개토록 하고 있다. 이에 개인정보 처리방침 수립 · 공개 현황은 개인정보 보호 수준을 파악하기 위한 지표 중 하나로 사용되면서 최근에는 이와 같은 개인정보 처리방침에 대한 중요성이 부각되어 심사제도 도입[6]이라던가 개인정보 처리방침 작성 및 공개에 대한 관리를 강화하는 내용의 개인정보 보호법 개정안이 발의[7]되는 등 많은 움직임이 있다.

이에 개인정보 처리방침에 대해 기존 다양한 조사를 통해 영역별, 기관별 수준을 파악하고 효과달성정도, 가독성 제고방안, 현황 분석방안 등에 대한 몇몇 연구가 진행[8]된 바 있으나 대부분 개인정보 처리방침 게시여부, 각 항목별 포함여부 등 양적 분석에 머물러 그 내용의 적정성, 질적 수준에 대해서는 깊이있게 다루지 않고 있다.

그러므로 본 고에서는 개인정보 처리방침 수립 · 공개 여부와 더불어 그 내용을 항목별 사례 중심으로 면밀히 분석하고 문제점을 진단해 봄으로써 추후 해당영역의 개인정보 처리방침 수립 시 양적, 질적 수준 제고를 기대코자 한다. 한편, 해당 영역을 선정함에 있어 개인정보 보호법 시행이후 최근 개인정보 보호의 필요성과 중요성이 한층 부각되고 있는 의료기관에서의 개인의료정보 보호를 위해 전(全) 의료기관을 선도하고 있는 43개 상급종합병원 홈페이지에 게시되어 있는 개인정보 처리방침을 분석대상으로 하였다. 본 조사분석결과를 통해 추후 의료기관에서는 개인정보 처리방침 수립 · 공개에 유용한 참고자료가 될 것이며, 궁극적으로는 의료기관의 개인의료정보 보호 수준향상을 기대코자 한다.

4) 김정덕(2008). 개인정보보호를 위한 관리체계와 거버넌스, **한국정보보호학회지, 18**(6), pp1~5, 서울: 한국정보보호학회.
5) 정찬모(2013). 개인정보취급방침 심사와 개인정보보호 감사제도 도입방안, **법학논총, 20**(1), pp3~29. 광주: 조선대학교 법학연구원.
6) 정찬모(2013), 전게서.
7) 중앙일보(2014.3.10.), 박남춘, '개인정보보호법개정안' 발의, http://style.joins.com/News/article/.Article.aspx?tm=ctg=&total_id=14109565.
8) 안전행정부 · 개인정보보호위원회(2013). **개인정보보호 실태조사;** 이기헌 · 서의진(2011). **개인정보 수집 제공관리실태 및 개선방안 조사결과,** 서울: 한국소비자원; 장원창 · 신일순(2012). 인터넷 이용자의 개인정보 처리방침에 대한 인지 및 확인과 온라인 거래 행동, **정보보호학회논문지, 22**(6), pp.1419~1427, 서울: 한국정보보호학회; 김두현 · 선원진 · 김현재(2014.2.). 읽기 쉬운 개인정보 처리방침, **NIA PRIVACY ISSUES, 10,** 서울: 한국정보화진흥원; 고유미 · 최재원 · 김범수(2014). 사용자 인지 제고를 위한 개인정보보호정책 알림방식의 비교연구, **정보보호학회논문지, 24**(1), pp.183~193, 서울: 한국정보보호학회; 이재근 · 강상욱 · 염흥열(2013). 개인정보처리방침의 데이터를 활용한 개인정보보호 현황 분석, **정보보호학회논문지, 23**(4), pp.767~779, 서울: 한국정보보호학회.

## 2. 개인정보 처리방침

정보주체의 개인정보를 수집하여 이용하는 자(者)는 개인정보를 안전하게 관리하여야 하고 이를 정보주체가 알 수 있도록 하여야 한다. 이러한 원칙은 OECD 프라이버시 가이드라인, EU 개인정보보호 지침, 세계 각국의 개인정보 보호관련 규정 뿐 아니라 우리나라의 개인정보 보호법, 정보통신망 이용촉진 및 정보보호등에 관한 법률(이하 정보통신망법)에서 공통적으로 명시하고 있다[9]. 이를 우리나라 개인정보 보호법에서는 "개인정보 처리방침"으로, 정보통신망법에서는 "개인정보 취급방침"으로 규정하고 있다.

개인정보 보호법은 전지역, 전 대상에게 공통적으로 적용되는 일반법이며, 정보통신망법은 특정 사람, 사물, 행위 또는 지역에 국한하여 적용되는 특별법으로, 본 고에서는 일반법 인 개인정보 보호법을 중심으로 "개인정보 처리방침"을 기준으로 하였다.

개인정보 처리방침은 개인정보처리자가 정보주체의 개인정보 처리(수집, 생성, 연계, 기록, 저장, 보유, 가공, 편집, 검색, 이용, 제공, 공개, 파기 등) 시 이행하는 기준 및 보호조치 등을 일정 원칙에 의해 정하는 것으로써, 이를 정하고 공개하는 제도에 대해 정찬모(2013)[10]는 개인정보 보호에 관한 개인정보처리자의 경각심을 불러일으키는 데 의의가 있다고 하였으며, 장원창 · 신일순(2012)[11]는 개인정보처리자와 정보주체와의 정보 비대칭성(information asymmetry)을 해결하고자 하는 제도라 하였다.

우리나라에서는 개인정보 보호법 제30조(개인정보 처리방침의 수립 및 공개), 동법 시행령 제31조(개인정보 처리방침의 내용 및 공개방법 등), 표준 개인정보 보호지침 제34조(개인정보 처리방침의 공개), 제35조(개인정보 처리방침의 변경), 제36조(개인정보 처리방침의 작성기준 등), 제37조(필수적 기재사항), 제38조(임의적 기재사항)에 의거하여 개인정보 처리방침을 수립하여 "개인정보 처리방침"이라는 명칭으로 공개토록 하고 있다. 이에 따라 개인정보처리자는 개인정보를 "처리" 함에 있어 개인정보 처리 목적, 개인정보 처리 및 보유기간, 개인정보 제3자 제공사항, 개인정보처리 위탁사항, 정보주체의 권리 · 의무 및 그 행사방법 사항, 처리 개인정보 항목, 개인정보 파기사항, 개인정보 안전성확보조치 사항 등에 관한 방침을 수립하고, 개인정보처리자의 인터넷 홈페이지에 지속적으로 게재토록 하고 있으며 이와 같은 개인정보 처리방침을 정하지 아니하거나 공개하지 아니한 경우, 1천만원 이하의 과태료가 부과된다[12]. 이와 같은 개인정보 처리방침에 대한 규제내용 및 법적근거 등은 <표 1>과 같다.

9) 윤주희(2013). 개인정보 취급방침의 변경에 따른 문제점과 관련법의 적용에 관한 연구, **법학논고 제41집**, pp.391~428, 대구: 경북대학교 법학연구원.
10) 정찬모(2013), 전게서.
11) 장원창 · 신일순(2012), 전게서.
12) 국가법령정보센터 사이트(http://www.law.go.kr/) 중 「개인정보 보호법」, [인용 2014.5.9.].

**표 1. 개인정보 처리방침 구성내용 및 법적 근거**

| 구분 | 내용 | 법적 근거 | 과태료 |
|---|---|---|---|
| 개인정보처리방침 수립 | – 개인정보처리방침을 수립하여야 함 | – 개인정보 보호법 제30조제1항 | 1천만원 |
| 개인정보처리방침 게시 | – 개인정보처리방침을 게시하여야 함 | – 개인정보 보호법 제30조제2항 | 이하의 과태료 |
| 개인정보 처리방침 내용 및 공개방법 등 | – 개인정보처리방침 내용에 처리항목, 파기사항, 안전성확보조치사항을 포함함<br>– 수립및변경 개인정보처리방침은 인터넷홈페이지에 지속적으로 게재하여야 함 | – 개인정보 보호법 시행령 제31조 | – |
| 개인정보처리방침 명칭 | – "개인정보 처리방침"이라는 명칭을 사용함 | – 표준 개인정보 보호지침 제34조 | – |
| 개인정보처리방침 변경 | – 개인정보 처리방침 변경시 변경내용을 지속적으로 공개함 | – 표준 개인정보 보호지침 제35조 | – |
| 개인정보처리방침 작성기준 | – 개인정보 처리목적에 필요한 최소한의 개인정보임을 밝힘<br>– 목적에 필요한 최소한의 개인정보와 추가서비스를 위한 개인정보를 구별하여 표시함 | – 표준 개인정보 보호지침 제36조 | – |
| 필수적 기재사항 | – 필수 기재항목을 포함하여야 함<br>• 개인정보 처리목적<br>• 개인정보 처리및보유기간<br>• 개인정보 제3자 제공 사항<br>• 개인정보 위탁 사항<br>• 정보주체의 권리 · 의무 및 행사방법 사항<br>• 처리 개인정보 항목<br>• 개인정보 파기 사항<br>• 개인정보 보호책임자 사항<br>• 개인정보 처리방침 변경사항<br>• 개인정보 안전성확보조치 사항 | – 표준 개인정보 보호지침 제37조 | – |
| 임의적 기재사항 | – 임의 기재항목을 포함할 수 있음<br>• 정보주체 권익침해 구제방법<br>• 개인정보 열람청구 접수 · 처리부서 | – 표준 개인정보 보호지침 제38조 | |

자료: 국가법령정보센터 사이트(http://www.law.go.kr/) 중 「개인정보 보호법」, 「개인정보 보호법 시행령」, 「표준 개인정보보호 지침」, [인용 2014.5.9.].

2013년 개인정보보호 실태조사 결과에 의하면, 이러한 개인정보 처리방침은 공공부문의 경우 92.7% 즉 대부분의 공공기관이 수립 · 공개하고 있는 반면, 민간 사업자의 경우 24.2%가 수립 · 공개하여 큰 차이를 나타내고 있고 수립 · 공개하지 않은 민간사업자 중 66.4%가 필요성을 못 느껴서, 26.4%가 의무사항인지 몰라서라고 답하여[13], 공공부문에 비해 민간 사업자의 경우 개인정보 처리방침의 의의와 법적 규제에 대한 이해도를 향상시킬 필요가 있다는 것을 시사하고 있다. 그러나 현행법에서는 개인정보 처리방침에 담아야 할 항목만을 제시하고 그 내

13) 안전행정부 · 개인정보보호위원회(2013), 전게서.

용의 적절성은 통제하지 않고 있어[14] 수립 · 공개율 향상 뿐 아니라 내용의 적절성, 충분성에 대한 관심도 불러일으킬 필요가 있다 하겠다.

## 3. 상급종합병원 개인정보 처리방침 현황

### 1) 분석대상 및 방법

본 고에서의 분석대상 주체인 상급종합병원은 의료법 제3조의4(상급종합병원 지정)에 의해 특정 요건을 갖추고, 중증질환에 대해 난이도가 높은 의료행위를 전문적으로 하는 종합병원으로써 보건복지부장관이 지정하며 매 3년마다 평가를 실시하여 재지정 혹은 지정을 취소할 수 있다[15]. 2014년 현재 우리나라 전체 327개 종합병원 중 약 13%인 43개가 지정되어 있다.

이들 상급종합병원은 상급종합병원의 지정 및 평가에 관한 규칙 제2조(상급종합병원의 지정 기준)에 의해 진료기능, 교육기능, 인력 · 시설 · 장비, 질병군별 환자의 구성비율, 의료서비스 수준, 진료권역별 소요병상 충족도 등 6가지 측면에서 일정 기준을 충족하여[16] 전체 의료기관을 선도하고 있는만큼 개인정보 보호 측면에서도 우선적인 수준제고의 대상이라 할 수 있다.

분석방법은 먼저, 개인정보 보호법령 및 의료기관 업무에 대해 잘 알고 있는 본 저자를 중심으로 하여 연구원 2명 등 총 3명의 연구원이 2014년 1월 13일부터 17일까지 5일간 43개 상급종합병원 각각의 홈페이지를 검색하여 개인정보 처리방침 유무, 개인정보 처리방침 명칭 사용여부, 필수 및 임의기재항목 유무, 그리고 각 항목에 대한 내용 등 양적, 질적 분석을 시도하였다. 이러한 분석을 위해 개인정보 보호법, 동법 시행령, 표준 개인정보 보호지침 등과 같은 관련 법령과 아울러 개인정보 처리방침 작성예시[17], 개인정보보호 종합지원포털 사이트[18] 등을 참고하였다.

### 2) 분석결과

먼저, 양적 분석에 있어 개인정보 처리방침은 43개 상급종합병원 모두 각각의 홈페이지에 100% 게시하고 있어 게시율에 있어서는 만족할만한 수준을 나타내었다[19]. 명칭 사용에 있어서는 29개 기관(67.4%)이 “개인정보 처리방침”이라는 용어를 바르게 사용하고 있었으며 나머지 14개(32.6%) 기관은 “개인정보 취급방침”이라는 용어를 사용하고 있었다. “개인정보 취급

14) 정찬모(2013), 전게서.
15) 국가법령정보센터(www.law.go.kr), 의료법 제3조의4(상급종합병원 지정). [인용 2014.5.11.].
16) 국가법령정보센터(www.law.go.kr), 상급종합병원의 지정 및 평가에 관한 규칙 제2조(상급종합병원의 지정 기준). [인용 2014.5.11.].
17) 행정안전부(2011). **개인정보처리방침 작성예시(민간용).**
18) 개인정보보호 종합지원 포털사이트(www.privacy.go.kr) 중 ‘개인정보처리방침 만들기’. [인용 2014.1.13.].
19) 전년도 한 연구(정영철 · 이야리 · 이기호(2013). **의료기관의 개인정보보호현황과 대책,** 한국보건사회연구원)에서 조사한 의료기관(의원, 병원, 종합병원, 상급종합병원 전체 30,000여 기관 대상)의 개인정보처리방침 평균 게시율은 51.4%.

방침” 은 정보통신망법 제27조의2(개인정보 취급방침의 공개)에 명시되어 있는 사항으로 만일 상급종합병원이 정보통신망법을 적용받는 기관이라면 특별법 우선의 원칙을 적용하여 개인정보 보호법상 “개인정보 처리방침”을 별도로 수립할 필요는 없다. 그러나 의료기관은 정보통신망법 제2조에 의한 “정보통신서비스 제공자”나 “통신과금서비스 제공자”는 아니므로 일반법 인 개인정보 보호법을 적용하는 것이 맞다 할 것이며 내용을 보더라도 개인정보 보호법에 의한 내용을 담고있어 각 의료기관들은 개인정보 보호법에 의한 “개인정보 처리방침”이라는 용어를 정확히 표현하여야 할 것이다. 다음으로 10개 필수기재항목, 2개 임의기재항목 유무에 대해 분석해본 결과 필수기재항목에 대해서는 평균 96.0%가 포함하고 있었으며 임의기재항목에 대해서는 평균 43.0%가 포함하고 있었다(표 2 참조). 그 중 정보주체의 권리 · 의무 및 행사방법, 처리 개인정보 항목, 개인정보 보호책임자 사항은 43개 기관 모두 포함하고 있었으며 제3자 제공과 위탁사항은 있는 경우에만 포함하게 되어 있어 정확한 기재율은 확신할 수 없었다. 한편 개인정보 처리방침 변경사항과 안전성 확보조치에 관한 사항은 기재율이 93.0%로 10개 필수 기재항목 중 낮게 나타났다. 임의 기재항목에서는 특히 개인정보 열람청구 접수 · 처리 부서에 대한 기재율이 11.6%로 낮게 나타나 이에 대한 추후 보완이 필요하다 할 것이다.

그러나 이러한 기재율은 단지 각 항목에 대해 포함이 되어 있다는 것을 나타낼 뿐 내용에 대

**표 2. 상급종합병원의 개인정보 처리방침 게시 등 현황**

| 구분 | | 기관수 | % |
|---|---|---|---|
| 게시 유무 | | 43 | 100.0 |
| 명칭사용 여부 | | 29 | 67.4 |
| 필수 기재항목 유무 | 평균 | | 96.0 |
| | 개인정보 처리목적 | 41 | 95.3 |
| | 개인정보 처리 및 보유기간 | 41 | 95.3 |
| | 개인정보 제3자 제공 사항 | 41 | 95.3 |
| | 개인정보 위탁 사항 | 39 | 90.7 |
| | 정보주체의 권리 · 의무 및 행사방법 사항 | 43 | 100.0 |
| | 처리 개인정보 항목 | 43 | 100.0 |
| | 개인정보 파기 사항 | 42 | 97.7 |
| | 개인정보 보호책임자 사항 | 43 | 100.0 |
| | 개인정보 처리방침 변경 사항 | 40 | 93.0 |
| | 개인정보 안전성 확보조치 사항 | 40 | 93.0 |
| 임의 기재항목 유무 | 평균 | | 43.0 |
| | 정보주체 권익침해 구제방법 | 32 | 74.4 |
| | 개인정보 열람청구 접수 · 처리 부서 | 5 | 11.6 |

한 정확성 혹은 충분성을 나타내는 지표는 아니다. 이에 각 항목별 게시된 내용에 대해 관련 법령에서 제시하는 준수기준을 중심으로 하고, 개인정보 처리방침 작성예시, 개인정보보호 종합지원포털 사이트 등을 참고하여 분석하였다.

첫 번째, '개인정보 처리목적'에서는 개인정보처리자(해당 의료기관)가 정보주체의 개인정보를 처리함에 대한 목적을 이해하기 쉽고 비교적 구체적이고도 상세히 밝히고, 필요한 최소한의 개인정보임을 밝혀야 하나[20] '개인정보 처리목적'을 게시한 41개 기관의 해당 내용을 분석해본 결과, 많은 기관들이 해당 기관이 처리하고 있는 개인정보 전체의 처리목적이라기보다는 단순 홈페이지 회원에 대한 개인정보 처리목적으로 기술하고 있어[21] 이에 대한 정확한 이해가 부족한 것을 알 수 있다. <표 3>은 '개인정보 처리목적'에 대한 적절한 예시이다.

두 번째, '개인정보 처리 및 보유기간'에서는 각각의 '개인정보 처리목적' 별로 구체적인 기간을 기술하여야 한다. 이 때 관계 법령에 의한 처리의 경우에는 해당 법령명과 조문번호를 같이 기재하며 예외 경우가 있을 시에는 예외사유와 이에 따른 기간을 같이 표시하는 것을 권고하고 있다[22]. 그러나 '개인정보 처리 및 보유기간'을 게시한 41개 기관의 해당 내용을 분석해본 결과, 개인정보 처리목적과 일대일로 대응하여 명확히 표시하지 않은 기관도 상당수가 있었으며 관계 법령에 의한 경우 조문번호를 꼼꼼히 표기하는 곳은 거의 없었다. 처리목적별 기간과 관계 법령 및 조문번호를 게시함으로써 정보주체가 이를 확인하고 정확히 인식함에 의의를 찾기 위해서는 보다 명확하고 정확한 내용을 기재하는 것이 필요하다. <표 4>는 '개인정보 처리 및 보유기간'에 대한 적절한 예시이다.

세 번째, '개인정보 제3자 제공사항'은 필수기재항목이긴 하나 모든 기관에 적용하는 항목은 아니며 제3자에게 개인정보를 제공하는 경우에만 작성하는 내용으로, 제3자 제공은 개인정보 보호법 제17조 및 제18조에 해당하는 경우, 즉 정보주체의 동의 혹은 관련법률의 특별

**표 3. 개인정보 처리방침 기재항목 중 '개인정보 처리목적'에 대한 예시**

**<의료기관명>**은 다음의 목적을 위해 최소한의 개인정보를 처리합니다. 처리하고 있는 개인정보는 다음의 목적 이외의 용도로는 사용되지 않으며, 이용 목적이 변경될 시에는 개인정보 보호법 제18조에 따라 별도의 사전동의를 받는 등 필요한 조치를 취할 것입니다.

1. < ~~~~ 처리목적1>
2. < ~~~~ 처리목적2>
~

20) 표준 개인정보 보호지침 제36조(개인정보 처리방침의 작성기준 등)
21) 예를 들어, "~~홈페이지 회원제 서비스 이용에 따른 본인확인, 홈페이지 불량회원의 부정 이용 방지를 위한 ~~"
22) 행정안전부(2011.12.), 개인정보 처리방침 작성 예시[민간기업/단체용].

**표 4. 개인정보 처리방침 기재항목 중 '개인정보 처리 및 보유기간'에 대한 예시**

**<의료기관명>**은 개인정보 수집 시 동의에 따른 혹은 법령에 따른 개인정보 보유 · 이용기간 내에서 개인정보를 처리 · 보유합니다.
각각의 개인정보 처리 및 보유 기간은 다음과 같습니다.

1. <처리목적1>: 수집 · 이용에 관한 동의일부터(혹은 <해당 법령명, 조문번호>에 따른) <처리 및 보유기간> 까지
2. <처리목적2>: 수집 · 이용에 관한 동의일부터(혹은 <해당 법령명, 조문번호>에 따른) <처리 및 보유기간> 까지
   – <예외사유> 시에는 <처리 및 보유기간> 까지

~

한 규정에 의해서만 할 수 있다. 개인정보 처리 업무에 대한 수탁자 혹은 영업을 양수하는 자는 제3자에서 제외되며 작성 시 정보주체의 동의 혹은 관련법률의 특별한 규정에 의한 경우 외에는 제공하지 않는다는 원칙과 함께 제공받는 자, 제공받는 자의 이용목적, 제공하는 개인정보 항목, 제공받는 자의 보유 · 이용기간 등을 표시할 것을 권고하고 있다[23]. '개인정보 제3자 제공사항'을 게시한 41개 기관의 해당 내용을 분석해본 결과 제3자 제공이 확실히 이루어지고 있는 기관의 경우에도 제공받는자, 이용목적, 제공 개인정보 항목, 보유 · 이용 기간 등에 대해 구체적으로 기술하고 있지 않아 정보주체의 정보비대칭성 문제 해결에 제한이 되고 있었다. <표 5>는 '개인정보 제3자 제공사항'에 대한 적절한 예시이다.

**표 5. 개인정보 처리방침 기재항목 중 '개인정보 제3자 제공 사항'에 대한 예시**

**<기관명>**은 정보주체의 동의, 법률의 특별한 규정 등 개인정보 보호법 제17조 및 제18조에 해당하는 경우에만 개인정보를 제3자에게 제공합니다.
제3자에게 제공하는 개인정보는 다음과 같습니다.

1. <제공받는 의료기관명1>
   – 개인정보를 제공받는 자: <제공받는 의료기관명1>
   – 제공받는 자의 개인정보 이용목적: <이용목적>
   – 제공하는 개인정보 항목: <개인정보 항목>
   – 제공받는 자의 보유 · 이용기간: <처리 및 보유기간>
2. <제공받는 의료기관명2>

~

23) 행정안전부(2011.12.), 전게서.

네 번째, '개인정보 위탁사항' 또한 필수기재 항목이긴 하나 모든 기관에 적용하는 항목은 아니며 위탁할 경우에만 작성하는 내용으로, 위탁업무 각각에 대해 위탁받는자, 위탁업무내용, 위탁기간을 기술하고 개인정보 보호법 제25조에 따라 위탁계약 체결 시 위탁업무 수행목적 외 개인정보 처리금지, 기술적 · 관리적 보호조치, 재위탁 제한, 수탁자에 대한 관리 · 감독, 손해배상 등 책임에 관한 사항을 계약서 등 문서에 명시하고 수탁자가 개인정보를 안전하게 처리하는 지 감독하고 있으며 위탁업무 내용 혹은 수탁자 변경시 지체없이 개인정보 처리방침을 통해 공개토록 한다는 것을 기술토록 권고하고 있다[24]. 이러한 '개인정보 위탁사항'을 게시한 39개 기관의 해당 내용을 분석해본 결과, 일부 의료기관이 게시한 내용 중에는 정보주체의 개인정보 처리와는 연관성이 없어보이는 업무도 있었으며 권장내용 중 위탁계약서, 수탁자 감독 및 번경에 대한 내용이 누락되어 있는 경우가 많았다. <표 6>은 '개인정보 위탁사항'에 대한 적절한 예시이다.

다섯 번째 '정보주체의 권리 · 의무 및 행사방법 사항'에서는 정보주체가 지니는 개인정보 보호 관련 권리와 의무, 그리고 그 행사방법에 대한 내용으로 개인정보 열람, 정정 · 삭제, 처리정지 등 행사방법과 이들에 대한 행사절차, 그리고 이에 대한 거절 및 제한에 대한 내용을 구체적으로 기재할 것을 권고하고 있다[25]. 이러한 '정보주체의 권리 · 의무 및 행사방법 사항'은 43개 기관이 모두 포함하고 있었으나 해당 내용을 분석해본 결과 일부 기관에서는 권리내용, 제한내용, 행사방법 등을 명확하게 구분하

**표 6. 개인정보 처리방침 기재항목 중 '개인정보 위탁사항'에 대한 예시**

**<의료기관명>**은 원활한 개인정보 업무처리를 위하여 다음과 같이 개인정보 처리업무를 위탁하고 있습니다.

1. <위탁업무명1>
   – 위탁받는 자(수탁자): <위탁받는 기관명>
   – 위탁하는 업무내용: <업무내용>
   – 위탁기간: <위탁기간>
2. <위탁업무명2>

~

**<의료기관명>**은 위탁계약 체결시 개인정보 보호법 제25조에 따라 위탁업무 수행목적 외 개인정보 처리금지, 기술적 · 관리적 보호조치, 재위탁 제한, 수탁자에 대한 관리 · 감독, 손해배상 등 책임에 관한 사항을 계약서 등 문서에 명시하고, 수탁자가 개인정보를 안전하게 처리하는지를 감독하고 있습니다.

위탁업무의 내용이나 수탁자가 변경될 경우에는 지체없이 본 개인정보 처리방침을 통하여 공개하도록 하겠습니다.

24) 행정안전부(2011.12.), 전게서.
25) 행정안전부(2011.12.), 전게서.

지 않거나 일부만을 게시하고 있었다. <표 7>은 '개인정보 위탁사항'에 대한 적절한 예시이다.

여섯 번째, '처리 개인정보 항목'에 대해서는 개인정보처리자가 처리하고 있는 개인정보 항목을 앞에서 언급한 처리목적 각각에 따라, 수집목적에 필요한 최소한의 정보(필수항목)와 그 외의 정보(선택항목)을 구분하여 기재하며 자동으로 생성 · 수집되는 개인정보가 있을 경우 이 또한 기재할 것을 권고하고 있다[26]. 그러나 '처리 개인정보 항목'을 게시한 43개 기관의 해당 내용을 분석해본 결과, 개인정보 처리목적과 일대일 대응하여 처리하는 개인정보 항목을 작성하지 않은 기관이 다수 있었다. <표 8>은 '처리 개인정보 항목'에 대한 적절한 예시이다.

일곱 번째, '개인정보 파기사항'에 대해서는 개인정보처리자가 처리하고 있는 목적별 보유기간 경과 후 지체없이 파기한다는 내용을 기재하는 것으로써 파기절차, 앞에서 기재한 처리목적별 파기기한, 그리고 파기방법 등에 관한 세부적인 내용을 기재하며, 개인정보를 파기하지 않고 관련 법령에 의해 보존하는 경우에는 해당 법령명 및 조문을 구체적으로 기재할 것을 권고하고 있다[27]. '개인정보 파기사항'에 대해 게시한 42개 기관의 내용을 분석해본 결과 각각의 처리

**표 7. 개인정보 처리방침 기재항목 중 '정보주체의 권리 · 의무 및 행사방법'에 대한 예시**

정보주체는 **<의료기관명>**에 대해 개인정보 보호법 제35조, 제36조, 제37조에 의해 다음 각 호의 개인정보 보호 관련 권리를 행사할 수 있습니다

1. 개인정보 열람 요구
2. 개인정보 정정 · 삭제요구
3. 개인정보 처리정지 요구

다만, 다음의 경우 **<의료기관명>**은 위와 같은 요구를 거절하거나 제한할 수 있습니다.

1. 법률에 명시되어 있거나 금지 또는 제한되는 경우
2. 다른 사람의 생명 · 신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우
3. 개인정보를 처리하지 않으면 정보주체와 약정한 서비스를 제공하지 못하는 등 계약이행이 곤란한 경우로 정보주체가 그 계약의 해지의사를 명확히 밝히지 않은 경우

이와 같은 권리행사는 개인정보 보호법 시행규칙 별지 제8호 서식에 따라 서면, 전자우편, 모사전송(FAX) 등을 통해 **<의료기관명>**에 하실 수 있으며 **<의료기관명>**은 이에 대해 지체없이 조치하겠습니다.

정보주체가 개인정보 정정 또는 삭제 요구시 **<의료기관명>**은 정정 또는 삭제 완료 시까지 해당 개인정보를 이용하거나 제공하지 않겠습니다.

이러한 권리행사는 정보주체의 법정대리인이나 위임을 받은 자 등 대리인을 통해서도 하실 수 있으며 이와 같은 경우 개인정보 보호법 시행규칙 별지 제11호 서식에 따른 위임장을 제출하셔야 합니다.

26) 행정안전부(2011.12.), 전게서.

**표 8. 개인정보 처리방침 기재항목 중 '처리 개인정보 항목'에 대한 예시**

**<의료기관명>**은 다음의 개인정보 항목을 처리하고 있습니다.

1.<처리목적1>
- 필수항목: <필수 개인정보 항목>
- 선택항목: <선택 개인정보 항목>

2.<처리목적2>

~

또한 인터넷 서비스 이용과정에서 다음과 같은 개인정보 항목이 자동으로 생성되어 수집될 수 있습니다.
- <자동으로 수집되는 개인정보 항목>

목적별 파기기한을 명시하지 않고 원칙적인 내용만을 기술한 기관이 대부분이었다. <표 9>는 '개인정보 파기사항'에 대한 적절한 예시이다.

여덟번째 '개인정보 보호책임자 사항'에 대

**표 9. 개인정보 처리방침 기재항목 중 '개인정보 파기사항'에 대한 예시**

**<의료기관명>**은 개인정보 보유기간 경과 혹은 처리목적 달성 등 개인정보가 불필요하게 되었을 때에는 지체없이 해당 개인정보를 파기합니다.
개인정보 파기절차 및 방법은 다음과 같습니다.

1. 파기절차
   <의료기관명>은 파기사유(보유기간 경과, 처리목적 달성, 사업종료 등)가 발생한 개인정보에 대해 개인정보 파기계획을 수립하고 개인정보 보호책임자의 승인을 받아 파기합니다.
2. 파기기한
   <의료기관명>은 다음과 같이 사유가 발생한 5일 이내에 해당 개인정보를 파기합니다.
   - <처리목적1>: 수집 · 이용에 관한 동의일부터(혹은 <해당 법령명, 조문번호>에 따른) <처리 및 보유기간> 이후 5일 이내
   - <처리목적2>: 수집 · 이용에 관한 동의일부터(혹은 <해당 법령명, 조문번호>에 따른) <처리 및 보유기간> 이후 5일 이내
   - 단, <해당 법령명, 조문번호>에 따라 개인정보를 계속 보존하여야 하는 경우에는 해당 개인정보를 별도의 데이터베이스(DB)로 옮기거나 보관장소를 달리하여 보존합니다.
3. 파기방법
   <의료기관명>은 전자적 파일형태의 개인정보는 기록을 재생할 수 없는 기술적 방법을 사용하며, 종이 문서에 기록 · 저장된 개인정보는 분쇄기로 분쇄하거나 소각하여 파기합니다.

27) 행정안전부(2011.12.), 전게서.

해서는 개인정보 보호법 제31조에 따라 지정한 개인정보 보호책임자의 성명, 직책, 연락처 등을 기재하는 것으로 그 외에 담당부서, 담당자 등을 기재하며 그 외에 개인정보 보호 담당부서 및 담당자 등을 기재하는 것도 권고하고 있다[28]. '개인정보 보호책임자 사항'을 게시한 43개 기관의 해당 내용을 분석해본 결과 일부기관에서는 책임자의 성명은 없이 직책만을 기재하고 있었으며 특히 인사이동에 따른 갱신이 제대로 이루어지지 않는 기관들이 있었다. <표 10>은 '개인정보 보호책임자 사항'에 대한 적절한 예시이다.

아홉 번째 '개인정보 처리방침 변경 사항'에 대해서는 개인정보 처리방침 시행일자, 변경이력을 게재하는 것으로써, 이전 방침이 있는 경우에는 링크서비스 등을 통해 정보주체가 이를 비교 · 열람할 수 있도록 할 것을 권고하고 있다[29]. '개인정보 처리방침 변경 사항'에 대해 40개 기관들의 게시내용을 분석해본 결과 이전 방침이 있는 경우 그 내용을 열람할 수 없는 경우가 많았다. <표 11>은 '개인정보 처리방침 변경 사항'에 대한 적절한 예시이다.

필수기재항목 중 마지막인 열 번째 '개인정보 안전성 확보조치 사항'에 대해서는 개인정보 보호법 제24조제2항, 제29조 및 시행령 제30조에 의한 사항을 기재하는 것으로 관리적, 기술적, 물리적 조치에 과한 내용을 가능한 자세히 기재토록 권고하고 있다[30]. '개인정보 안

**표 10. 개인정보 처리방침 기재항목 중 '개인정보 보호 책임자'에 대한 예시**

**<의료기관명>**은 개인정보 처리에 관한 업무를 총괄하여 책임지고, 개인정보 처리와 관련한 정보주체의 불만처리, 피해구제 등을 위하여 다음과 같이 개인정보 보호책임자를 지정하고 있습니다.

1. 개인정보 보호책임자
   - 성명: <개인정보 보호책임자 성명>
   - 직책: <개인정보 보호책임자 직책>
   - 연락처: <개인정보 보호책임자 연락처(전화번호, 이메일, 팩스번호 등)>
2. 개인정보 보호 담당부서
   - 부서명: <개인정보 보호 담당부서명>
   - 담당자: <개인정보 보호 담당부서 담당자>
   - 연락처: <개인정보 보호 담당부서 담당자 연락처(전화번호, 이메일, 팩스번호 등)>

정보주체께서는 **<의료기관명>**의 서비스를 이용하시며 발생한 모든 개인정보 보호 관련 문의, 불만처리, 피해구제 등에 관한 사항을 개인정보 보호책임자 및 담당부서로 문의하실 수 있습니다. **<의료기관명>**은 정보주체의 문의에 대해 지체 없이 답변 및 처리해드릴 것입니다.

28) 행정안전부(2011.12.), 전게서.
29) 행정안전부(2011.12.), 전게서.
30) 행정안전부(2011.12.), 전게서.

전성 확보조치 사항'을 게시한 40개 기관의 내용을 분석해본 결과 일부 기관들은 관리적, 기술적, 물리적 조치를 다 제시하지 않고 있었다. <표 12>는 '개인정보 안전성 확보조치 사항'에 대한 적절한 예시이다.

그 외 임의 기재항목으로 '정보주체 권익침해 구제방법'에서는 정보주체가 개인정보침해에 대한 구제를 받을 수 있도록 하기 위해 개인정보침해신고센터, 개인정보 분쟁조정위원회 등과 같은 개인정보 보호법에 따른 전문기관이나 대검찰청 사이버범죄수사단, 경찰청 사이버범죄수사단 등과 같은 수사기관을 안내토록 권

**표 11. 개인정보 처리방침 기재항목 중 '개인정보 처리방침 변경 사항'에 대한 예시**

이 개인정보 처리방침은 〈20XX.XX.XX〉부터 적용되며, 법령 및 방침에 따른 내용 추가, 삭제 및 정정 시 변경사항 시행 7일 전부터 공지사항을 통해 고지할 것입니다.
이 전의 개인정보 처리방침은 아래에서 확인하실 수 있습니다.

– 〈20XX.XX.XX ~ 20XX.XX.XX〉 적용 (클릭)
– 〈20XX.XX.XX ~ 20XX.XX.XX〉 적용 (클릭)
~

**표 12. 개인정보 처리방침 기재항목 중 '개인정보 안전성 확보조치 사항'에 대한 예시**

**〈의료기관명〉**은 개인정보의 안전성 확보를 위하여 다음과 같은 조치를 취하고 있습니다.

1. 관리적 조치
   – 내부관리계획 수립 및 시행
   – 개인정보 취급직원에 대한 정기적 교육: 〈주기〉
   – 정기적 자체 감사 실시: 〈주기〉
2. 기술적 조치
   – 정보주체 개인정보에 대한 암호화
   – 개인정보 처리시스템에 대한 접근통제를 위한 접근권한 관리 및 무단접근 통제를 위한 침입차단시스템 설치
   – 외부 해킹이나 컴퓨터 바이러스 등에 의한 개인정보 유출 및 훼손방지를 위한 보안프로그램 설치와 주기적인 갱신 · 점검
   – 개인정보처리시스템 접속기록에 대한 위변조 및 도난, 분실을 막기 위한 보안기능 사용 및 최소 6개월 이상 보관 · 관리
3. 물리적 조치
   – 개인정보가 포함된 서류, 보조저장매체 등은 잠금장치가 있는 안전한 〈장소〉에 보관
   – 〈장소〉에 대한 비인가자의 출입통제 절차 수립 및 운영

고하고 있다[31]. '정보주체 권익침해 구제방법'에 대해 게시하고 있는 32개 기관들의 내용을 분석해본 결과 대부분 권고하고 있는 내용을 담고 있었다. <표 13>은 '정보주체 권익침해 구제방법'에 대한 적절한 예시이다.

마지막으로 '개인정보 열람청구 접수 · 처리 부서' 항목은 임의기재항목으로 정보주체가 해당 기관에 개인정보 열람청구를 신청할 수 있는 부서명을 기재하는 것으로 그 외 안전행정부의 개인정보 보호 종합지원 포털 웹사이트를 통해서도 개인정보 열람청구가 가능함을 기재토록 권고하고 있다[32]. 43개 기관 중 5개 기관만이 게시하고 있었으나 권고하고 있는 내용 중 개인정보 보호 종합지원포털사이트에서 열람청구할 수 있다는 내용은 담고 있지 않았다. <표 14>는 '개인정보 열람청구 접수 · 처리 부서'에 대한 적절한 예시이다.

## 4. 시사점

본 분석결과에서 알 수 있듯이 우리나라 상급종합병원의 개인정보처리방침 수립 · 공개율은 100%이다. 그러나 각각의 해당 항목내용을 상세 검토해본 결과 관계법령에서 제시하고 있는 명칭사용, 기본원칙 및 개념 기술, 세부내용 기술에 있어 미흡한 점이 많이 나타났으며 일부 기관에서는 각 항목별 기본원칙 및 개념만을 기

**표 13. 개인정보 처리방침 기재항목 중 '정보주체 권익침해 구제방법'에 대한 예시**

정보주체는 **<의료기관명>**의 자체적인 개인정보 불만처리, 개인정보 침해에 대한 피해구제, 상담 등에 대해 만족하지 못하시거나 보다 자세한 도움이 필요하시면 아래 기관에 문의하여 주시기 바랍니다.

1. 개인정보 침해신고센터(한국인터넷진흥원 운영)
   - 소관업무: 개인정보 침해사실 신고, 상담 신청
   - 홈페이지: privacy.kisa.or.kr
   - 전화: (국번없이) 118
   - 주소: (138-950) 서울시 송파구 중대로 135 한국인터넷진흥원 개인정보침해신고센터
2. 개인정보 분쟁조정위원회(한국인터넷진흥원 운영)
   - 소관업무: 개인정보 분쟁조정신청, 집단분쟁조정(민사적 해결)
   - 홈페이지: privacy.kisa.or.kr
   - 전화: (국번없이) 118
   - 주소: (138-950) 서울시 송파구 중대로 135 한국인터넷진흥원 개인정보침해신고센터
3. 대검찰청 사이버범죄수사단: 02-3480-3573(www.spo.go.kr)
4. 경찰청 사이버범죄수사단: 1566-0112(www.netan.go.kr)

31) 행정안전부(2011.12.), 전게서.
32) 행정안전부(2011.12.), 전게서.

**표 14. 개인정보 처리방침 기재항목 중 '개인정보 열람청구 접수 · 처리 부서'에 대한 예시**

정보주체는 개인정보 보호법 제35조에 따른 개인정보의 열람 청구를 다음과 같은 부서에 할 수 있으며 **〈의료기관명〉**은 정보주체의 개인정보 열람청구가 신속하게 처리되도록 노력하겠습니다.

1. 개인정보 열람청구 접수 · 처리 부서
   - 부서명: 〈개인정보 보호 담당부서〉
   - 담당자: 〈담당자〉
   - 연락처: 〈개인정보 보호 담당자 연락처(전화번호, 이메일, 팩스번호 등)〉

또한 정보주체께서는 **〈의료기관명〉**의 **〈개인정보 보호 담당부서〉** 이외에도 안전행정부의 '개인정보 보호 종합지원 포털 사이트(www.privacy.go.kr)'를 통해 개인정보 열람청구를 하실 수 있습니다.

2. 안전행정부 개인정보 보호 종합지원 포털 → 개인정보 민원 → 개인정보 열람 등 요구

술하거나 혹은 기존에 배포된 사례집[33] 내용을 각자 기관에 맞게 수정하여 사용하지 않고 그대로 기술하는 등 공개율에 비해 충분성에 있어서는 만족할만한 수준을 나타내지 않고 있다. 더욱이 실제로 개인정보처리에 있어 공식적으로 표명하고 있는 이러한 처리방침과 실제 운영간에는 괴리가 크다는 것[34] 즉, 정확성이 떨어진다는 것도 감안한다면 현재 상급종합병원의 개인정보 처리방침은 충분성과 정확성 모두 현저히 미흡한 상황으로 우리나라 의료기관의 개인정보 처리방침에 대한 질적 수준은 제고의 여지가 있음을 나타내고 있다.

앞에서도 언급하였듯이 개인정보 처리방침은 개인정보처리자와 정보주체 모두에게 중요한 의미를 지니고 있고, 해당 기관의 개인정보 보호수준을 파악할 수 있는 지표로도 활용될 수 있어 이를 제대로 수립하고 공개하는 것은 개인정보 보호수준 향상을 위한 첫걸음이라 할 수 있을 것이다.

그러므로 각 의료기관에서는 항목별 제시한 예시를 기반으로 하여 개인정보처리방침을 제대로 수립하고 공개함으로써 의료기관 개인정보 보호수준 향상을 위한 첫걸음을 시작하는데 본 고의 의의를 두고자 한다. 또한 개인정보처리방침 질적 분석에 대한 선험적인 연구로서의 의의와 함께 향후 내용의 적절성과 충분성 즉 질적 수준을 보다 계량화하여 측정하기 위한 상세한 기준에 대해 진일보된 연구를 기대코자 한다. 보건복지

33) 행정안전부(2011.12.), 전게서.
34) 정찬모(2013), 전게서.