



저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:



저작자표시. 귀하는 원저작자를 표시하여야 합니다.



비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.



변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 [이용허락규약\(Legal Code\)](#)을 이해하기 쉽게 요약한 것입니다.

[Disclaimer](#)

碩士學位論文

의료기관의 개인정보 중요도와
활용도에 대한 IPA 분석

濟州大學校 大學院

經營情報學科

金聖訓

2019年 2月

의료기관의 개인정보 중요도와 활용도에 대한 IPA 분석

지도교수 김 근 형

김 성 훈

이 論文을 經營情報學 碩士學位 論文으로 提出함

2018年 12月

김성훈의 經營情報學 碩士學位 論文을 認准함

審査委員長 _____ (인)

委 員 _____ (인)

委 員 _____ (인)

濟州大學校 大學院

2018年 12月

An IPA Analysis on the Importance and Utilization of Personal Information in Medical Institutions

Sung Hun Kim
(Supervised by professor Keun-hyung Kim)

A thesis submitted in partial fulfillment of the requirement for the degree of Master of Management Information Systems

December 2018.

This thesis has been examined and approved.

.....
.....
.....

December 2018.
.....

Department of Management Information Systems

GRADUATE SCHOOL

JEJU NATIONAL UNIVERSITY

<제 목 차 례>

Abstract	vii
I. 서 론	1
1. 연구의 배경	1
2. 연구의 목적	2
II. 이론적 배경	4
1. 개인정보의 개념	4
2. 의료정보의 개념	5
가. 의료정보의 일반적 개념	5
나. 의료정보의 특성	7
3. 민감정보 및 고유식별정보	9
4. 개인정보 개념의 국제비교	9
가. OECD 프라이버시 가이드라인	10
나. EU 개인정보 보호지침	10
다. 미국의 HIPAA 프라이버시 규칙	11
라. 개인정보의 안전성 확보조치 기준	11
마. 유럽	12
바. 일본	13
5. 개인정보파일의 정의	13
6. 개인정보의 등급	14
7. IPA분석	16
8. 관련 연구 고찰	18
III. 연구방법	20

IV. 조사 분석	22
1. 데이터 수집 및 표준화	22
2. IPA 분석결과	26
V. 결론	29
참고문헌	31

<표 차 례>

<표 1> 의료정보 기술 발전 경과	6
<표 2> 개인정보파일의 등록 및 공개	14
<표 3> 개인정보 영향도 등급 표	15
<표 4> 기관별 개인정보파일 명칭	22
<표 5> 개인정보의 중요도와 활용도 데이터 원본 및 표준화	24
<표 6> 구간별 속성의 분포	28

<그림 차례>

<그림 1> IPA 매트릭스	18
<그림 2> 개인정보의 중요도 및 활용도에 따른 관리전략 모형	20
<그림 3> IPA 분석결과	27

<국문요약>

의료기관의 개인정보 중요도와 활용도에 대한 IPA 분석

개인정보 보호의 중요성은 아무리 강조해도 지나치지 않으며, 환자 개인정보의 보호에 대한 사회적 요구가 증가하고, 의료기관은 환자의 건강상태 정보, 진료정보, 병력, 민감정보, 주민등록번호 등 관련법에 따라 개인정보를 수집하고 있으며, 그 밖에 신용카드번호, 통장계좌번호, 근로정보, 개인영상정보 등 다양한 개인정보를 처리하고 있다. 국내 의료기관은 의료서비스 질 향상, 의료정보시스템, 의료진의 효율적 환자관리 업무흐름 개선, 영상 및 검사의 판독업무 위탁, 학술연구 및 통계작성, 병원 간 진료정보 교류 등 개인정보는 다양하게 활용하고 있다.

개인정보의 유출로 인하여 환자 및 의료기관 근로자는 자신의 개인정보 자기결정권을 침해받고, 유출된 개인정보로 인하여 2차적 피해를 받게 될 뿐 만 아니라, 생명·신체에 대한 위협 및 재산상의 손실, 사회적 평가저하 등 다양한 불이익을 받을 수 있다.

이를 위하여 본 논문에서 제안하는 방법을 효과적으로 수행하기 위해 개인정보 항목의 데이터 수집은 「행정안전부 개인정보보호 종합지원시스템 [<https://intra.privacy.go.kr>]에 등록된 기관별 개인정보파일 중 5개의 국립대학교 병원을 기준으로 개인정보파일 명칭의 공통 개인정보 항목 61개를 조사 하였다. 산출된 개인정보 항목 61개는 ‘개인정보보호법’ 개인정보영향평가의 개인정보영향도 등급표를 활용하여 개인정보의 중요도 등급을 측정하였다.

개인정보 항목의 분류는 15개의 속성(고유식별정보, 민감정보, 인증정보, 신용정보, 금융정보, 의료정보, 위치정보, 기타 중요정보, 개인식별정보, 개인관련정보, 기타 개인정보, 자동생성정보, 가공정보, 제한적 본인 식별정보, 기타 간접 개인정보)으로 분류하고 수치범위는 동일범위로 축소하고 표준화 하여 IPA분석을 진행하였다.

본 연구의 IPA분석 결과에 대한 시사점은 다음과 같다. 첫째, IPA분석의 1사분

면에 위치한 개인정보의 중요도가 높고 활용도가 낮은 개인정보 항목을 중점 개선해야 한다. 의료정보의 경우 학술연구 및 통계작성, 병원 간 진료정보 교류, 제 3자 기관에 개인정보를 제공하기 때문에 자칫 개인정보 담당자 및 취급자들이 개인정보의 중요도 및 활용도를 낮게 측정하여 당초 수집 목적의 범위를 초과하여 이용 및 제공하거나 실무에 적용할 우려가 있어 제공되는 정보에 따라 개인정보 활용시 분실·도난·유출·위조·변조되지 않도록 더 철저한 관리가 필요하며, 개인정보의 활용도는 높여, 개인정보는 안전장치를 강화하여 훨씬 더 두텁게 보호해야 한다.

둘째, 개인정보 중요도 등급이 높다고 활용도가 높은 것은 아니며, 중요도와 관계없이 개인정보의 활용도는 다양한 분포를 나타냈다. 이러한 분포는 개인정보를 수집·이용·제공 하면서 시급한 노력의 투입이 필요 없는 영역이라고 판단할 수도 있으나, 이론적 배경에서도 언급되었듯 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 활용되거나, 의료기관의 개인정보 유출 및 오·남용으로 인하여 생명, 신체에 대한 위협 등을 생각한다면 개인정보 담당자 및 취급자는 보다 신중하게 해석할 여지가 있으며, 적절한 내부통제시스템 구축 및 운영을 위해 노력해야 한다.

<Abstract>

An IPA Analysis on the Importance and Utilization of Personal Information in Medical Institutions

The importance of personal information protection cannot be overemphasized, social demand for protection of patient personal information is increasing, and the medical institution collects personal information according to relevant laws such as patient health status information, medical care information, history, sensitivity information, and resident registration numbers, and handles various personal information such as credit card number, account number, work information, and personal image information. The domestic medical institution utilizes diverse personal information such as improvement of the quality of medical services, improvement of the medical information system, efficient flow of patient care, consignment of reading work for images and examinations, preparation of academic research and statistics, and exchange of medical information between hospitals.

The leakage of personal information violates the right to self-determination of personal information, secondary damages caused by personal information leaked, and a variety of disadvantages such as threats to life and body, property loss, and social degradation.

To carry out the methods proposed in this paper effectively, the data collection of personal information items was examined in 61 common items of personal information file names based on hospitals at national universities among the five personal information files registered in the Comprehensive Support System for Personal Information Protection by the Ministry of Public Administration and Security[<https://intra.privacy.go.kr>]” The 61 items of personal information calculated were measured by utilizing the privacy impact rating scale of the Personal Information Protection Act.

The classification of personal information items was divided into 15 attributes (unique identification, sensitive information, authentication information, credit information, financial information, medical information, location information, other important information, personal identification, personal information, other personal information, automatic generation information, processing information, limited identification information, and other indirect personal information) and the IPA analysis was performed by reducing the scope to the same scope.

The implications for the IPA analysis results of this study are as follows. First, the items of personal information that are located in the first quadrant of the IPA analysis should be significantly improved, with high importance and low utilization. As medical information provides academic research and statistics, exchange of medical information between hospitals, and personal information to third-party organizations, it is necessary to thoroughly manage and enhance the level of personal information utilization so that it is not lost, stolen, leaked, falsified, or manipulated in the event of the information provided to personal information utilization, as the importance and utilization of personal information is lowered by personal information staff and the users of the information is likely to be used beyond the scope of the original collection purpose, or applied in practice.

Second, the degree of importance of personal information does not mean that it is highly utilized, and utilization of personal information regardless of its importance has been shown to be diverse. Such distribution can be judged to be an area in which urgent efforts are not required to collect, use or provide personal information, but, as stated in the theoretical context, it is possible for personal information personnel and handlers to be interpreted more carefully, considering threats to life and body due to personal information leakage and misuse by medical institutions, and to make efforts to establish and operate appropriate internal controls and systems.

I. 서론

1. 연구의 배경

2012년 IBM은 매일 15페타바이트(PB, 1015Bytes)의 양으로 새로운 정보가 생산된다고 발표하였고, 2018년 초 데이터플로크(Dataflog)사는 일평균 약 2.5엑사바이트(EB, 1018Bytes)의 정보가 생산되고 있는 것으로 추산했고, 매일 생산되는 데이터가 2제타바이트(ZB, 1021Bytes)까지 도달한다(<http://ieic.kdi.re.kr>). 가히 폭발을 넘어 데이터 빅뱅 수준이며, 그렇게 생산·축적된 데이터를 이용해 비즈니스를 영위하고, 발전된 ICT 기술에 의해 데이터가 재 생성되고, 데이터와 데이터가 결합해 새로운 정보·지식을 만드는 시대, 4차 산업혁명 시대, 미래 산업의 원유가 바로 데이터이다(<http://ieic.kdi.re.kr>).

의료기관도 4차 산업의 주요 기술인 클라우드, 인공지능, 빅데이터 기술 등 새로운 도전에 직면하고 있으며, 디지털 환경에서 생성되는 데이터로 그 규모가 방대하고 생성 주기도 짧으며 형태도 수치 데이터 뿐 아니라 문자와 영상 데이터를 포함하며 정보유통 속에서 개인정보의 유출 사고는 지속적으로 증가하고 있다. 국민건강보험공단, 건강보험심사평가원 등 보건의료 공공기관 4곳의 데이터 양식을 통일해 공익 목적에 한해 가공·익명정보를 민간에 개방한다고 밝혔으나, 시민단체는 개인 건강정보가 민간기업에 넘어가는 과정에서 돈벌이 수단으로 변질되거나 개인정보 유출 위험이 커질 수 있다고 우려를 제기하고 있다 (www.etnews.com).

즉, 개인정보가 제공될 때 보안 핵심요소인 정보의 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)을 동시에 만족시키기 위해서는 제공되는 자료가 충분한 활용가치가 있으면서도 개인정보 노출의 최소화를 위해 기술적, 관리적 조치가 수반되어야 한다(박철현 등, 2015). 악성코드, 해킹 등 고유식별정보, 의료정보, 민감정보 등 사이버침해사고가 증가하고 있으며, 환자의 개인정보 처리 단계별 개인정보 수집·이용·제공 단계에서 수집된 개인정보의 중요도 등급에

따라 IPA 분석을 하고자 한다. 개인정보의 중요도 등급은 ‘개인정보영향평가 가이드’의 개인정보 영향도 등급표를 참조하였으며, 등급은 3단계(1 ~ 3등급)로, 자산가치(5, 3, 1)의 값을 정하여 15가지 항목분류로 산출하였다(행정안전부 개인정보 영향평가 수행 안내서, 2018). 자산가치 기준으로 개인정보를 관리하고 있으나 활용도는 전혀 고려하고 있지 않다.

개인정보의 활용도는 5개의 국립대학교병원에서 수집된 개인정보 중 개인정보보호법 제32조에 의해 등록·공개된 ‘행정안전부 개인정보보호종합지원시스템’에서 확인할 수 있다(<https://intra.privacy.go.kr>).

행정안전부 2013 ~ 2017 개인정보 실태점검 및 행정 처분 사례 중 공공기관은 개인정보파일의 명칭, 운영근거 및 목적, 기록되는 개인정보 항목, 처리 방법 및 보유기간 등의 개인정보파일 등록사항 공개가 이루어지지 않아 개인정보파일 등록 및 공개위반에 따라 개인정보보호법 위반에 해당사례가 있으며, 개인정보의 활용도는 점차 증가하고 있다(행정안전부 개인정보실태점검 및 행정처분 사례집, 2018). 특히 활용도가 많은 개인정보는 정보주체의 동의를 받거나, 법률의 규정, 공공기관의 법령에서 정한 소관업무 이행, 정보주체의 생명·신체·재산의 이익보호 외에는 기관 외 제공해서 활용할 수 없기 때문에 기관에서 수집·이용 중인 개인정보는 대장기록에 잘 관리될 필요가 있으며 개인정보의 중요도와 활용도에 따른 시사점을 도출하기 위하여 IPA분석 모형을 사용한다.

2. 연구의 목적

국내 의료기관은 의료서비스 질 향상, 의료정보시스템, 의료진의 효율적 환자 관리 업무 흐름 개선 및 병원 간 진료정보 교류를 위하여 개인정보는 다양하게 활용되고, 개인정보 보호의 중요성은 아무리 강조해도 지나치지 않으며, 환자의 개인정보 보호에 대한 사회적 요구가 증가하고 있다.

의료기관에서 취급하는 개인정보는 이름, 주소, 전화번호, 주민등록번호, 계좌번호, 얼굴 이미지나 사진, 개인 특이사항 등 개인식별정보는 기본이다. 여기에 질병이나 부상에 대한 예방정보, 진단 및 치료 정보, 재활과 출산, 사망, 건강검진에 관한 건강정보, 근로정보 등 다양한 여러 개인정보를 처리하고 있다. 개인

정보의 유출로 인하여 환자 및 의료기관 근무자는 자신의 개인정보 자기결정권을 침해받고, 유출된 개인정보로 인하여 2차·3차적 피해를 받을 수 있으며 생명 및 신체, 정신적 위협 뿐 아니라 사회적 평가저하, 재산상의 손실 등 다양한 불이익을 받을 수 있다. 개인정보유출로 인한 온라인에서의 피해가 발생하면 회복이 어려울 뿐 아니라 온라인 게시판 및 SNS 등으로 전달됨으로써 피해가 '실시간'으로 발생할 수 있다는 특성이 있으며 개인정보 유출의 근원을 확인하는데 많은 인적·물적 자원이 소모되기도 한다.

본 논문에서는 개인정보의 중요도와 활용도와의 관계를 IPA분석 기법으로 살펴보고자 한다. 중요도가 높고 활용도가 높은 개인정보가 어떤 유형인지, 중요도가 높고 활용도가 낮은 개인정보가 어떤 유형인지, 중요도가 낮고 활용도가 높은 개인정보가 어떤 유형인지, 중요도가 낮고 활용도가 낮은 개인정보가 어떤 유형인지를 분석하고자 한다. 이를 바탕으로 개인정보를 더 정교하게 관리하기 위한 방안에 대한 시사점을 도출하고자 한다.

II. 이론적 배경

1. 개인정보의 개념

개인정보보호법은 개인정보보호를 위한 법체계를 일원화하고 개인의 권익 보호를 강화하기 위한 일반법으로서 2011년 3월 29일 제정되어 동년 9월 30일부터 시행되었다. 이 법은 개인정보의 수집·유출·오용·남용으로부터 사생활의 비밀 등을 보호함으로써 국민의 권리와 이익을 증진하고, 나아가 개인의 존엄과 가치를 구현하기 위하여 개인정보 처리에 관한 사항을 규정함을 목적으로 한다(<http://www.law.go.kr>).

개인정보보호법은 적용대상 주체에 있어 개인정보를 처리하는 공공부문의 모든 개인정보처리자를 대상으로 하며, 민간처리자 까지 확대하고, 관리정보도 전자정보 외 수기문서 등 모든 정보를 포괄함으로써 전에 없던 정보보호의 사각지대를 해소하였다는 점에서 큰 의미를 가지며 개인정보보호에 관한 일반원칙을 제시하고 개인정보의 수집·이용 및 제공·파기라는 단계적 처리절차를 규율하고 있다는 점도 동 법에서의 중요한 성과라 할 수 있다(박지용, 2012).

‘개인정보보호법’에서의 ‘개인정보’는 살아 있는 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 포함한다.) 또한 ‘정보통신망 이용촉진 및 정보보호 등에 관한 법률’에서는 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보로서 유사한 정의를 하고 있다(<http://www.law.go.kr>).

이러한 법의 개념들을 종합해 보면 ‘살아있는’, ‘생존하는’ 개인 식별정보라 해석 할 수 있고 생존하고 있는 자연인에 관한 정보이어야 하며, 법인이나 단체에 관한 정보는 원칙적으로 개인정보에 해당하지 않으며, 사자(死者)에 관한 정보는 개인정보에 해당하지 않는다. 다만 사망자의 정보가 사망자와 유족과의 관계를 나타내는 정보이거나 유족 등의 사생활과 연관된 경우에는 개인정보에 해당될

수 있다(<http://www.law.go.kr>).

2. 의료정보의 개념

가. 의료정보의 일반적 개념

현행 의료법에서는 의료행위에 대한 개념정의를 명시하고 있지 않다. 다만, 의료인은 업무를 수행함으로써 국민보건 향상을 이루고 국민의 건강한 생활 확보에 이바지할 사명으로 한다고 규정(의료법 제2조 제2항)함으로써 의료 행위가 위의 기능을 담당하고 있음을 알 수 있을 뿐이다.

협회의 의료행위는 행위의 주체가 의사의 범위에 속하는 자의 행위이어야 하고, 행위의 내용이 사회적으로 의료인의 행위라고 인정되는 것이어야 하며, 그 행위의 대상이 환자이어야만 한다(<http://www.law.go.kr>). 우리나라 의료기관에 정보화가 도입되기 시작한 시기는 의료보험이 실시된 시기와 비슷하며(전기홍, 조우현, 1994) 1990년대 접어들면서 시스템 도입이 급격하게 증가하게 되었다.

정영철 등(2013)은 건강보험심사평가원에서 실시한 요양기관 정보화 실태조사 결과에 따르면, 우리나라 전국 종합병원 및 병원의 정보화 현황은 처방전달시스템(OCS)의 경우, 1999년 종합병원에 대한 도입현황이 50% 못 미치던 것이 2010년에는 94%로 대부분의 종합병원에서 사용하고 있었다. 전자의무기록시스템의 경우에도 1999년 미미한 현황에서 2010년에는 종합병원의 60%대, 병원의 50% 가까이 도입하여 사용하는 등 현저히 증가함을 나타내고 있다(정영철 등, 2013). 상대적으로 개인정보 유출 및 정보보안의 문제를 많이 초래할 수 있을 것으로 판단되며, 이것은 기관에서 의료정보시스템을 직접운영 보다 위탁관리에 의존하는 비율이 높다는 것이다.

이처럼 의료정보시스템 사용율이 높아지면서 대규모 전산화가 이루어지고 의료기관의 근무자 뿐 아니라 외부인의 접근이 수반되어 웹 및 모바일 환경의 확대, u-health care, PaaS, 빅데이터 등 IT기술이 발전하면서 의료정보에 대한 접근성과 이동성이 증가하고, 개인 의료정보에 대한 침해, 유·노출의 위험은 점점 더 증가하고 있다. 실제로 미국에서는 2009년 이후부터 서터메디컬재단 및 서터

피지션 서비스 이용 고객의 환자 의료정보 유출을 포함해 미국 내에서 약 600여 건의 유출사건이 일어나 2,200만명의 피해자가 발생하였다고 하며, 우리나라에서도 의료기관 및 관련기관에서 환자개인정보에 대해 불법적인 수집, 환자의 동의 없이 진료목적 이외의 사용 및 제3자 제공, 개인정보의 안정성확보조치 미흡에 따른 의료정보의 소홀한 관리로 인한 환자정보 유출, 내부 개인정보취급자 및 협력사에 의한 고의적인 환자정보 유·노출 사건이 지속적으로 발생되고 있다(정영철 등, 2013).

한편, 행정안전부가 개인정보보호법 시행이후 2012년도에 실시한 총47회 756개소에 대한 현장점검 결과, 과태료 57건, 시정조치 360건등 총 441건의 행정처분이 부과되었으며 이중 의료업의 경우에는 위반비율이 52.4%로 타 분야보다는 낮게 나타났으며, 의료·보건 분야에서의 주요 위반내용으로는 개인정보 동의시 필수 고지사항 누락, 고유식별정보 별도동의 위반, 개인정보보호책임자 미지정, 접근권한관리 의무위반 등으로 나타났다(정영철 등, 2013). 개인의료정보의 전산화로 의료기관 및 환자 모두 편리해졌지만 병의원 및 약국 등에서 민감한 의료정보를 다량 보유하게 되면서 개인정보의 대량 노출 가능성과, 희소성 및 활용성이 높아졌다.

[표1] 의료정보 기술 발전 경과(참고 : 비트컴퓨터)

년도구분	병원급 의료기관		의원급 의료기관	
	기능	제품	기능	제품
70년대 후반	진료비 수납 및 의료보험 청구	원무관리시스템 (HIS)		
80년도 초반			의료보험청구 전산화	청구 프로그램
80년대 후반			회원관리/환자 관리	의원관리프로그램
90년대 초반	병원내 Slip 전산화	처방전달시스템 (OCS)		

90년대 후반	의료영상의 전산화	의료영상정보 전송시스템 (PACS)	환자마케팅 정보화	환자마케팅지 원프로그램 (CRM)
00년대 초반	병원 내 차트 전산화	전산의무기록 (EMR)		
2010년대 ~	스마트병원, 모바일병원, 유헤 스케어, 원격의료, 개인정보보 호 및 보안		개인정보보호 및 보안, 원격의 료	

나. 의료정보의 특성

이상목(2007)은 각 의료기관별로 의료정보시스템을 구축함에 따라 의료정보는 대부분 전자적인 형태로 보관되기 때문에 과거에 종이문서로 보관될 때와 비교하여 더 많은 업무관련 내부 개인정보취급자 및 파견 근무자, 협력사 등 정보에 접근할 수 있게 되었다. 이한주(2012)는 직접적으로 의료기관에서 의료행위를 하는 의사, 간호사, 의료기사는 환자의 진료와 관련 있는 근무자는 당연히 정보주체의 환자 의료정보에 대한 접근권한과 이용이 가능하다. 그 외에도 원무수납·보험심사·입원관리 분야에서 여러 개인정보취급자가 있으며, 본인의 업무와 관련하여 개인정보취급자로서 의료정보에 대한 접근권한 및 이용이 가능하고, 심지어 의료정보(전산) 담당자도 환자와의 직접적인 관련성은 없다 하더라도 본인의 업무범위 내에서 개인별·부서별 접근권한에 따라 의료정보에 대한 이용이 가능한 것으로 해석할 수 있다(이한주, 2012). 의료기관 근무자는 대부분의 개인정보취급자로 분류되며, 의료정보시스템은 공공·연구기관, 의료장비와 데이터가 연동되는 경우가 많고 보안프로그램 운영 및 미설치 기관이 많아 개인정보 안정성확보조치에 만전을 기해야 한다. 환자의 입장에서는 선택적으로 동의 여부를 결정하는 것은 현실적으로 불가능하므로 본인의 의사와 관계없이 의료정보에 대한 침해가 발생할 수 있고 의료기관 종사자에 대하여 본인의 업무 범위 내에서 정보에 대한 접근권한 및 이용이 가능해야 하고, 통제할 수 있는 내부규정 및 지침 또는 개인정보보호 내부관리계획 등 규율할 수 있는 안전장치가 반드시 마련되어야

한다(이한주, 2012).

개인정보보호법(제18조)에 따라 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공할 수 있다(<http://www.law.go.kr>). 그 외에도 동법(제15조)에서 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우, 국민건강보험공단에게 급여비용 심사·지급·대상여부 확인 등을 위한 경우, 의료기관으로부터 자동차보험진료수가를 청구 받은 보험회사 등이 의료기관에 대하여 관련 기록을 청구하는 등의 경우에는 정보주체의 동의와 관계없이 법률의 규정에 의해 제3자에게 제공할 수 있게 되어 제공 받은 기관(제3자)은 제공 받은 목적의 범위 내에서 이용할 수 있다(<http://www.law.go.kr>).

이한주(2012)는 일반 개인정보와의 결합 하는 경우 의료정보는 전문적인 지식·기술·경험 등을 바탕으로 생성되지만, 이러한 정보들로만 구성되는 것은 아니다. 이는 결국 의료정보를 어떻게 볼 것인가의 문제와 관련 있는데, 최소한 성명, 주민등록번호와 같이 본인임을 식별할 수 있는 정보와 결합될 경우 의료정보로 인정할 수 있다. 또한 주소, 전화번호, 직장, 경력 등의 정보를 결합하여 본인임을 식별할 가능성이 있는 정보에 대해서도 의료정보를 인정할 수 있다. 따라서 의료정보는 전문성을 지닌 의료정보와 본인을 식별하거나 할 수 있는 개인정보와의 결합을 통하여 생성된다고 할 수 있다. 의료정보 침해의 문제는 정보주체의 의료와 관련된 정보만의 문제가 아니라 이는 결국 일반 개인정보에 대한 침해도 가져올 수밖에 없으며, 반대로 일반 개인정보에 대한 침해를 통해서도 의료정보에 대한 침해가 가능할 수 있으므로 침해의 위험성이 증가한다.

이한주(2012)는 전문 의료지식과 경험, IT기술과 결합하는 의료정보는 정보주체(환자)의 일반정보, 문진·검사 등을 통한 진료정보 등과 의료인의 전문적인 지식과 경험이 결합하여 생성된다. 환자에게 정보주체성이 인정된다는 점에서는 의견이 일치되지만, 의사 등 의료인 또는 의료기관에 대해서 정보주체성을 인정할 수 있는지의 문제에 대한 검토가 필요하다(이한주, 2012). 또한 개인정보보호법(제18조)에 따라 의료인 및 연구자 등이 정보주체로부터 별도의 동의를 받은 경우 학술연구 등의 목적으로 의료정보를 이용하여 새로운 결과물(정보)을 완성한 경우에, 정보주체가 본인의 정보를 이용했음을 이유로 새로운 정보가 본인에게

귀속된다고 주장하거나 동의의 철회를 통하여 학술연구의 결과물에 대한 효력을 부정하는 것은 문제가 있다(이한주, 2012). 특히 새로운 정보가 경제적인 목적으로 이용될 경우 원 정보를 제공한 정보주체에 대해서 지분권을 인정할 수 있는지에 대해서는 의문이다(이한주, 2012).

3. 민감정보 및 고유식별정보

현행 개인정보보호법제에는 개인정보와 유사한 개념을 함께 사용하고 있다. 이를 인식하지 하지 못한 채 개인정보의 개념을 사용할 경우 개인정보의 개념을 둘러싼 혼란이 더욱 가중될 수 있다.

개인정보보호법은 개인정보 외에 민감정보와 고유식별정보라는 개념을 따로 두고 있다. 여기서 민감정보는 “사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령이 정하는 정보”(개인정보보호법 제23조)를 의미하며, 동법 시행령 제18조는 유전자검사 등의 결과로 얻어진 정보와 범죄경력 자료에 해당하는 정보를 민감정보로 분류하고 있다. 한편 고유식별정보는 “개인을 고유하게 구별하기 위하여 부여된 식별정보”(개인정보보호법 제24조)를 의미하며, 동법 시행령 제19조는 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호를 고유식별정보로 분류하고 있다.

개인정보 정의에 따르면, 민감정보는 개인정보의 일종이지만 고유식별정보는 개인정보의 구성요소일 뿐이다. 민감정보 및 고유식별정보는 개인정보 중에서도 정보주체의 사생활을 현저히 침해할 우려가 큰 정보이기 때문에 특별히 잘 관리할 필요가 있다. 개인정보처리자는 민감정보나 고유식별정보를 원칙적으로 처리할 수 없으며, 정보주체에게 내용을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우 또는 법령에서 처리를 요구 또는 허용하는 경우에 한하여 처리할 수 있다(개인정보보호법 제23조 및 제24조).

4. 개인정보 개념의 국제비교

국내외 개인정보보호 관련 법·제도는 내용과 효력, 그리고 적용범위에 있어 점차 강화되고, 확대되고 있으며 자국 내 뿐 아니라 국제적인 교류에 있어서도 상호 적용되는 추세이다(정영철 등, 2013). 또한 의료정보 보호에 대해서는 의료분야 특성에 맞추어 의료정보 보호의 중요성이 더욱 더 부각되어 의료정보 제공자의 관리책임성 강화, 정보주체의 자기정보에 대한 권리 강화 추세가 반영되고 있으며 통합(omnibus)방식의 법률체계에서도 고시, 지침 등을 통해 점차 상세 규정화하고 있다(정영철 등, 2013).

가. OECD 프라이버시 가이드라인

OECD는 1980년 ‘프라이버시 및 국가간 개인정보 이전에 대한 가이드라인(Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 이하 프라이버시 가이드라인)’을 제정하였으며, 가이드라인은 개인정보 수집 및 관리에 관한 국제사회의 일치된 의견을 수렴하여 반영한 것으로 OECD 회원국은 물론, 세계 각각의 개인정보 관련 법률과 지침 개발을 위한 기초자료로 활용되어 오고 있다(<http://www.itfind.or.kr>). 이는 개인정보보호와 관련하여 국제조직 차원에서 관심을 가지고 추진한 최초의 노력이라 할 수 있다.

OECD 프라이버시 가이드라인은 수집제한의 원칙, 정보내용 정확성의 원칙, 목적 명확성의 원칙, 이용제한의 원칙, 안전성 확보의 원칙, 공개의 원칙, 정보주체 참여의 원칙, 책임의 원칙 등 모두 8개 원칙으로 구성되어있으며 1980년 처음 제정된 이후 2008년 개정되었고, 2013년 7월11일 OECD 이사회에서 개정안을 채택하였다(정영철 등, 2013).

나. EU 개인정보 보호지침

EU 개인정보 보호지침은 1995년 10월 EU 회원국 시민들의 기본권과 자유, 특히 개인정보 처리와 관련된 개인의 프라이버시를 보호하기 위해 ‘개인정보 처리에 관한 개인의 보호 및 해당 데이터의 자유로운 이동에 관한 95/46/EC 지침(이하 개인정보 보호지침)’을 채택하였다(김기열, 2010). 이러한 지침(directive)은 회

원국들을 대상으로 적용되는 EU 차원의 최초 입법형식으로 정보처리자의 의무, 정보주체의 권리, 제3국으로의 정보이전 금지, 독립기구 설치 등을 주요 내용으로 구성하고 있다(전은정 등, 2012).

다. 미국의 HIPAA(Health Insurance Portability and Accountability Act) 프라이버시 규칙

전은정 등(2012)은 미국의 공공부문의 개인정보보호를 위하여 1974년 프라이버시법(Federal Privacy Act)을 제정하였으나, 민간부문에서 발생하는 개인정보의 침해 방지를 위한 일반법은 제정하지 않고 있으며, 윤리적인 통제만 가능하다. 영역별로 보호의 필요가 있을 때마다 개별법을 제정하여 대처하고 있고, 미국 프라이버시법상 규율대상은 개인기록(record)이다(전은정 등, 2012).

다른 국가와 달리 개인정보보호를 위해 프라이버시법과 더불어 공공, 금융, 통신, 의료, 등 영역별 별도의 개별 법률을 마련하고 있다.(김기열, 2010). 그 중에서 의료와 관련해서 개인정보보호를 위해서는 1996년 연방의회에서 제정된 ‘의료보험의 이전과 그에 수반하는 책임에 관한 법률(Health Insurance Portability and Accountability Act, 이하 HIPAA)인 개별법에서 다루어지고 있다(김동수, 김민수, 2006). HIPAA 프라이버시 규칙은 전자적 형태 혹은 종이기반 형태 모두 적용되며 이에 포함된 환자의 권리는 프라이버시 관행에 대한 통지권, 열람접근권, 정정청구권, 공개내역 수급권, 제한요청권, 비밀 의사소통 요청권 등이 있다(김동수, 김민수, 2006).

미국 정부는 ‘건강보험책임법’이라 불리우기도 하고, 의료서비스 제공자와 건강보험 민원을 처리하는 기관간의 책임을 명확히 하고, 사고 발생시 보건부(HHS)에 보고토록 하고 있다(정영철 등, 2013).

라. 개인정보의 안전성 확보조치 기준

‘개인정보의 안전성 확보조치 기준(행정안전부고시 제2016-35호, 개정)’은 개인정보보호법 제23조(민감정보의 처리 제한), 제24조(고유식별정보의 처리 제한) 및

제29조(안전조치의무)와 동법 시행령 제21조(고유식별정보의 안전성 확보 조치) 및 제30조(개인정보의 안전성 확보 조치)에 따라 개인정보처리자가 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성을 확보하기 위한 세부적인 기준을 정하고 있다(<http://www.law.go.kr>).

이와 같은 ‘개인정보의 안전성 확보조치 기준’은 목적, 정의, 개인정보 내부관리 계획의 수립 및 시행, 접근 권한의 관리, 접근통제, 개인정보의 암호화, 접속 기록의 보관 및 점검, 악성프로그램 등 방지, 관리용 단말기의 안전조치, 물리적 안전조치, 재해·재난 대비 안전조치, 개인정보의 파기와 같이 13개의 조와 부칙으로 구성되어 있다(<http://www.law.go.kr>).

마. 유럽

문재완(2016)은 유럽 국가의 개인정보보호법은 1995. 10. 24. 제정된 개인정보보호지침(Directive 95/46/EC, 이하 ‘정보 보호지침’이라 한다)에 기초하고 있다. 정보보호지침에 따라 영국은 1998년 개인정보보호법(Data Protection Act 1988)을 제정하였으며, 프랑스는 1978년 개인정보보호법(Loi n° 78-17 du 6 janvier 1978)을 2004년 개정하고, 독일은 연방정보보호법 (Bundesdatenschutzgesetz, BDSG)을 2001년 개정하였다.

정보보호지침은 EU가 출범하기 전에 만들어 졌으며, 당시는 유럽 시장의 통합과 조화를 중시하는 분위기였기 때문에 개인정보의 처리와 자유로운 유통의 목적으로 제시되었고, 정보보호지침은 개인정보 보호를 국가 차원이 아닌 유럽공동체 차원에서 추진하였다는 점에서 그 의미가 크다(문재완, 2016). 문재완(2016)은 유럽연합(EU) 개인정보보호법의 특징은 첫째, 공공부문과 민간부문에 모두 적용되는 옴니버스 체제(omnibus regime)이고, 둘째, 개인정보의 처리를 적법하게 하는 체제(legitimizing regime)다. 달리 말하면, 법에서 정한 원칙과 기준을 준수할 경우 개인정보의 처리가 허용 되지만, 그렇지 않을 경우 개인정보의 처리는 금지된다. 셋째, 권리에 기초한 체제(right-based regime)이며, 정보주체에게 구체적인 권리를 부여하고 있다. 넷째, 유럽연합 회원국뿐 아니라, 비회원국에게도 영향력이 큰 체제(extraterritorial impact of the EU regime)다. 개인정보의 제3국 이

전을 규제하고, 제3국의 개인정보 보호수준을 EU집행위원회가 평가함으로써 EU 개인정보보호법이 우월적 지위를 차지한다.(문재완, 2016).

바. 일본

일본은 개인정보 침해 사례가 늘어나자 OECD의 프라이버시 가이드라인과 EU의 개인정보보호지침을 참고하여, 개인정보보호의 일반법으로 ‘개인정보의 보호에 관한 법률’을 2003년 제정, 2005. 4월부터 시행하고 있다(전은정 등, 2012). 일본의 경우처럼 기본법과 일반법의 이층구조의 법률은 매우 드문 형태이다. 일본의 개인정보보호법제는 기본법적 방식에 관해서는 옴니버스 방식을, 일반법적 부분에 있어서는 세그먼트 방식을 취하여 양자의 성격이 포함된 절충적인 형태라 하겠다(전은정 등, 2012).

5. 개인정보파일의 정의

국내 법에서의 ‘개인정보파일’이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말하며, 개인별 업무분장 또는 정보시스템에서 처리하는 단위업무 수준이며, 데이터베이스 기준이 아니다(<http://www.law.go.kr>). 기관의 업무를 추진하기 위해 수집한 개인정보를 집합물의 형태(개인정보파일)로 생성, 보유, 이용·제공, 파기 등을 하는 행위이며, 개인정보의 열람, 정정·삭제 및 처리정지 요청 등 정보주체의 권리 보장을 위해 공공기관이 보유한 개인정보파일은 개인정보 변경 시 정비 또한 필요하다.

개인정보파일을 등록, 관리하고 있는 내용은 궁극적으로 개인이 등록 된 내역을 쉽게 확인할 수 있도록 공개하는 것이 필요하기 때문에 정보주체(개인)는 자신에 관한 개인정보가 어느 공공기관에서 어떠한 형태의 개인정보파일에 포함되어, 어떻게 관리되고 있는지를 확인하고 이를 통하여 열람 및 정정 등을 요구할 수 있다(<http://www.law.go.kr>).

개인정보파일의 경우 이용목적에 따라 1차적으로 환자의 건강을 유지·증진하

려는 목적에 이용하는 것으로 모든 정보 제공이 원칙이며, 예외적으로 필요 최대한의 정보를 제공하며, 2차적으로 이용하는 경우 보험청구, 교육 및 연구, 병원관리 목적, 수사기관이나 공공기관에서 특수목적을 위해 사용된다. 보험청구의 경우 정보주체의 동의 없이 정보제공 가능하며, 교육 및 연구는 원칙적으로 정보주체(환자) 동의가 필요하다. 병원 운영관리 측면에서 환자관리, 의료기관 경영관리, 의료기관 질관리, 병원 인증평가 등 목적으로 이용된다.

[표2] 개인정보파일의 등록 및 공개

개인정보파일의 등록 및 공개	공공기관의 장이 개인정보파일을 운용하는 경우 행정안전부장관에게 등록 여부 확인
	공공기관의 장은 개인정보파일 운용을 시작한 날부터 60일 이내 등록 신청 여부 확인
	개인정보파일의 보유·파기 현황을 주기적으로 조사하는지 여부 확인

참고 : <https://intra.privacy.go.kr>.

6. 개인정보의 등급

개인정보의 중요성은 자산의 가치, 중요도 및 중요도 등급, 식별성, 민감성에 따라 여러 방법으로 등급화 되고 있다. 차건상 등(2011)에 의하면 개인정보를 ‘민감정보, 활동정보, 속성정보’로 분류하고 정보유출시 개인정보의 피해 규모에 따른 개인정보의 중요도를 3개의 등급으로 분류하였다. 또한 행정안전부는 개인정보의 영향도에 따라 3개의 등급으로 분류하고 등급별 자산 가치를 부여하였다(행정안전부 개인정보 영향평가 수행 안내서, 2018).

대부분 고유식별정보, 민감정보, 신용정보, 의료정보는 높은 중요도 등급을 부여하며, 개인 속성정보 등 중요도 등급이 낮은 정보라 하더라도 개인정보가 조합되어 유추·식별할 수 있으면 중요도 등급이 높아질 수 있음을 보여주고 있다. 그러나 업무의 특성에 따라 개인정보가 제공될 때 정보의 수준은 복잡해 질 수

있고 개인의 속성정보 및 고유식별정보 등 개인의 신분을 특정할 수 있는 정보의 명시 여부에 등급화는 한계가 있다. 따라서 익명화된 민감정보에 대해서도 추정기법을 통해 신분과 속성이 노출되는 경우에 대한 분석이 추가로 요구된다(천명호 등, 2013). 즉, 행정안전부나 한국인터넷진흥원(KISA)은 공공기관에서 제시하는 개인정보 수준 및 영향평가에 대한 안내서(행정안전부 개인정보 영향평가 수행 안내서, 2018), 또는 소셜 네트워크 내 개인정보유출 및 유출위험도에 대한 연구(천명호 등, 2013) 등 개인정보 유출의 위험성과 그에 대한 등급화에 대해 다루고 있는 주요 연구들은 특정집단의 민감정보 식별 용이성에 대해 정량적으로 다루고 있지는 않다(박철현 등, 2015).

본 논문에서는 개인정보의 등급은 개인정보영향평가 가이드의 개인정보 영향도 등급표를 참조하였으며, 등급은 3단계(1 ~ 3등급)로, 자산가치(5, 3, 1)의 값을 정하여 15가지 항목분류로 산출하였다(행정안전부 개인정보 영향평가 수행 안내서, 2018).

[표3] 개인정보 영향도 등급 표

순번	등급	조합설명	중요도 등급	자산가치	분류
1	1등급	그 자체로 개인의 식별이 가능하거나 매우 민감한 개인정보 또는 관련 법령에 따라 처리가 엄격하게 제한된 개인정보	5	고유식별정보	주민등록번호, 여권번호, 운전면허번호, 외국인등록번호
				민감정보	사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 병력(病歷), 신체적·정신적 장애, 성적(性的) 취향, 유전자 검사정보, 범죄경력 정보 등 사생활을 현저하게 침해할 수 있는 정보

				인증정보	비밀번호, 바이오정보 (지문, 홍채, 정맥 등)
				신용정보/ 금융정보	신용정보, 신용카드번 호, 계좌번호 등
				의료정보	건강상태, 진료기록 등
				위치정보	개인 위치정보 등
				기타 중요정보	해당 사업의 특성에 따라 별도 정의
2	3등급	조합되면 명확 히 개인의 식별 이 가능한 개인 정보	3	개인식별정보	이름, 주소, 전화번호, 핸드폰번호, 이메일 주 소, 생년월일, 성별 등 개인관련정보
				개인관련정보	학력, 직업, 키, 몸무 게, 혼인여부, 가족상 황, 취미 등
				기타 개인정보	해당 사업의 특성에 따라 별도 정의
3	5등급	개인식별정보와 조합되면 부가 적인 정보를 제 공하는 간접 개 인정보	1	자동생성정보	IP정보, MAC주소, 사 이트 방문기록, 쿠키 (cookie) 등
				가공정보	통계성 정보 등
				제한적 본인식별 정보	회원번호, 사번, 내부 용 개인식별정보 등
				기타 간접 개인정보	해당 사업의 특성에 따라 별도 정의

참고 : 행정안전부(2018) KISA-GD-2018-0004 개인정보 영향평가 수행 안내서

7. IPA분석

IPA(Importance Performance Analysis)는 다속성 모델에 기반한 분석방법으로
서 각 속성의 상대적 중요도와 성취도를 동시에 비교하는 평가방법이다(Martilla

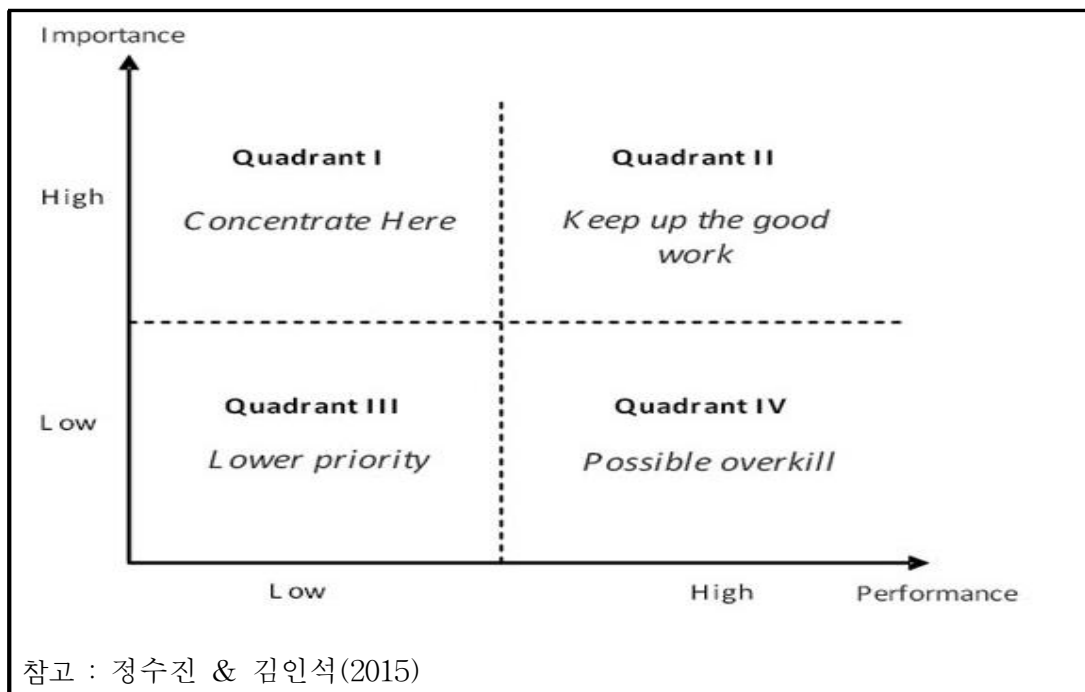
& James, 1977). IPA는 이용자의 만족도를 측정하기 위한 것으로 이용 전에는 각 속성의 중요도를 파악하고 이용 후에는 성취도를 이용자가 스스로 평가하게 하여 각 속성의 상대적인 중요도와 성취도를 비교·평가하는 기법이다 (Hammit, Bixlet & Noe, 1996). 특히, 사용이 간편하고 결과해석이 용이하며 문제 제시가 명확하다는 점에서 활용도가 매우 높다는 장점이 있어 마케팅, 은행, 교육, 스포츠심리학, 보건의료 등 여러 분야에서 활용되고 있으며(이형래, 2005), 다양하고 복잡한 성격을 가진 항목을 평가할 수 있을 뿐만 아니라 어려운 통계적 기법을 사용하지 않고도 평가요인의 평균값과 매트릭스를 이용하여 빠르고 쉽게 결과를 도출할 수 있기 때문에 정해진 인력과 예산으로 우선적으로 해결해야 될 사항을 결정 하는데 유용한 정보를 제공한다(공기열, 2006).

또한 IPA는 상품이나 서비스가 지니고 있는 중요 요인들에 대하여 중요도(importance) 및 수행도(performance)를 소비자가 어떻게 인식하고 있는지를 동시에 분석하기 위해 마케팅에서 개발된 기법으로 이용자의 고객만족을 측정하기 위하여 우선 이용자가 어떤 요인을 중요하게 여기는지를 조사한 뒤 이용 전에는 각 요인의 중요도를 그리고 이용 후에는 고객만족을 이용자 스스로가 평가하게 하여 요인을 상대적으로 중요도와 성취도를 동시에 비교·분석하는 기법이다(고순영, 2005). 구체적으로는 중요도와 성취도의 평균값을 점점으로 하는 방법(Oh, 2001)과 중요도와 성취도의 중앙값을 활용하는 방법, 그리고 표준 편차에 의한 계산방법(손대현, 김병삼, 1999) 및 임의적인 방법 등이 있는데 대부분의 연구에서는 중요도와 성취도의 평균값을 가지고 점점을 잡아서 IPA Matrix의 교차점으로 사용하고 있다. 추가적으로 IPA는 기업에서 고객만족에 초점이 맞추어진 분석방법이며, 두 가지 차원의 조사가 진행되는 데 X축에 사용되는 요인의 중요도와 Y축에 사용되는 실제수행도 고객 만족을 조사하게 된다. 고객은 특정한 요인의 기업이나 서비스나 제품을 평가하는데 얼마나 중요한 요인 인가를 스스로 평가하게 하고 동시에 특정제품이나 서비스가 이러한 요소들을 얼마나 잘 달성하고 있는가를 평가하게 한다. 이때 규명되는 요인은 분석결과의 유용성을 판별하는데 결정적인 역할을 하게 되기 때문에 기존자료 대한 면밀한 검토를 필요로 하게 된다(김문수, 2003). 실제 이러한 IPA 분석은 단순하지만 매우 간단한 방법으로 실무적으로 활용이 가능한 평가방법으로 분류되고 있다. 특히 한정된 자원

을 가지고 만족을 극대화 할 수 있는 자원배분의 조합을 찾기 위해 많이 활용되는 방법이다(Matzleretal, 2004).

이와 같이 IPA분석은 차이가 발생하는 요소들에 대해 어떤 요소가 과잉투자 혹은 과소투자 되었는지를 파악하여 전략적 관점에서 개선책을 찾아내는데 유용하게 사용될 수 있다.

〈그림 1〉 IPA 매트릭스



8. 관련 연구 고찰

개인정보와 관련된 연구들은 개인정보의 등급분야에서는 비교적 활발하게 연구가 이루어져 왔으며, 최근 들어 빅데이터 환경에서 개인정보 연구들이 이루어지고 있다. 박철현 등(2015)에 의하면 직접적인 신분 정보가 없어도 추정 방법을 통해 신분 뿐 만 아니라 민감한 속성까지 노출 되는 경우에 대하여 공개위험척도를 적용한 보호 등급 개선 방안을 제시하였다. 정수진·김인석(2015)은 금융사의 개인정보 취급방침을 통하여 알아낸 개인정보 항목 중 비밀번호 앞2자리, 신용도, 카드유효기간, CVC값 등은 중요도가 높게 분석되었으며, 개인정보영향도 등급표를 참조하여 개인정보의 중요도 및 가중치를 산출하고 IPA기법을 이용하

여 개인정보의 위험도를 정량적으로 분석하여 객관적인 지표로 사용 될 수 있는 기준을 제시하였다. 이한주(2012)는 의료정보는 다른 정보와 달리 보호뿐만 아니라 이용의 필요성도 제시하였고 보호와 이용의 필요성을 균형적으로 고려하는 것이 중요하다고 제시하였다. 변현수(2017)는 개인정보보호에 주력하여, 빅데이터를 정책에 활용하기 위해 데이터 관리의 중요성과 더불어 데이터를 재확인하고 현실 적용 능력을 배가시켜야 한다는 것을 제안하였다. 김숙영(2014)은 모바일을 통한 의료정보 활용 목적은 병원·의료관련 정보의 홍보목적이 가장 적합하고 건강관리 애플리케이션의 활용목적이 가장 낮다고 인식 하는 것으로 나타났으므로, 우선적으로 모바일을 통한 의료정보 활용목적이 병원을 홍보하는 매체라는 인식에서 벗어나, 병원홍보 뿐만 아니라 건강(질환) 관리 애플리케이션 및 다양한 의료정보 서비스를 한꺼번에 제공할 수 있는 새로운 모바일 플랫폼을 제시하여 커뮤니케이션 활성화를 유도할 필요가 있다.

여기서 살펴 본 것처럼 개인정보의 중요도 등급 개선방향, 위험도분석, 개인정보 이용의 필요성, 빅데이터 활용을 위한 데이터 관리의 중요성 유형으로 나눌 수 있으며, 본 연구에서는 IPA분석을 통해 개인정보의 중요도와 활용도에 따른 시사점을 도출하고자 한다.

Ⅲ. 연구방법

본 논문에서는 개인정보의 중요도와 활용도에 따른 시사점을 도출하기 위하여 IPA분석 모형을 사용한다. 개인정보의 중요도는 개인정보 영향도 등급표를 활용하여 산출한다. 개인정보의 활용도는 해당 개인정보의 활용을 위한 요구건수 등을 전처리하여 산출한다.

<그림 2>에 나타난 바와 같이, 중요도는 높고 활용도는 낮은 개인정보는 관리전략 A에 따라 관리될 필요가 있고, 중요도와 활용도가 모두 높은 개인정보는 관리전략 B, 중요도와 활용도가 모두 낮은 개인정보는 관리전략 C, 중요도는 낮고 활용도는 높은 개인정보는 관리전략 D에 따라 관리될 필요가 있다.

<그림 2> 개인정보의 중요도 및 활용도에 따른 관리전략 모형

↑ 중 요 도	I. 관리전략 A	II. 관리전략 B
	III. 관리전략 C	IV. 관리전략 D
	===== 활 용 도 =====>	

관리전략 A는 중점개선 전략으로서 개인정보 보호와 개인정보 활용의 조화를 위해 개인정보의 개념을 정확하게 할 필요가 있다. 다만 개인과 관련한 정보를 개인정보, 가명정보, 익명정보로 구분하여 개인정보는 철저히 보호하고, 가명정보는 개인정보화 할 수 없도록 확실한 안전장치 후 개인정보를 활용할 수 있게 해야 한다. 관리전략 B는 유지강화 전략으로서 개인정보 유출 및 오·남용 방지를 위해 기술적 측면에서 국정원 검증필 암호 알고리즘을 이용해 암호화 조치를 해야 한다. 관리전략 C는 점진개선 전략으로서 개인정보의 중요도 및 활용을 자칫

잘못 판단할 소지가 있어서, 개인정보 담당자는 개인정보 취급자의 사전교육 및 모니터링을 통해 개인정보 활용에 대한 관리감독을 지속적으로 진행해야 한다. 관리전략 D는 지속유지 전략으로서 개인정보를 활용하는 과정에서 개인을 알아볼 수 있게 되거나 사생활이 침해되지 않도록 관련 개인정보 활용 규정 및 지침을 정비해서, 개인정보를 더욱 철저하게 관리해야 한다.

IV. 조사 분석

1. 데이터 수집 및 표준화

본 논문에서 제안하는 방법을 효과적으로 수행하기 위해 개인정보항목의 데이터 수집은 「행정안전부 개인정보보호 종합지원시스템[<https://intra.privacy.go.kr>]」에 등록된 기관별 개인정보파일 중 5개의 국립대학교 병원을 기준으로 기관별 개인정보파일 명칭<표4>을 조사하였다.

<표4> 기관별 개인정보파일 명칭

기관 명	개인정보파일 명
J병원	병리검사대장, 지역 암관리사업, 제주지역 암등록 조사사업, Stoke CP데이터, AMI CP 데이터, 유전자검사동의서, 방사선치료기기사용기록, 병리검사보고서, 사례관리등록대장, 제증명 관리시스템에 의한 환자정보, 응급실기반 손상감시체계, 국가응급환자진료정보망(NEDIS), 암환자 코호트 사업, 건강검진 문진표, 사실조회, 신체감정, 촉탁, 통합의료정보시스템, 발전후원회명단, 장례식장 임대차 계약서, 병리검사의뢰서, 구급활동일지 과별서식 자료, 취약계층 관절수술 지원 사업, 폐암검진 시범사업, 리퍼홈페이지 회원관리, 의뢰의사관리
B병원	건강검진자 명부, 민원신청자 명부, 발전후원회 후원자 명부, 자원봉사자 명부, 제증명 발급 신청자 명부, 폐암검진시범사업 환자명부, 암환자 등록명부, 의료영상 촬영 대상자 명부, 감면대상자 명부, 연대보증인 명부, 환자명부, 연구자 이력서, CRA 회원 가입, 임상연구 담당자 정보등록신청서, 뇌사판정관련자료, 이식대상자 선정 승인 관련 서류, 장기 등 및 조직 기증자 등록 신청서, 장기 등 및 조직 기증희망자 등록신청서, 장기 등 이식대

	<p>기자 등록신청서, 적출 및 이식통보서, 요양급여 적정성평가 대상자 명부, 의료비청구 대상자 명부, 헌혈자 명부, 한방병원_암환자 등록 명부, 한방병원_의료비 청구 대상자 명부, 한방병원_임상질지표 평가대상자 명부, 한방병원_민원신청자 명부, 한방병원_연대보증인 명부, 한방병원_외래환자 진료명부, 한방병원_입원환자 진료명부, 한방병원_제증명발급 신청자 명부, 한방병원_환자명부, COPD 발굴사업 대상 명단, 홈페이지 회원정보</p>
C병원	<p>종합검진비 할인 신청서, 종합검진비 협약서 및 청구문서, 민원관리대장, 지역아동센터 방문 검진결과 관리, 사전연명의료의향서, 연명의료 중단 등 결정, 의료사회사업 상담 관리, 의료소송, 사실조회, 신체감정, 촉탁, 구분산정 의뢰, 미수(차상위/의료급여 장애인) 관리, 미수(체납진료비) 환자관리, 민원관리, 산재보험 환자 관리, 자동차보험 환자 관리, 장애인 미수내역 관리, 재원 환자 관리, 정신건강 환자 입·퇴원 관리, 진료비 사후관리(가퇴원, 산정특례), 필수예방접종 의료지원, 환자 의료지 비원, 연구사업, 뇌사기증자 관리, 살아있는 기증자의 장기 기증 관리, 장기 기증자 희망 등록자 등록, 장기이식 대기자 등록, 장기이식자의 이식 후 통보관리, 조직기증 및 이식관리, 조직기증자 병력 및 투약이력 조사, 조직기증자 조사 자료, 홈페이지 회원 관리</p>
G병원	<p>법정감염병신고서, 환자명부, 방사선사진 및 그 소견서, 진단서, 처방전, 환자명부, 퇴원분석정보, 일반검진정보, 각막이식대기자, 각막이식환자, 뇌사 장기기증자, 종합검진정보, 외주 수탁검사장부, 청구명세서, 기부금 관리, 홈페이지회원정보</p>
S병원	<p>홈페이지회원정보, 고객 불편 우편 접수물 및 공공기관 민원 관련 외부문서, 고객의 소리, 1천만원 이상 기부자, 약정서, 자원봉사자 정보, 후원인 및 후원인 가족 정보, 보험청구신청자 정보, 민원신청자 명부, 의료급여 자격확인 정보, 의무기록사본 발급 정보, 환자 명부, 의료영상정보시스템 환자 정보, 헌혈자 정보,</p>

	협력병원 의사 정보, 홈페이지 회원정보, 홈페이지 회원관리, 환자정보 DB, 진료협력팀 홈페이지 회원정보, 홈페이지 회원정보
--	---

조사된 개인정보파일 명을 가지고 공통 개인정보 항목의 61개의 속성을 파악하였으며, 파악된 61개의 속성은 개인정보보호법의 개인정보영향평가 영역의 개인정보 영향도 등급표를 활용하여 개인정보의 중요도 등급을 측정하였다.

개인정보 항목의 분류는 15개의 속성(고유식별정보, 민감정보, 인증정보, 신용정보, 금융정보, 의료정보, 위치정보, 기타 중요정보, 개인식별정보, 개인관련정보, 기타 개인정보, 자동생성정보, 가공정보, 제한적 본인 식별정보, 기타 간접 개인정보)으로 분류하고 <표5>와 같이 수치범위는 동일범위로 축소하여 표준화 하였다.

[표5] 개인정보의 중요도와 활용도 데이터 원본 및 표준화

개인정보 분류 및 항목		중요도 등급	중요도 표준값	활용도 (건)	활용도 변환	활용도변환 표준값
개인 식별 정보	성명	3.00	0.25081	128	5.00	4.35292
	성별	3.00	0.25081	25	1.00	-0.36758
	영어가이름	3.00	0.25081	1	1.00	-0.36758
	나이	3.00	0.25081	12	1.00	-0.36758
	생년월일	3.00	0.25081	49	2.00	0.81254
	이메일	3.00	0.25081	29	2.00	0.81254
	집연락처 (직장연락처)	3.00	0.25081	62	3.00	1.99267
	핸드폰번호	3.00	0.25081	85	4.00	3.17279
	집주소 (직장주소)	3.00	0.25081	90	4.00	3.17279
	우편번호	3.00	0.25081	1	1.00	-0.36758
개인 관련 정보	가족관계 (증명서 포함)	3.00	0.25081	11	1.00	-0.36758
	학력	3.00	0.25081	2	1.00	-0.36758
	종교	3.00	0.25081	3	1.00	-0.36758
	결혼여부	3.00	0.25081	1	1.00	-0.36758

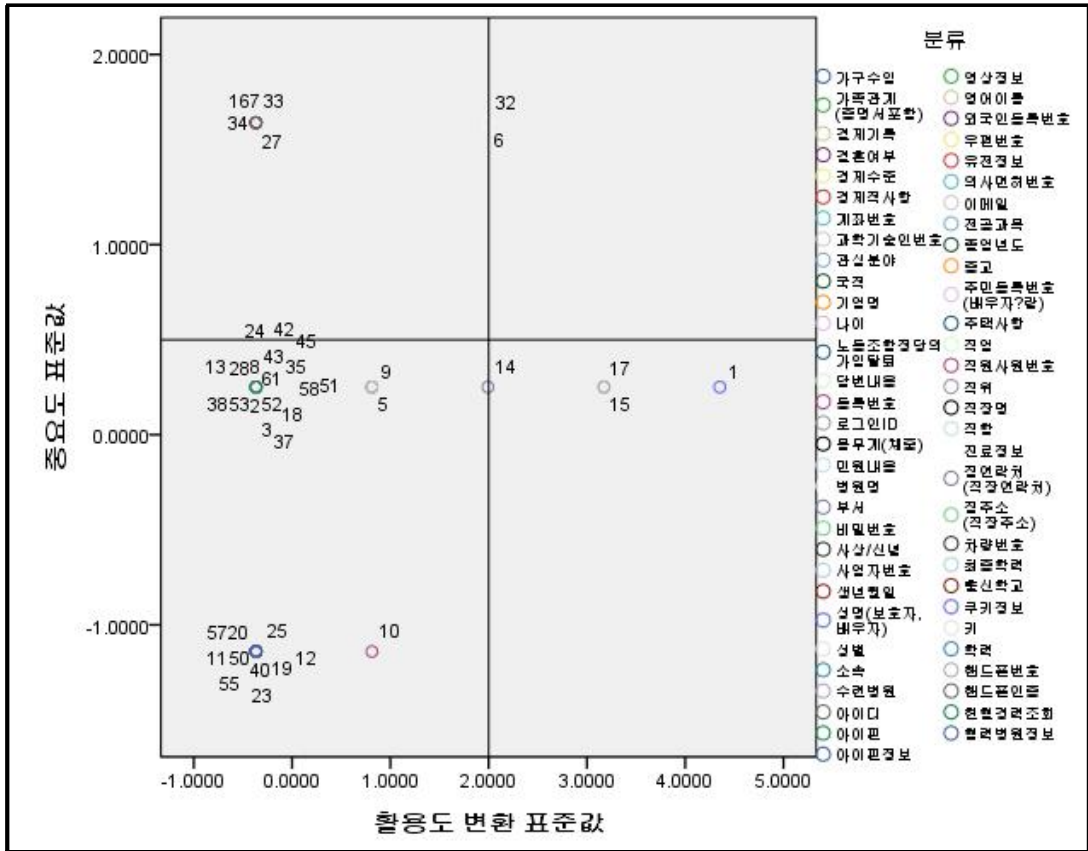
	경제수준	3.00	0.25081	1	1.00	-0.36758
	출신학교	3.00	0.25081	1	1.00	-0.36758
	최종학력	3.00	0.25081	1	1.00	-0.36758
	주택사항	3.00	0.25081	1	1.00	-0.36758
	경제적사항	3.00	0.25081	1	1.00	-0.36758
	키	3.00	0.25081	2	1.00	-0.36758
	몸무게(체중)	3.00	0.25081	3	1.00	-0.36758
	국적	3.00	0.25081	1	1.00	-0.36758
	헌혈경력조회	3.00	0.25081	1	1.00	-0.36758
	가구수입	3.00	0.25081	1	1.00	-0.36758
고유 식별 정보	주민등록번호	5.00	1.64166	68	3.00	1.99267
	외국인등록번호	5.00	1.64166	2	1.00	-0.36758
기타 간접 개인 정보	민원내용	1.00	-1.14004	1	1.00	-0.36758
	답변내용	1.00	-1.14004	1	1.00	-0.36758
	졸업년도	3.00	0.25081	1	1.00	-0.36758
	차량번호	1.00	-1.14004	2	1.00	-0.36758
	과학기술인번호	1.00	-1.14004	1	1.00	-0.36758
	수련병원	1.00	-1.14004	1	1.00	-0.36758
	아이핀	1.00	-1.14004	1	1.00	-0.36758
	전공과목	1.00	-1.14004	1	1.00	-0.36758
	관심분야	1.00	-1.14004	1	1.00	-0.36758
기타 간접정보	기업명	1.00	-1.14004	1	1.00	-0.36758
기타 개인정보	의사면허번호	3.00	0.25081	4	1.00	-0.36758
민감 정보	유전정보	5.00	1.64166	9	1.00	-0.36758
	노동조합정당의 가입	5.00	1.64166	1	1.00	-0.36758
	사상/신념	5.00	1.64166	1	1.00	-0.36758
신용 정보	계좌번호	5.00	1.64166	4	1.00	-0.36758
	결제기록	5.00	1.64166	1	1.00	-0.36758
의료	영상정보	5.00	1.64166	4	1.00	-0.36758

정보	진료정보	5.00	1.64166	54	3.00	1.99267
인증 정보	핸드폰인증	5.00	1.64166	1	1.00	-0.36758
	비밀번호	5.00	1.64166	2	1.00	-0.36758
자동 생성 정보	아이핀정보	1.00	-1.14004	1	1.00	-0.36758
	로그인ID	1.00	-1.14004	2	1.00	-0.36758
	아이디	1.00	-1.14004	1	1.00	-0.36758
	쿠키정보	1.00	-1.14004	1	1.00	-0.36758
제한적 본인 식별 정보	등록번호	1.00	-1.14004	35	2.00	0.81254
	직원사원번호	1.00	-1.14004	1	1.00	-0.36758
	직장명	1.00	-1.14004	5	1.00	-0.36758
	소속	1.00	-1.14004	1	1.00	-0.36758
	부서	1.00	-1.14004	1	1.00	-0.36758
	직함	1.00	-1.14004	1	1.00	-0.36758
	직위	3.00	0.25081	1	1.00	-0.36758
	협력병원정보	1.00	-1.14004	1	1.00	-0.36758
	병원명	1.00	-1.14004	1	1.00	-0.36758
	직업	3.00	0.25081	3	1.00	-0.36758
	사업자번호	1.00	-1.14004	1	1.00	-0.36758

2. IPA 분석 결과

본 연구는 의료기관을 대상으로 기관마다 관리되는 공개된 개인정보파일의 개인정보 중요도와 활용도를 분석한 결과 개인정보의 중요도가 높다고 활용도가 증가하지는 않은 것으로 나타났으며, IPA기법을 이용한 분석결과는 <그림 3>과 같다. <그림 3>과 같이 의료기관에서 수집하는 개인정보의 중요도와 활용도를 2차원 공간상에 일목요연하게 나타냈다. X축은 개인정보의 활용도를 타나내고 있으며, 우측으로 갈수록 그 정도는 높다. 또한 Y축은 개인정보의 중요도를 의미하며 위로 올라갈수록 중요도가 높다.

<그림 3> IPA 분석결과



IPA분석의 구간별 속성의 분포를 정리하면 <표6>과 같이 제 I 사분면에는 12개, 제 II 사분면에 2개, 제 III 사분면에 43개, 제 IV 사분면에 4개의 개인정보가 존재하고 있다.

IPA 분석결과 <그림 3>과 구간별 속성의 분포 <표 6>를 살펴 본 결과 제 I 사분면은 중요도는 높고, 활용도는 낮은 정보들로서 외국인 등록번호, 영상정보, 결제기록, 비밀번호, 계좌번호, 핸드폰 인증 등이 있으며, 해당 정보들의 활용되는 측면으로는 학술연구 및 통계작성의 목적, 국민건강보험공단, 건강보험심사평가원, 보험회사 및 병원 간 진료정보교류 등이 있으며, 자칫 개인정보 담당자들이 개인정보의 가치를 낮게 측정하여 실무에 적용할 수도 있다. 활용도가 많은 개인정보는 개인정보의 안정성 확보 조치 기준의 관리적/기술적 조치 외에도 개인정보 활용시 분실·도난·유출·위조·변조되지 않게 더 철저한 관리가 필요하며, 개인정보의 활용도는 높이되, 개인정보는 안전장치를 강화하여 훨씬 더 두텁게 보호

해야 한다. 제2사분면은 중요도와 활용도 모두 높은 개인정보들로서 주민등록번호, 진료정보가 여기에 속한다. 개인정보의 중요도 등급에 관계없이 주민등록번호는 기술적 측면에서 온라인(전자적 형태) 문서의 경우 암호화 알고리즘(국정원 검증필 암호 알고리즘)을 이용해 암호화 조치하여야 하고, 서류문서는 잠금장치가 있는 안전한 장소에서 관리되어야 한다. 또한 진료정보 중 이미지파일 형태의 영상정보도 암호화 조치가 이뤄져야 한다. 현재의 상태를 지속적으로 유지하는 노력이 필요하다. 제3사분면은 중요도와 가중치 모두 낮은 개인정보들은 의사면허번호, 학력, 가족관계, 나이, 몸무게, 키, 결혼여부, 생년월일 등으로 나타났다. 중요도와 활용도가 낮으나 개인정보취급자가 다른 개인정보와 쉽게 결합하여 활용 할 경우 위험도를 낮게 측정 하여 실무에 적용할 수 도 있으며 주의가 필요하다. 제4사분면은 중요도는 낮고 활용도가 높은 항목들로서 집 연락처, 집 주소, 핸드폰번호, 성명 등이 해당한다.

<표6> 구간별 속성의 분포

구분	개인정보 항목
Quadrant 1	외국인등록번호, 영상정보, 결제기록, 비밀번호, 계좌번호, 유전정보, 핸드폰인증, 노동조합 정당의 가입탈퇴, 사상/신념, 최종학력, 종교, 이메일
Quadrant 2	진료정보, 주민등록번호
Quadrant 3	의사면허번호, 가구수입, 졸업년도, 주택사항, 직업, 우편번호, 학력, 성명, 나이, 가족관계, 경제적 사항, 몸무게, 경제수준, 키, 국적, 현혈경력조회, 영어이름, 출신학교, 직위, 결혼여부, 생년월일, 사업자번호, 차량번호, 아이핀 정보, 병원명, 부서, 직장명, 답변내용, 소속, 협력병원정보, 기업명, 로그인ID, 과학기술인번호, 직원사원번호, 관심분야, 직함, 전공과목, 아이핀, 아이디, 쿠키정보, 등록번호, 수련병원, 민원내용
Quadrant 4	집 연락처, 집 주소, 핸드폰번호, 성명

V. 결론

기존 개인정보의 중요도는 개인정보보호법(제33조) 개인정보 영향평가의 평가 등급표에 의해 개인정보의 등급이 만들어지고, 행정안전부에서 관리하는 개인정보영향평가 및 개인정보보호 관리수진 진단을 통해 개인정보보호 관리체계 및 침해예방, 개인정보의 평가관리를 확인할 수 있으나, 해당 내용은 정량적 평가기준이 포함되어 있으나, 대부분 개인정보 담당자의 정성적 분석의 형태를 보이고 있다.

본 논문에서는 개인정보의 중요도와 활용도를 IPA분석으로 수행하였으며, 개인정보 담당자 및 취급자의 주관적인 판단을 배제하였고, 개인정보 중요도와 활용도 분석의 객관적인 지표로 볼 수 있다.

첫째, IPA분석의 제1사분면에 위치한 개인정보의 중요도가 높고 활용도가 낮은 개인정보 항목을 중점 개선해야 한다. 의료정보의 경우 학술연구 및 통계작성, 병원 간 진료정보 교류, 제3자 기관에 개인정보를 제공하기 때문에 자칫 개인정보 담당자 및 취급자들이 개인정보의 중요도 및 활용도를 낮게 측정하여 당초 수집 목적의 범위를 초과하여 이용 및 제공하거나 실무에 적용할 우려가 있어 제공되는 정보에 따라 개인정보 활용시 분실·도난·유출·위조·변조되지 않도록 더 철저한 관리가 필요하며, 개인정보의 활용도는 높여, 개인정보는 안전장치를 강화하여 훨씬 더 두텁게 보호해야 한다.

둘째, 개인정보 중요도 등급이 높다고 활용도가 높은 것은 아니며, 중요도와 관계없이 개인정보의 활용도는 다양한 분포를 나타냈다. 이러한 분포는 개인정보를 수집·이용·제공 하면서 시급한 노력의 투입이 필요 없는 영역이라고 판단할 수도 있으나, 이론적 배경에서도 언급되었듯 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 활용되거나, 의료기관의 개인정보 유출 및 오·남용으로 인하여 생명, 신체에 대한 위협 등을 생각한다면 개인정보 담당자 및 취급자는 보다 신중하게 해석할 여지가 있으며, 적절한 내부통제시스템 구축 및 운영을 위해 노력해야 한다.

본 연구의 한계점으로는 개인정보의 중요도와 활용도를 분석하기 위해 수집한 데이터가 일부 의료기관의 개인정보파일현황의 데이터만 활용함으로서 대표성을 갖는지에 대한 한계가 있다. 다른 분야에서도 개인정보를 활용하기 때문에 업권 별로 개인정보 항목을 수집하여 통일된 개인정보파일 형태의 개인정보 항목을 가지고 개인정보 활용도를 산출하여 분석해 볼 수 있는 연구가 추가적으로 필요하다.

<국내문헌>

- [1] 고순영(2007) 민박입지유형별 이용객이 민박요인에 대한 중요도 고객만족 분석, 미간행 석사학위논문, 동의대학교 대학원.
- [2] 공기열(2006) IPA 기법을 이용한 여가활동 평가, 관광연구지, 20(3), 285-303.
- [3] 김기열(2010) 공공부문에 관한 외국의 개인정보 보호 법제와 국내 입법의 검토방향. 월간법제, 2010.09.
- [4] 김동수·김민수(2006). e-Health 시대의 진전에 따른 의료정보보호 쟁점 및 정책방향. 정보화정책, 13(4), pp.128~148. 서울: 한국정보화진흥원.
- [5] 김문수(2003) 호텔정보시스템의 중요도 성과분석, 관광연구지, 18(2), 284-300.
- [6] 김숙영(2014) 모바일을 통한 의료정보 활용에 대한 인식비교.
- [7] 김영대(1996) 계층화 분석과정(AHP)에 의한 개인정보 보호정책의 중요도 분석. 정책분석평가학회보, 6, 147-165.
- [8] 문재완(2016) 유럽연합(EU) 개인정보보호법의 특징과 최근 발전.
- [9] 박지용(2012) 환자의 프라이버시 및 정보보호의 법적 근거 고찰. 한국의료법학회지, 20(2), 163-190.
- [10] 박철현, 김철수, 김영성, 안훈상, 배종호(2015). 공개위험측도를 활용한 군 개인정보 등급 분류 개선. 보안공학연구논문지, 12(6), 581-596.
- [11] 손대현·김병삼(1999)관광지의 서비스품질 재고 : IPA 기법을 중심으로, 한양대 사회과학논집,18,217-249.
- [12] 이재식(2013) 빅데이터 환경에서 개인정보보호를 위한기술. Internet & Security Focus, 79-104.
- [13] 이한주(2012) 의료영역에서의 개인정보보호의 문제점과 해결방안. 한국의료법학회지, 20(2), 267-293.
- [14] 이형래(2005) 호텔연회서비스의 중요도-성취도에 관한 연구. 대구대학교 대학원. 석사학위논문.
- [15] 전은정·김학범·염홍열(2012) 유럽의 개인정보보호 법·제도 동향. 정보보호학회지, 22(2), pp58~72.
- [16] 전은정·김학범·염홍열(2012) 미국의 개인정보보호 법·제도 동향.
- [17] 전은정·김학범·염홍열(2012) 일본·중국의 개인정보보호 법·제도 동향.

- [18] 정영철·이기호·이야리(2013) 의료기관의 개인정보보호현황과 대책.
- [19] 전기홍·조우현(1994) 우리나라 병원정보시스템 실태에 관한 연구. 보건행정학회지, 4(2), pp.1~16. 서울: 한국보건행정학회.
- [20] 정수진·김인석(2015) IPA를 이용한 개인정보 위험도 분석 연구. 한국인터넷방송통신학회 논문지, 15(6), 267-273.
- [21] 천명호, 최종석, 신용태(2013) SNS에서 개인정보유출방지를 위한 개인정보 유출위험도 측정 방법. 정보보호학회논문지, 23(6), 1199-1206.
- [22] 변현수(2017) 정부 및 공공기관에서의 빅데이터 활용에 대한 현황 및 실행 방안 제안. 디지털융복합연구, 15(4), 13-25.
- [23] 행정안전부(2018) KISA-GD-2018-0004 개인정보 영향평가 수행 안내서.
- [24] 행정안전부(2018) 개인정보실태점검 및 행정처분 사례집.
- [25] <http://eiec.kdi.re.kr>.
- [26] <http://www.etnews.com>.
- [27] <https://intra.privacy.go.kr>.
- [28] <http://www.itfind.or.kr>.
- [29] <http://www.law.go.kr>[개인정보보호법 인용].

<국외문헌>

- [1] G.S. Cha and Y.T. Shin, A Study on Standardization for Sensitivity Level of Personal Information, Korea Institute of Communication Sciences 11-6, Vol.36, No.6 (2011).
- [2] Hammitt, W.E., Bixler, D.N. and P. Francis(1996), “Going Beyond Important Performance Analysis to Analyze the Observance-Influence of Park Impact,” Journal of Park and Recreation Administration, 14(1), 45-62.
- [3] J. A. Martilla and J. C. James, 『Importance-Performance Analysis』, Journal of Marketing』, Vol. 41, pp. 77-79, 1977.
- [4] Martilla J.A. and James J.C.(1977), Importance-performance Analysis, Journal of Marketing, 41(1), 77-118.