의료정보화와 환자개인정보보호 방안

신승중*, 지혜정**, 곽계달**
한세대학교 컴퓨터공학과
한양대학교 공학대학원 컴퓨터공학과
e-mail: expersin@hansei.ac.kr

A Study on the Patient Privacy Protection of Medical Information

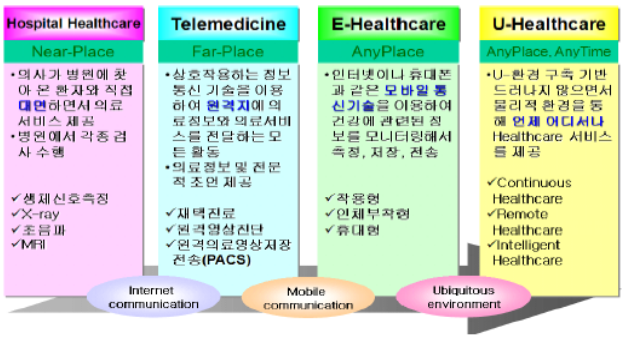
Seung-Jung Shin*, Hye-Jung Ji**, Kae-Dal Kwack***
*Dept of Computer Engineering, Hansei University
**Dept of Computer Engineering, Hanyang University

요 약

의료정보화는 환자의 개인정보를 침해할 수 있다. 우리나라의 상당수 의료기관은 환자개인정보보호에 소극적이다. 의료정보의 유출을 방지하기 위한 법령과 표준안 및 체계적인 지침이 개발되어 있지 않다. 환자 개인정보 침해유형을 사례를 통해 살펴보고, 법제도적 측면·기술적 측면·관리적 측면에서 환자 개인정보를 보호 할 수 있는 방안을 모색해 보고자 한다.

1. 서론

정보통신 기술과 의료기술의 발전으로 국민들의 삶의 질이 향상되면서 의료서비스에 대한 관심이 커지고 있다. 여기에 국내 의료기관들의 경쟁력 향상을 위한 노력이 계속되고 있는 가운데, 의료정보화는 e-Health를 거쳐 m-health, u-Health로 진행을 가속화하고 있다.



[그림1] IT기술과 융합된 u-Health, (ETRI Leader Academy "유비쿼터스 라이프케어" 발표자료 2007.08)

의료정보화는 환자 원무기록의 디지털화, 영상정보저장기록화, 병원업무전산화등 병원정보화단계를 거쳐 인터넷이나 무선기기를 이용한 원격의료등이 현실화되고 있는 단계이다. 또한 일부 병원에서는 센서를 이용한 의료정보의 획득과 상시접근을 통한 유비쿼터스의 개념이 실현되어 가고 있다. 이러한 의료정보화 분야의 눈부신 발전으로 환자들은 기존의 의료서비스보다 업그레이드된 의료서비스를 누릴 수 있으며, 서비스를 제공하는 비용 또한 획기적으로 줄일 수 있어 국가 정보화 차원에서 매우 중요한 분야 가운데 하나로 여겨지고 있다.

그러나 다른 정보화 분야에서와 마찬가지로 정보화 역기능을 제대로 예방, 대응하지 못할 경우 다른 분야보다 훨씬 큰 보안위협 가능성을 수반할 수 있다.

개인의 민감한 의료정보가 적절히 관리되지 않아 누출될 경우, 프라이버시 침해는 다른 정보의 누출보다 훨씬 심각할 것으로 예상된다.

환자관리의 편의성 때문에 빈번히 사용되는 무선통신의 보안 취약점으로 인하여, 원격의료나 인터넷병원은 내·외부의 침입으로부터 취약하다. 또한 병원내부의 권한 관리 체계도 미흡하여 내부자를 통한 정보유출의 가능성이 상존하고 있다.

효율적인 의료전달 체계의 확립에 필요한 의료정보의 공유화, 원격의료서비스, 의약분업제도 시행과 더불어 제안 되고 있는 원외 처방전달시스템, 의료기관을 대상으로 하는 ASP사업 활성화등이 추진되면 더욱 환자정보보호의 필요성이 증대되고 있다. 의료정보화를 추진하는 선진국들이 모두 이에 대한 법령, 표준안, 지침등을 마련하여 환자정보를 보호하고 있다.

그러나 아직 우리나라에서는 정보화 환경에서의 의료정보의 보안과 활용에 따른 정보 유출을 방지하기 위한 법령과 표준안 및 체계적인 지침이 개발되어 있지 않다. 의료정보보안 관리자를 임명하는 등 정보화에 따른 정보보호에 관심을 가진 의료기관은 아직 소수일 뿐이다.

아직도 환자가 차트를 소지하고 진료과를 이동하거나 검사를 받으러 다니는 의료기관이 상당수 있다. 그래서 의무기록 보안 및 정보관리에 대한 새로운 표준지침개발과 개인정보를 보호할 수 있는 방안 모색이 필요하다.

따라서 본 연구에서는 의료정보화의 개념을 파악하고, 의료서비스 패러다임의 변화를 살펴보고, 현재 의료정보화에 따른 보안위협사례를 분석하여, 환자 의료정보 보호 개선 방안을 제시하고자 한다.

2. 의료정보화의 이해

1) 의료정보화의 개념

의료정보란 의료라는 특정상황에서 환자의 상태와 치료의 경과등 의료행위에 관한 사항과 소견을 의미하는 것이라고 볼 수 있다. 즉, 의료정보는 환자 상태에 대한 진단,

치료의 경과, 경과관찰등의 전과정에서 수집된 자료를 의미하며, 넓게는 의사가 의료행위를 하면서 수집한 자료와 그 자료를 기초로 연구·분석된 정보를 포괄한다.
의료정보화란 이러한 의료정보와 정보기술이 접목된 것을 의미한다.

2) 의료정보화의 현황 및 도입 유형

건강보험심사평가원은 2005년 대한의료정보학회와 함께 종합전문병원(42개)·종합병원(78개)·의원(3619개)·약국(2702개)등 1만966개 요양기관을 대상으로 "요양기관 정보화 실태조사"를 시행했다.

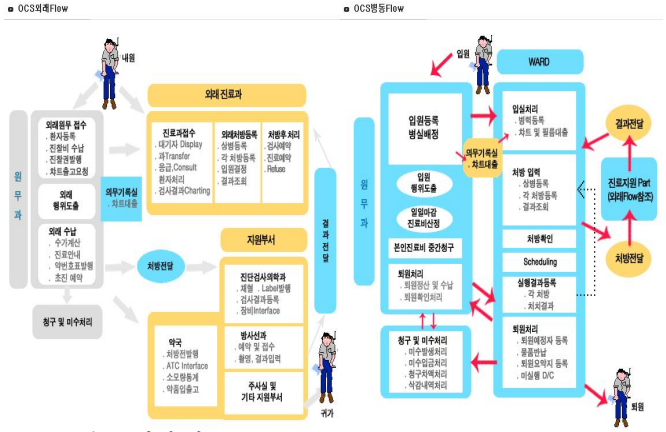
[표1] 병원급 이상 정보화 현황

업무 내용	도입율	
	1999년	2005년
외래OCS	50.5%	75.6%
병동OCS	47.9%	70.6%
의료영상저장전송시스템(PACS)	4.7%	47.1%
청구전자문서결재(EDI)	0%	94.3%
입원·외래 전자의무기록(EMR)	8.7%	20.7%

위의 표에서 볼 수 있듯이 병원급이상 의료기관의 정보화는 급속히 진전되고 있음을 알 수 있다.

① 처방전달시스템(Order Communication System,OCS)

처방의 원활한 전달을 위해 구성된 시스템으로 진료의사에 의하여 발생된 처방은 신속, 정확하게 필요한 부서로 전달되어 처리된다. 즉, 원무부서로 이동된 처방은 정확한 수납계산과 건강보험 청구를 시행하게 해주고, 약국/검사부서등 지원부서로 이동된 처방은 투약과 검사를 시행하도록 해준다. 그리고 검사결과, 투약력등의 자료는 다시 Feedback되어 진료에 도움을 줄수 있다.

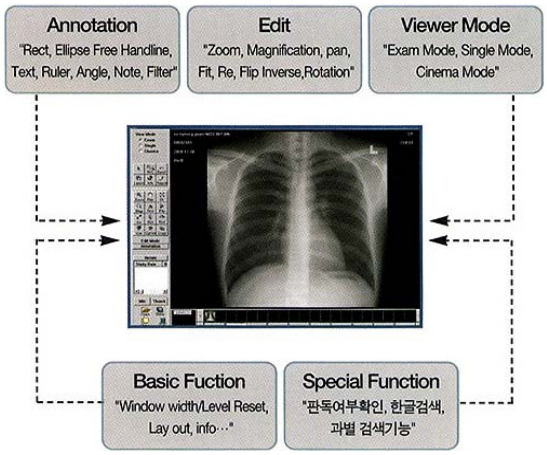


[그림2] 외래/병동 OCS FLOW, http://hmc.hanyang.ac.kr

② 의료영상저장전송시스템(Picture Archiving and Communication System, PACS)

의료환경에서 발생되는 각종 의학영상(X선, CT, MRI, PET, SPECT등)을 디지털 데이터로 획득하고 컴퓨터 저장장치에 저장하며 이를 네트워크에 연결된 다수의 컴퓨터에 전송하여 조회 활용할 수 있게 하는 시스템이다.

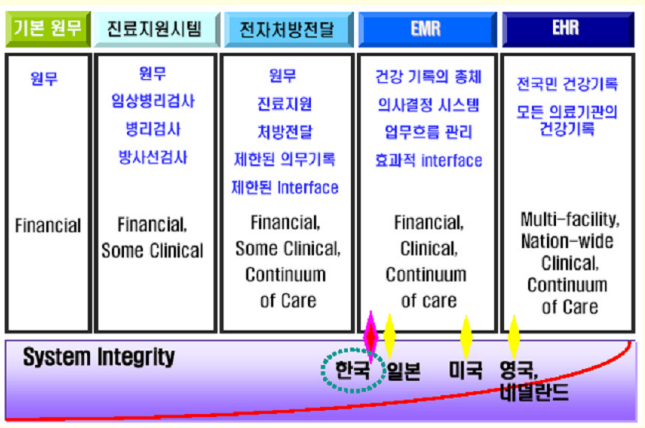
과거 필름을 이용할때와 비교했을때 분실 우려도 없을 뿐아니라 여러 의료인이 동시에 데이터를 사용할 수 있다. 또한 접근이 용이하며, 필름 보관 공간이 필요 없고, 인력 낭비도 줄일 수 있는 등 다양한 장점이 있다.



[그림3] 의료영상의 효율적 관리시스템(Medi Viewer), http://www.bit.co.kr

③ 전자의무기록(Electronic Medical Record, EMR)

종이의무기록을 전산화한 형태로 종이 매체에 의해 기록되어온 모든 의료기록을 그 업무처리구조나 정보의 범위, 정보 내용에 있어 변형없이 동일하게 전산화를 통해 업그레이드 시킨 형태를 말한다.(미국 MRIMedical Record Institute 정의) 즉, 환자의 진료과정에서 발생된 모든 자료나 기록을 전산에 입력·보관하는 시스템을 말한다. 따라서 종이 기록을 전산화했다는 것 뿐만아니라, 환자 대기시간 감소 및 정보저장의 편의성, 접근 용이성, 보험청구 업무의 자동화, 자동통계처리, 인건비 절감등의 장점이 있다.



[그림4]가톨릭대학교 의료경영대학원 의료경영이슈특강 강의교재, "EMR 병원정보화의 혁명", 이해석, 2005년4월

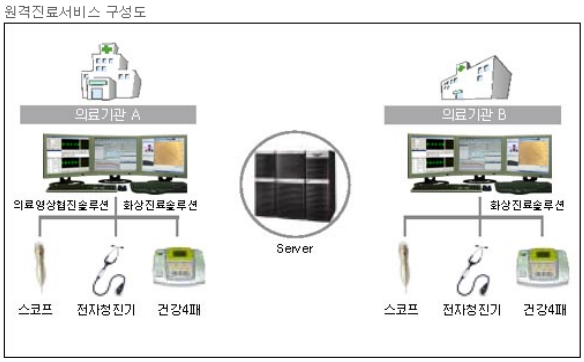
④ 원격의료(Telemedicine)

e-Health는 정보통신 기술을 이용하여 최대한 의학지식과 환자정보를 제공함으로써 환자진료 및 개인건강관리시에 효율적이고 합리적인 의사결정을 지원할 수 있는 정보체계이다.(보건복지부정의)

이러한 e-Health의 대표적 서비스인 원격의료는 정보통신 기술을 이용해서 원거리에 의료정보나 의료서비스를 전달하는 모든 활동으로 정의할 수 있다.

90년대 중반이후 의료인의 효율적 시간활용, 신속하고 편리한 진료의뢰, 지속적 진료, 자료공유등의 장점으로 시범사업을 추진해 왔으나, 정보통신기술의 한계와 의료에 대한 사회적 인식, 원격의료 책임문제, 원격의료 보험수가

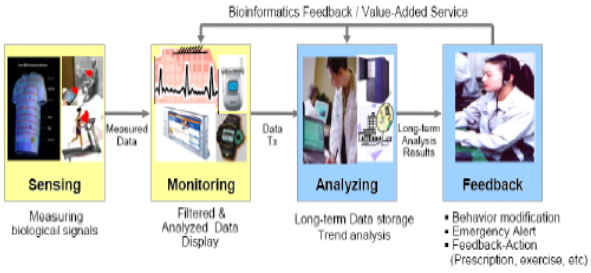
문제등의 제도적 문제가 해결되지 않아 활성화되지 않고 있다.



[그림5] 원격진료서비스 구성도, http://www.bit.co.kr

⑤ u-Health(ubiquitous Health)

정보기술과 보건의료를 결합하여 언제 어디서나 환자의 질병에 대한 예방·진단·치료·사후처리 등 보건의료 서비스를 제공하는 것을 의미한다. 즉, 때와 장소를 초월하여 가능한 연속적인 의료서비스로 시간·조직·공간의 제약을 넘어서 보다 자연스럽고 은밀하게 제공되는 Pervasive Healthcare서비스를 의미한다.



[그림6] 유비쿼터스시대의 보건의료, 진한엠엔비, 2006

3. 의료정보의 보안 특성

1) 정보의 요인적 특성

①비밀성

Pervasive Computing기술이 실현되는 의료환경에서는 환자의 의료기록에 언제 어디서나 접근가능하며, 무선으로 의료정보가 전송됨에 따라 의료정보의 비밀성과 무결성을 위협하게 된다.

②무결성

컴퓨터 바이러스 등의 악성코드로 인한 의료정보의 파괴나 시스템 소프트웨어 버그나 하드웨어 고장으로 인한 의료정보의 변질은 잘못된 진단으로 인한 생명의 위협으로도 연결될 가능성이 있다.

③가용성

의료정보가 저장된 무선 단말기, 랩톱 컴퓨터 등 도난사건 발생시나 정전이나 홍수·화재등 재난 발생시등 무시할 수 없는 기기의 고장으로 인해, 필요한 서비스를 제공하지 못하는 경우에는 저장된 의료정보의 비밀성뿐만 아니라 가용성도 위협하게 된다.

2) 의료정보화에 따른 보안 위협

의료의 분야에 있어서도 다른 분야처럼 의료기술의 진보등과 발은 맞추어 정보량은 현저하게 늘어나고 이를 효율적으로 다루기 위하여 정보기술과 통신기술이 도입되고 있다. 이에 따라 의료정보가 집적되게 되었고, 경우에 따라서는 의료정보를 쉽게 열람할 수도 있게 되었다. 따라서 정보기술의 도입은 어떤 의미에서는 환자의 개인정보로서 의료정보를 침해할 위험을 증대시키고 있다.

서울대병원, 세브란스병원, 서울아산병원, 삼성서울병원 등 전산망을 통한 전자의무기록제도를 채택하고 있는 국내 10개 대형병원을 조사한 결과에 따르면(중앙일보 2005) 10개 모두 환자의 진료 내역이 주치의 등 해당 진료의사 외 병원직원들에게 고스란히 노출되어 있는 것으로 밝혀졌다. 입원환자의 성명만 단말기에 기입하면 환자의 주민등록번호와 주소등 신상명세는 물론 혈액검사등 주요 검사 결과와 현재 어떤 약을 투여하고 있고, 어떤 수술을 받았는지 모두 알 수 있다고 한다. 여기엔 각종 성병과 인공중절수술 과거력, 정신병여부등 민감한 프라이버시가 담긴 내용도 담겨있다.

또한 환자들의 정보는 병원 직원들뿐만 아니라 의료정보 업체 직원들에게도 무방비로 노출되어 있다. 환자기록관리 상의 편의를 위해 상당수 병·의원에서는 프로그램 공급 업체 영업사원들이 언제든지 병원 환자정보를 병원외부로 유출할 가능성이 있는 프로그램(PC anywhere)을 설치하고 있기 때문이다.

그리고 의료기관 종별 정보보안제도 조사(2005) 결과에 따르면, 종합전문 요양기관 40개중 보안교육 및 보안서약서 작성등 인적 정보보안제도를 적용하고 있지 않는 곳이 16개(40%)다.

표2에서 보듯이 의료기관에서 생성되는 의료정보에 대하여 현재는 각 의료기관별로 통일된 지침이 마련되어 있지 않아 의료기관 내부지침에 의해 접근하고 있는 실정이다. 즉, 각 의료기관에 따라서 동일한 용도나 직책이어도 접근권한에 차이가 나는 것들이 있는데 이러한 접근 권한에 대한 통일적이고 객관적인 기준이 아직 마련되어 있지 않다는 것도 의료정보보호에 문제점으로 지적할 수 있다.

[표2] 현재 운영 중인 정보 보안 제도의 적용 범위

구분		종합전문	종합	병원	계
인적 정보 보안	보안교육실시및 보안서약서작성	8(20.0)	9(12.7)	11(6.4)	28(9.9)
	보안교육만실시	12(30.0)	30(42.3)	67(39.0)	109(38.5)
	보안서약서만 작성	4(10.0)	4(5.6%)	7(4.1)	15(5.3)
	적용안함	16(40.0)	28(99.4%)	87(50.5)	131(46.3)
	계	40(100.0)	71(100.0)	172(100.0)	283(100.0)
관리적 정보 보안	접근통제 및 사용통제 적용	29(70.7)	40(55.6)	57(32.8)	126(43.9)
	접근통제 적용	4(9.8)	12(16.7)	28(16.1)	44(15.3)
	사용통제 적용	7(17.1)	14(19.4)	49(28.2)	70(24.4)
	적용안함	1(2.4)	6(8.3)	40(23.0)	47(16.4)
	계	41(100.0)	72(100.0)	174(100.0)	287(100.0)

다음으로 환자 정보 유출을 3가지 사례를 살펴보고 개선방안을 찾아보고자 한다.

첫째, 내부자에 의한 환자 개인정보 유출 사례로 의료정보에 대한 권한이 없는 개인의 접근으로 의료정보가 폭로·조작될 수 있으며, 특히 병원내부자에 의한 환자개인의료정보의 유출 사례가 발생하고 있다. 지난 4월12일자 신문기사 중 미국 뉴욕 프레스비테리언(NYP)병원의 직원 한명이 병원에서 치료를 받았던 환자 4만명의 개인 신상기록을 빼돌린 사건을 예로 들 수 있다.

둘째, 동의 없이 개인 의료정보를 제공 및 과도한 개인정보 수집으로 인한 침해사례이다. u-Health의 경우, 센싱 기능의 부정확성으로 인한 진단오류 및 RFID등을 이용한 과도한 개인정보 수집은 환자 개인의 프라이버시를 침해할 수 있다.

마지막으로 기술적/관리적 조치 미비로 인한 개인정보 침해 사례이다. e-Health의 경우, 의료정보의 이동성이 증가하면서 의료정보에 대한 외부로부터 공격가능성이 증가하였다. 즉 원격지 환자를 진료하는 동안 교환 및 저장되는 데이터에 대한 보안 장치가 허술한 경우, 해커등 공격자들로부터 공격을 받아 민감한 환자 개인 의료정보가 유출될 수 있다. 지난 4월18일 전자신문 기사에 의하면 일본 의과대 부속병원에서 환자의 이름·병명·검사결과등 개인정보 1만7000여건이 기록된 PC가 감쪽같이 사라져 일본 경찰이 수사에 들어간 사건을 예로 들 수 있다.

4. 시사성 및 결론

1) 법제도적 측면

현재 개별 법령에 산재되어 있는 환자 프라이버시 보호 관련 법안을 일관된 법체계로 통합하여 환자의 권리를 보장하고 의료기관의 정보보호 수준제고를 위한 관련 법률과 제도를 정비하는 것이 가장 시급한 문제이다.

국내에서는 미국의 HIPAA 프라이버시 규정 및 보안 규정과 기타 국내외 관련 법령등을 참조하여 환자의 개인의료정보 보호를 위한 법률안 제정 작업이 진행중이다. 환자의 개인의료정보보호 법률안에는 환자 개인의 보건의료정보에 대한 프라이버시를 보장하기 위한 의료정보에 대한 접근 권한과 공개에 대한 조건 등의 내용뿐만 아니라 정보보호 수준 제고를 위한 의료정보 취급기관의 의무가 포함되어야 한다.

2) 기술적 측면

개인의료정보의 비밀성, 무결성, 가용성을 보장하기 위한 보안 대책을 표준 규정으로 개발·보급하여 개별 의료기관의 정보보호 수준을 제고할 필요가 있다.

또한 특정의료인으로 한정되어야 할 시스템 접근 권한 제한이 기술적으로 확립되어야 한다. 그 방법으로는 접근권한을 운영체제 레벨에서 통제하는 보안운영체제에서부터 시스템, 내부에서 일어나는 기술적인 침입까지 탐지하는 호스트 기반 침입시스템 IDS(Intrusion Detection System), 침입탐지 뿐만 아니라 접근까지 차단하는 IPS(Intrusion Protection System)가 있다. 또한 중요한 문서를 암호화해 저장하는 문서보안(DRM)과 중요 데이터의 위·변조를 방지하는 DB보안, 네트워크 트래픽이나 메시지 또는 이메일등을 감시하는 각종 솔루션등의 방법이 있다.

3) 관리적 측면

내부자에 대한 침해사례를 줄이기 위해서는 병원내의 정보보호 교육 및 물리적 보안을 수행하는 것이 중요하다. 또한 의무기록 자료 불출을 감시하거나 환자의 개인정보를 저장, 조회, 출력, 복사할 때 관리자의 승인 및 인증을 받도록 하는 관리적인 정책이 중요하다. 또한 환자 프라이버시 보호에 관한 윤리 또는 의무를 의료종사자들에 부과하는 것도 하나의 방법이다.

환자의 진료정보는 반드시 보호되어야 한다. 개인의 비밀정보를 개인의 승낙없이 활용하거나 유출하는 것은 범법행위이다. 법의 제재를 받기 전에 의료인 뿐아니라 모든 사람들이 의료정보의 유출이 심각한 윤리적인 문제임을 인식하여야 한다. 윤리적 바탕위에 강제성을 부여하는 예방적 측면에서의 법제화가 필요하다. 그래서 국민을 대상으로 하는 교육과 홍보가 필요하다.

진료기록이 전자의무기록으로 전환될 수밖에 없다. 이에 대한 법적 효력부여가 이루어지면서 보안 문제에 대한 제도적 기술적방법이 완벽하게 준비되어야 한다. 비밀 보장을 위한 하드웨어와 소프트웨어의 개발을 통한 기술의 보강이 필요하다. 또한 컴퓨터를 사용하는 사람들에 대한 책임의 소재도 항상 명확하게 정의되어야 한다.

5. 참고문헌

[1] 최준영, 병원정보시스템에서 개인정보보호에 관한 연구, 원광대학교 정보과학대학원 석사학위논문, 2007

[2] 왕경해, 국내의료기관의 정보화현황 및 관련요인분석, 연세대 보건대학원석사논문, 200602

[3] 곽은아, 병원정보시스템 관리상의 주요 이슈에 관한 연구, 연세대 보건대학원석사논문, 2006

[4] 김홍근, 지식정보사회 의료 패러다임 변화와 정보보안, 2006.05

[5] 환자정보의 보호와 보안(서울대 조한익 교수 발표자료)

[6] 의료기관 전산·정보화 실태와 문제점, 개선방안에 관한 연구(전국보건의료산업노동조합 연구자료)

[7] 김진태 외 2명, 네트워크 기반의 u-health 서비스 추진 동향, 주간기술동향 통권1321호

[8] 박건희, 보건의료정보화와 개인정보보호, 서울의대 의료관리학교실, 2006.06.20

[9] 웹기반 의료정보시스템 ASP사례(IT Service Conference2005발표자료), 현대정보기술 정상경과장

[10] 김동수/김민수, e-health 시대의 진전에 따른 의료정보보호 쟁점 및 정책방향, 정보화정책 제13권제4호, 2006년 겨울, pp.128~148

[11] 2005년/2006년 개인정보분쟁조정사례집

[12] 백윤철·김상겸, 미국의 의료정보보호에 대한 연구, 한국학술정보(주)

[13] 2000년 정보화역기능사례집, 한국정보보호센터, 2000.12

[14] 쿠키뉴스(2008.04.17)
http://www.kukinews.com/special/article/opinion_view.asp?page=1&gCode=opi&arcid=0920867096&sec=1343

[15] 비트컴퓨터, http://www.bit.co.kr/index.htm

[16] 전자신문
http://www.etnews.co.kr/news/detail.html?id=200804170140

[17] 뉴시스
http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=104&oid=003&aid=0002047431