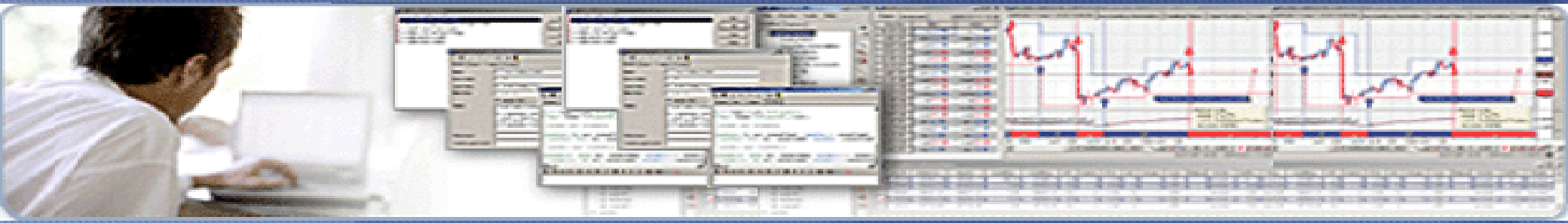
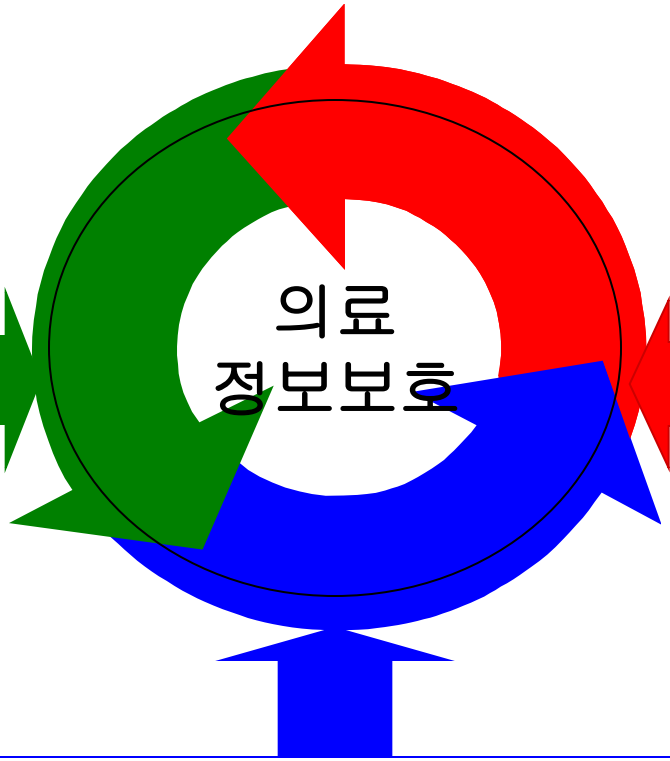
간호전문인으로서의
의료정보보호



정보관리에서
Ethics, privacy, & Security

의료정보보호의 필요성

의료의 질과 병원 경쟁력 향상을 위하여 의료정보의 **Digital**화 가속화됨



개인 의료정보의 악용 가능성이 증가

의료정보에 대한 보안요구 증대

의료보안에 대한 국민의식 강화

의료정보보호를 위한 법적/제도적 장치 필요

의료정보보호의 필요성

1)환자의무기록 최신성 유지 및 승인하의 접근관리

2)병원간의 중복 검사 및 불필요한 진료 방지

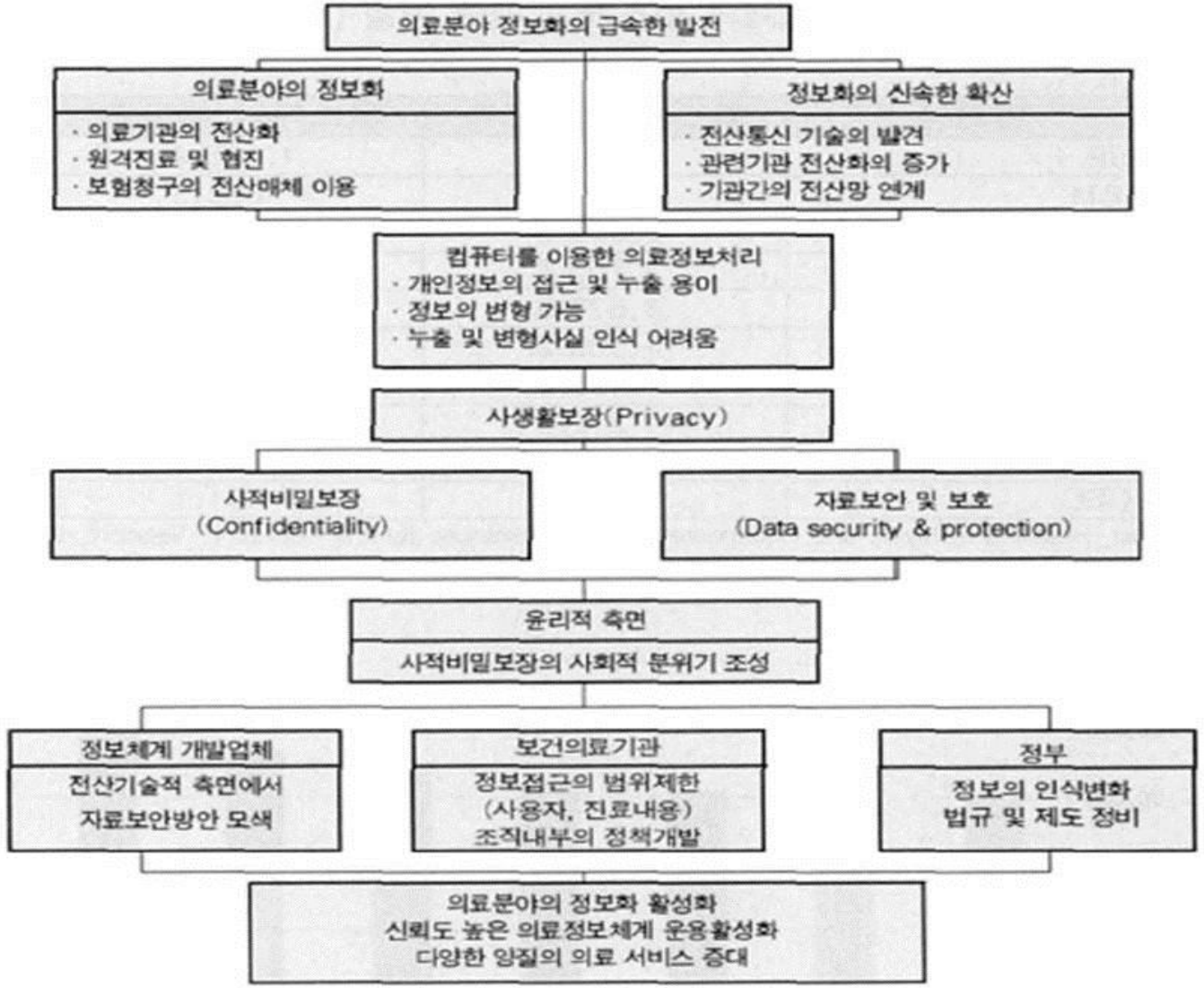
3)의료 과오 감소에 일조

4)공공 보건에 관한 사항, 특히 유행병의 발병이나 바이오 테러의 조기경보를 위한 중앙 정보관리 및 치료 연구 가능

5)향상된 품질과 저렴한 가격의 의료 기록 제공

6)사생활 보호

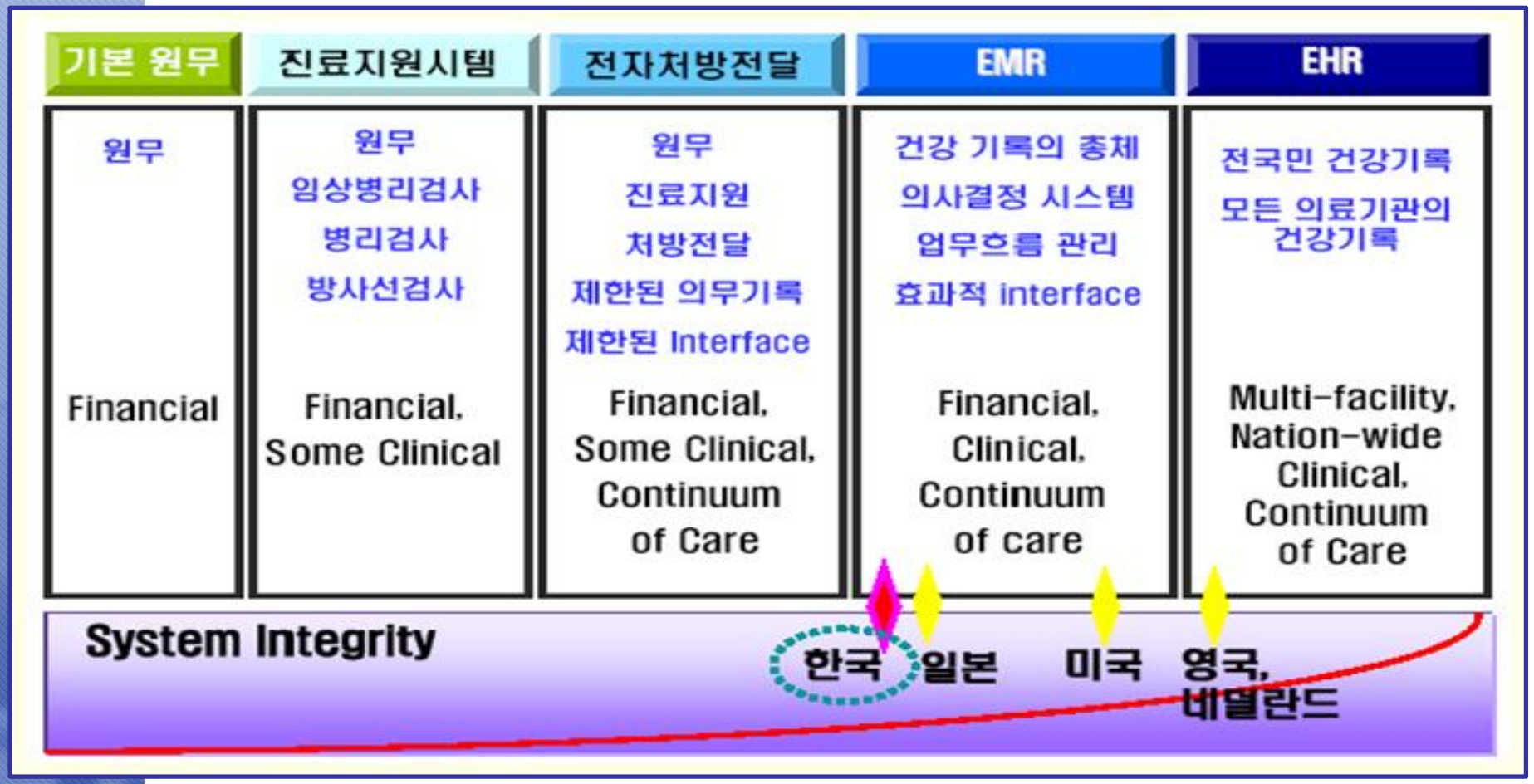
의료정보 보안의 필요성



〈그림 3〉 환자비밀보호의 배경과 필요성

출처) 의료정보보안의 현황과 전망, 임채균, 2010

주요국의 보건의료 정보화 수준



- 전체적인 국내 의료기관의 수준은 아직까지 의료정보화 도입단계인 원무업무 전산화 수준에 그치고 있음

출처 : community.snu.ac.kr/bbs/servlet/DownLoad?SEQ=24626

의료정보화에 따른 보안위협

PD수첩 진료비 부당청구의 비밀;2013-10-22

정보유출사례

사 례 1

내부자에 의한 환자 개인정보 유출 사례로 의료정보에 대한 권한이 없는 개인의 접근으로 의료정보가 폭로, 조작될 수 있으며 특히 병원 내부자에 의한 정보유출 사례가 발생하고 있다.

예) 미국 뉴욕 프레스비테리언 병원의 직원 한명이 병원에서 치료를 받았던 환자 4만명의 개인 신상기록을 빼돌림.

사 례 2

동의 없이 개인 의료정보를 제공하고 과도한 개인정보 수집으로 인한 침해 사례로 u-Health의 경우 센싱기능의 부정확성으로 인한 진단오류 및 RFID 등을 이용한 과도한 개인정보 수집은 환자 개인의 프라이버시를 침해 할 수 있다.

사 례 3

기술적/관리적 조치 미비로 인한 개인정보 침해사례로 원격지 환자를 진료하는 동안 교환 및 저장되는 데이터에 대한 보안 장치가 허술할 경우 해커 등 공격자들로 부터 공격을 받아 정보가 유출 되었다.

예) 일본의과대 부속병원에서 환자의 이름, 병명, 검사결과 등 개인정보 1만 7,000여건이 기록된 PC가 도난 당함.

의료정보화에 따른 보안위협

의료 정보의
불법 수집

의료 정보의
불법 축적

의료 정보의
불법 처리

의료 정보의
불법 이용

의료 정보의
불법 유통

의료 정보의
유출 피해

의료정보화에 따른 보안위협

▪개인의 건강에 대한 사항
▪환자의 병력기록

개인의 **사생활**에
매우 민감한 정보

사적 비밀보장

※ 개인 정보의
사생활 보장을 위해
취할 수 있는 방법

보 안

의료정보화에 따른 보안위협

우리의
보안 현실

http://www.zdnet.co.kr/news/news_view.asp?artice_id=20130614192302

의료정보보호를 위한 원칙

1) **건강증진의 목적**으로만 공개될 수 있다.

2) 해당 환자의 동의 없이는 공개되어서는 안 되며 자료를 획득한 자는 **반드시 비밀을 지켜야 할 의무**를 진다

3) 개인은 자신의 정보에 접근할 권리를 가지며, 자신에 대한 정보를 열람한 후 변경 을 요구할 수 있어야 하며, 정보 이용과 관련된 사항들에 대하여 **고지를 받을 권리**를 가진다.

4) 의료정보를 부당하게 취급하는 자는 **법적 책임**을 진다.

5) 의료정보에 대한 개인의 비밀은 국민건강, 의학연구, 의료보험 등의 필요성에 의하여 **침해되어서는 안 된다.**

보호대상 건강정보

(protected health information : PHI)

1) 정의

개인을 확인하거나 정보를 이용하여 개인을 확인할 수 있는 정보로 예전에 의무 기록이라 했으나 의무기록 외 정보도 보호 대상이므로 **보호대상 건강정보(PHI)**라 한다.

2) 분류

이름, 주소(거주지, 지역), 전화번화/팩스번호, 이메일/웹페이지/IP주소, 주민등록 번호/계좌번호, 병원등록번호/건강보험번호, 증명서/자격증 번호, 자동자 번호/차 량의 종류, 얼굴전체 이미지나 사진, 생물측정인식사항(지문, DNA, 목소리 등), 개인만의 특이사항 (점, 상처)

의료 정보보호의 필요성과 관련된 기사

보안 닷컴. 2011년 2월 16일 게재

: 의료 개인정보보호 '휴지조각' 병원 개인정보 가이드라인 무시. 개인정보보호법 발효 시급

환자의 병력이나 신체정보 등을 보유한 병원들이 정부의 개인정보보호 가이드라인을 거의 지키지 않는 것으로 나타났다.

전자의무기록(EMR), 처방전달시스템(OCS), 의료영상저장전송시스템(PACS) 등 병원 정보화시스템 보급률이 높아지면서 **전자화된 의료 개인정보의 다량 유출사고 위험이 커지는 추세**여서 행정당국의 강력한 관리가 시급한 실정이다.

16일 관련업계에 따르면 보건복지부가 지난해 마련해 배포한 '의료기관 개인정보보호 가이드라인'이 지난 1년 동안 일선 병원에서 거의 지켜지지 않는 것으로 조사됐다.

의료 정보보호의 필요성과 관련된 기사

- “거의 모든 대학병원에선 기존 정보화 담당부서 직원들이 보안에 대한 업무도 함께 맡고 있다”며 “평균 30억원 정도의 대학 병원 정보화 예산 중 보안 관련 비용이 따로 책정되지 않는 경우가 허다하다”고 말했다. 가이드라인에서 말하는 위원회나 감사는 더욱 찾아보기 힘들다. 서울아산병원·순천향병원 등 극히 일부에서만 최근 위원회를 구성해 활동하기 시작했다.

최근에는 한 소프트웨어 업체가 의료용 SW를 이용해 의료 데이터를 빼돌려 팔았다는 의혹까지 불거진 상태다. 대한의사협회도 진료비 청구 SW기업 유비케어가 지난해 11월 병·의원을 상대로 자료를 수집하는 과정에서 의사나 환자의 동의를 받지 않고 무단으로 환자 개인정보를 추출했다며 검찰에 고발해 법적 공방을 앞두고 있다.

…이하생략

정보 보안 관련 표준 및 가이드 라인

ISO 17799 (BS 7799)

- International Standards Organization, 국제 표준
- 포괄적인 관리적, 기술적, 물리적 보안 요구사항 포함

HIPAA

- Health Insurance and Portability and Accountability Act of 1996, 미국의 법률
- 의료정보의 안전한 보관・활용에 관한 법률
- 병원 준수 사항 제시

MEDIS - DC

- The Medical Information System Development Center, 일본 전자기록 연구기구
- 전자의무기록의 관리적 보안 사항 상세히 제시

ISO 17799

통제항목	통제사항
정보보호정책	정보보호 **정책의 문서화**, 정보보호 정책에 대한 **적절한 평가와 재검토**
정보보호조직	정보보호**위원회**(forum), 정보보호 조정기능, **책임**할당, 정보처리 설비에 관한 **권한**부여, 전문가의 정보보호 조언기능, 정보보호에 관한 조직 간의 협조, 독립된 인력에 의한 정보보호 적정성 검토, **제3자(third party)에 의한 정보보호 통제**, 문서화된 계약
자산의 분류와 통제	정보시스템에 관련된 **자산들에 대한 상세 정리** 및 책임자 명시, 정보자산의 비밀 정도에 대한 **적절한 등급** 분류, 정보등급표시, 등급에 부합하는 보호정책
인적 보안	인적 채용 과정에서 위험인물 배제, 정보보호 **교육 및 훈련**, 정보보호 통제에 대한 직원의 동의서 확보, 보안사고에 대한 **직원들의 적절한 대응과 보고**, 보안 위반자에 대한 **처벌**
준수관리	**정보보호 정책, 관련법규나 내부 규정, 표준** 등을 준수
시스템 운영 관리	**운영절차의 문서화**, 변경사항에 대한 통제, 사고관리체계, 직무분리, 개발시설과 운영시설의 분리, 외부 설비 관리, 시스템 계획, 악성코드에 대한 보호, 시스템 백업 및 로그, 네트워크 전자매체 취급 보안, 조직 간 정보교환시의 보안
접근 통제	**접근 통제 정책의 수립**, 사용자 등록, 특별 접속 권한, 패스워드 관리, 접속 권한의 재검토와 같은 사용자 접속 관리, 패스워드 사용시의 사용자 책무, 자리를 비운 기기에 대한 관리와 같은 사용자 책무, 네트워크 접근통제, 운영체제 접근통제, 응용 시스템 접근 통제, 시스템 접속과 사용에 대한 모니터링, 모바일 컴퓨팅과 원격근무의 보안사항
업무 지속성 관리	비상사태 발생시 **조속한 복구를 위한 관리적 대책** 수립

HIPAA

통제항목	통제사항
보안 관리 과정	위험분석, 위험관리, 제재정책, 정보 시스템 활동 점검
보안책임자 지정	전직원 대상 보안 권한 부여 및 감독, 직원접근 절차, 접근 권한 종료
정보 접근 관리	의료정보센터 접근절차, 접근승인, 접근권한 변경
보안인식 및 훈련	보안의식 상기
보안사고 처리 절차	대응 및 보고
비상계획	자료백업계획, 테스트와 개정절차
재해복구계획	어플리케이션 중요성 평가
비상시 운영계획	자료의 중요성 평가
기타	악성소프트웨어 보안, 로그인 모니터링, 패스워드 관리, 평가, 서면계약과 협정

반드시 알아야 할 개정된HIPAA법의 4가지 조항

2013년 1월에 개정된 HIPAA의 4가지 조항.

- 비지니스 파트너와 하청 업체도 환자 의료 정보 보호에 대한 의무를 지게 되었다. 기존에는 계약서에 명시된 경우에만 해당되었지만, 새로운 법에서는 의료 정보의 전달이나 저장을 담당하는 업체 및 클라우드 서비스 제공자도 해당된다.
- 환자가 자신의 의료 기록을 전자 형태로 언제든 발급 받을 수 있게 되었다. 또한 필요하면 다른 의사나 간병인, 온라인 사이트 및 모바일 앱 등으로 보내달라고 요청할 수도 있다.
- 환자가 자신의 의료 정보의 공개를 제한하도록 요청할 수 있는 권한이 향상되었다. 예를 들어, 환자 자신이 의료비를 모두 부담하는 경우에 관련 의료 정보를 보험 회사에 알리지 않도록 병원 측에 요청할 수 있다.
- 모든 개인 의료 정보의 노출은 전부 사고로 보고해야 한다. 예전에는 정보의 누출이 재무 리스크나 평판 리스크가 큰 경우나 개인에게 해가 되는 경우에만 보고해야 했으나 지금은 의료 서비스 제공자가 정보 누출이 개인에게 피해가 없다는 것을 입증해야 한다. 개인 정보에 허가되지 않은 수집, 접근, 사용 및 공개는 의료 서비스 제공자가 해당 사고 발생 가능성이 매우 낮다는 것을 리스크 평가를 통해 입증할 때까지 누출 사고로 간주된다.

MEDIS - DC

일본 보안 지침 사항
정보보안의 정의 및 전체의 목적과 범위
정보보안의 목표와 원칙을 지시하는 경영진의 의사표명
의료기관 특유의 **보안방침, 원칙, 표준, 승낙의 필요요건 기술**
법규 및 계약상의 요건 승낙
보안에 대한 교육 - 바이러스 예방 및 검출 방침
전자의무기록시스템에 관한 의료업무의 계속 계획방침
진료에 관련되는 정보에 대해서 누구에게 어느 정도의 **권한**을 부여하는 것에 대한 권한 결정
긴급시(응급시)전자의무기록시스템의 이용(접근성)**방침**
정보보안의 모든 측면의 전반적 및 특정적 책임의 정의
보안에 관한 보고(분쟁이 발생한 경우 등)의 방법에 대한 설명
정보보안 방침을 구체적으로 실현 할 지침(guideline) 마련
보안방침을 시스템의 변경 등에 대비해서 적절하게 사용할 수 있는 방안 마련
보안 지침서 의료기관의 전원에게 배부, 교육

정보 보안의 핵심영역

전산시스템의 안전한 운영을 위한 *DB,S/W,H/W*

조직의 거시적 측면에서 보안문제를 다룸

5년 내 지식정보보안산업 규모는 **10**조 원에 이를 것 2012-12-10 16:54:00
http://news.donga.com/It/Com/3/0809/20121210/51473333/3

정보의 요인적 특성

기밀성의 정의 및 위험성

정의

- 합법적인 사용자가 아닌 사용자들은 컴퓨터 시스템상이 데이터 또는 컴퓨터 시스템 간에 통신회선을 통하여 교환, 전송되는 데이터의 내용을 볼 수 없게 하는 기능

위험성

- 환자의 의무기록 접근성 용이
- 무선으로 의료정보 전송
- 지나가던 사람에게 정보 공개 위험
- 작업중인 사람 뒤에서 훔쳐보는 행위

무결성의 정의 및 위험성

정의

- 정보가 오직 허가된 사람들에게만 접근가능하고, 또 그들에 의해서만 수정 또는 변경될 수 있음을 보장하는 것을 의미

위험성

- 컴퓨터 바이러스 등의 악성코드로 인한 의료정보의 파괴
- 시스템 소프트웨어 버그나 하드웨어 고장으로 인한 의료정보 변질

가용성의 정의 및 위험성

정의

- 시스템을 구성하는 요소가 일정 시간 동안 일정 조건에서 필요한 기능을 수행할 수 있는 확률
- 필요할 때 정보 네트워크에 접근 가능한 것

위험성

- 정전이나 기상재해와 관련한 데이터의 손실
- 의료정보가 저장된 단말기의 도난 발생 등

관리적 보안의 정의

- 보건의료 자료와 정보에 대한 거시적 차원의 보완
- 보안정책, 보안절차, 보안지침, 보안조직

가이드라인 중 개인정보보호 및 보안에 관한 관리적 지침

개인정보보호 및 보안관리조직

- 개인정보보호위원회
- 의료기관 대표자의 책임
- 개인정보관리책임자, 보호 및 보안 실무책임자
- 개인정보취급자의 책임
- 개인정보보호 관련 고충처리
- 개인정보보호 감사 및 외부안전진단

개인정보보호 및 보안관리정책

- 개인정보보호 및 보안정책의 운영방안
- 관련법령의 준수

가이드라인 중 개인정보보호 및 보안에 관한 관리적 지침

인적 관리

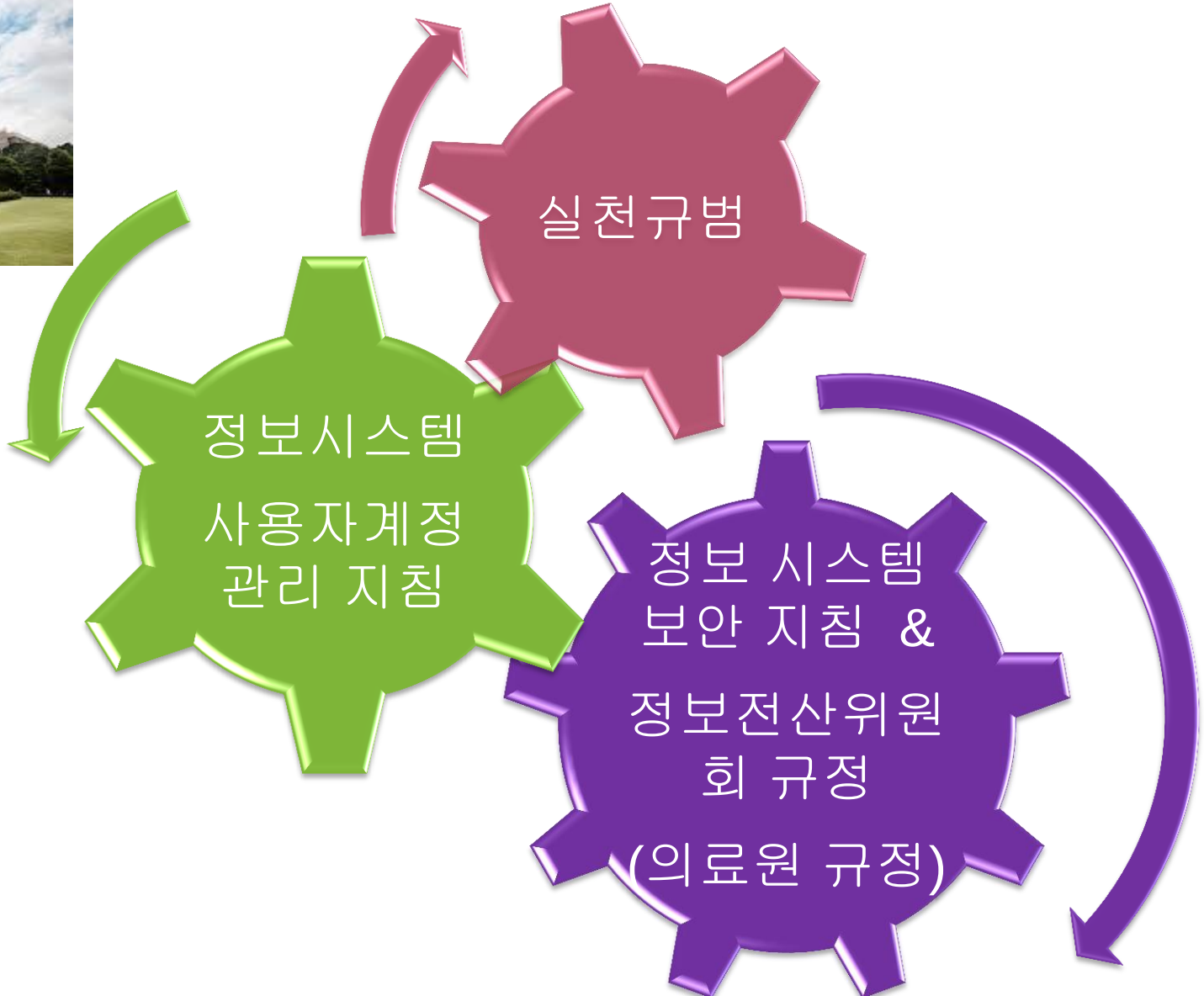
- 채용시 관리
- 직무수행 관리
- 교육 및 훈련
- 직무 변경 및 퇴직 관리
- 외부자 및 위탁업체에 대한 관리

정보자산관리

- 정보자산의 목록화
- 정보자산의 관리자 지정
- 정보자산의 보안등급 평가
- 개인정보 취급의 특정

고려대학교 의료원의 관리적 보안 현황

출처 :
http://anam.kumc.or.kr/introduction/newsView.do?BNO=677&cPage=18&BOARD_ID=B022



고려대학교 의료원의 관리적 보안 현황

출처 :
http://ask.nate.com/qna/view.html?n=8862189

<정보보안관리 제13조>

고려대학교 의료원 포탈사이트, 의료원 광장-윤리경영-실천규범

♣ 교직원은 직무수행 중 취득한 환자의 정보는 치료 목적으로만 이용하며 정보를 누설하거나 부당하게 이용하지 않는다.

♣ 교직원은 환자 정보의 유출에 따른 일차적인 책임이 있음을 인식하고, 환자 정보보호 준수에 최선을 다한다.

♣ 교직원은 병원 내부의 지적 재산, 기밀 정보는 적절한 사전허가나 절차 없이 외부에 유출하지 아니한다.

♣ 교직원은 대화 또는 통화 중 병원 내부의 기밀정보가 유출되지 않도록 주의한다.

고려대학교 의료원의 관리적 보안 현황

출처 :
http://ask.nate.com/qna/view.html?n=8862189

<정보시스템 보안 지침 , 총칙 – 고려대학교 의료원 규정 중>

정보시스템 자산 분류

- 보안 등급 : 일반/대외비, 작성자의 해당 부서장 결정
- 소유권 : 의료원
- 작성 부서장은 해당 자산에 대한 관리 책임과 배포 권한 가짐
- 외부입수자료 : 입수자 등급 분류, 보관

보안서약

- 입사 시 모든 교직원, 일정기간 이상 근무하는 모든 외부업체 임직원(계약직 포함) 작성

입・퇴사/전배 보안

- 퇴직자 발생 시 2주 이내 해당기관 보안담당자 통보, 접수 즉시 해당 사용자 계정 등 사용 권한 폐기
- 타부서 전배 시 2주 이내 해당기관 보안담당자 통보, 접수 즉시 기존 정보시스템 사용권한 회수, 전배 부서장은 정보시스템 사용권한 문서 요청
- 보직자 변동 시 인사부는 보안관리자에게 변동 현황 통보

고려대학교 의료원의 관리적 보안 현황

출처 :
http://ask.nate.com/qna/view.html?n=8862189

<정보시스템 보안 지침 , 보안조직 구성 >

보안조직 구성

- 정보 전산 위원회 – 정보 보안 실무 협의회

정보보안실무협의회

- 의장 : 정보전산실장
- 위원 : 정보기획팀장, 정보운영팀장 및 각 파트장과 정보시스템 실무담당자 (각 병원 및 보건과학대학 네트워크 관리자, 시스템 관리자, PC 관리자)
- 임기 : 보직재임기간 및 해당 업무 기간
- 보안관리자(의료원 전체 보안관리 총괄) : 의료원 정보운영팀장
- 보안담당자 : 해당기관 정보시스템 실무 담당자 중 1인
- 정보시스템 실무 담당자

고려대학교 의료원의 관리적 보안 현황

출처 :
http://ask.nate.com/qna/view.html?n=8862189

<정보시스템 보안 지침 , 정보자산의 분류 및 통제, 인적 보안>

정보시스템 자산 분류

- 보안 등급 : 일반/대외비, 작성자의 해당 부서장 결정
- 소유권 : 의료원
- 작성 부서장은 해당 자산에 대한 관리 책임과 배포 권한 가짐
- 외부입수자료 : 입수자 등급 분류, 보관

보안서약

- 입사 시 모든 교직원, 일정기간 이상 근무하는 모든 외부업체 임직원(계약직 포함) 작성

입・퇴사/전배 보안

- 퇴직자 발생 시 2주 이내 해당기관 보안담당자 통보, 접수 즉시 해당 사용자 계정 등 사용 권한 폐기
- 타부서 전배 시 2주 이내 해당기관 보안담당자 통보, 접수 즉시 기존 정보시스템 사용권한 회수, 전배 부서장은 정보시스템 사용권한 문서 요청
- 보직자 변동 시 인사부는 보안관리자에게 변동 현황 통보

고려대학교 의료원의 관리적 보안 현황

출처 : http://www.tpcc.or.kr/board/prodataBoardList.mctp?CONTENT_SUMMARY=S1&currentPage=4

<정보시스템 보안 지침 , 인적 보안>

보안교육

- 년 1회 정기교육, 필요시 수시 교육
- 온라인, 비디오, 문서 등의 형태 가능
- 내용 : 정보보호 일반, 보안정책・지침 및 관계법령 소개, 일반 사용자 보안

보안사고 대응

- 보안관리자의 조치
- 침입 가능성 수시 점검, 불법 침입 사전 예방
- 시스템 비정상적 활동, 징후 시 무단 침입자 유무 즉각 점검
- 해킹에 따른 즉각 조치, 협의회 의장에게 보고
- 침입해결, 침입흔적 발견시 즉시 협의회 의장에게 보고, 정보자산 이상유무 점검

보안사고 상벌제도

- 보안관리자 , 보안위반사항 발생시 정보전산위원회에 보고
- 위원회는 심의 거쳐 해당 징계위원회에 회부
- 우수 교직원, 우수 부서 포상, 홈페이지 또는 포탈에 공지

고려대학교 의료원의 관리적 보안 현황

출처 : http://www.tpcc.or.kr/board/prodataBoardList.mctp?CONTENT_SUMMARY=S1&currentPage=4

<정보전산위원회 규정 – 고려대학교 의료원 규정 중>

목적

- 위원회의 구성과 운영에 관한 사항 규정 → 정보전산 발전을 위한 방향제시와 효율적인 정보전산관리 운영 유지, 증진

기능

- 의료원의 정보화 전략 및 추진 방향 심의
- 의료원의 정보화 투자 계획 심의
- 정보시스템의 통합화 및 표준화 심의
- 정보기술의 교육에 관한 사항 심의
- 정보시스템 보안에 관한 사항 심의
- 소위원회 (병원 별 OCS 위원회, 부문별 위원회, 기타 실무 소위원회)에서 부의된 요구사항 중 중요정책 심의
- 기타 의료원장의 지시사항 및 위 내용의 부수 사항 심의

구성 및 임기

- 당연직위원 : 정보전산실장, 사무국장, 정보기획팀장, 각 병원 기획실장, 각 병원경영관리실장 (보직 재임기간)
- 위촉위원 : 의료원장이 위촉하는 위원, 15명 이내 (2년)

기술적 보안의 정의

- 보건의료 자료와 정보에 대한 접근을 통제하는데 사용되는 정책과 절차(HIPAA)

- 전산시스템의 안전한 운영을 위한 운영체제 DB, 소프트웨어, 하드웨어 등을 보안기술을 이용하여 보호하는 행위 (안선주, 2005)

개인건강정보 보안이 필요한 영역

이 모든 영역에서 정보보안이 필요함

의료정보보호를 위한 병원에서의 기술적 대책

PIMS: Personal Information Management Software (개인정보보호관리체계인증)

항목 위주로 접근

1) 접근통제 정책 수립 및 개인정보 취급자의 접근통제/모니터링 이행

가) 개인정보보호 요구사항에 기초한 *접근통제 정책 수립* 여부

⇒ 현재 개인건강정보 관리 시스템의 담당자별 업무분장에 따라 개인건강정보에 접근할 수 있는 권한을 차별화하고 개인건강정보의 대상과 범위 등을 차별화한 접근권한 관리를 하고 있다.

나) *개인정보 취급자의 계정관리*절차 문서화 및 시행 여부 등

다) 개인정보취급자 *최소 접근 권한관리* 시행 여부 등

⇒ 각 병동 및 부서에서는 각 정보에 접근권한을 다르게 가지고 있다. 예를들어 EMR 정보 조회의 권한은 EMR 동의서를 작성한 직원들에 한해 조회가 가능하고, 좀 더 취약한 환자로 보고 있는 정신과 환자들의 정보접근 권한은 정신과에 근무하고 있는 의사, 간호사에게만 주어져 정보의 노출을 최소화한다.

PIMS 인증제도란?

개인정보보호 관리체계(PIMS)란 기업의 개인정보를 지속적으로 관리·운영하기 위한 종합적인 체계를 말하며, 이를 인증하는 제도가 PIMS인증

PIMS 인증제도 추진 배경

❖ **인증제도 기반 마련 (2009년)**
- 개인정보보호 관리체계 인증 심사항목 개발
- 대량 개인정보 취급 사업자 대상 모의 인증 수행

❖ **기반요소 검증 (2010년)**
- 사업자 규모별 모의인증 수행
- 개인정보보호관리체계인증 공청회

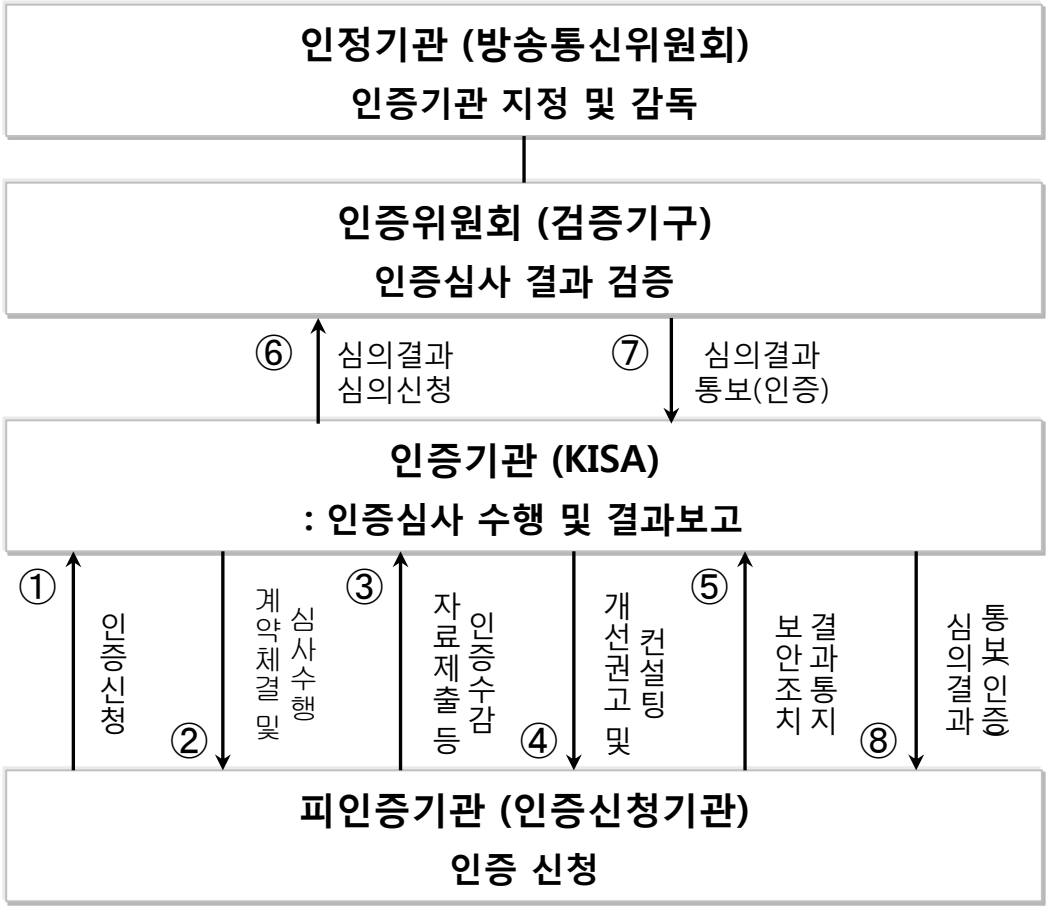
❖ **개인정보보호 인증제도 도입 (2010.11.15)**
- 개인정보보호 인증제도 방송통신위원회 의결

PIMS 인증 심사비용

산정기준	대기업	중규모 기업
개인정보취급자 어플리케이션 개인정보취급 DB	1200명 20대 1대	40명 1대 1대
*인증심사비용	약 1500만원	약 700만원

※ 심사비용 = 신청비 + 직접인건비 + 직접 경비

PIMS 인증 신청 절차



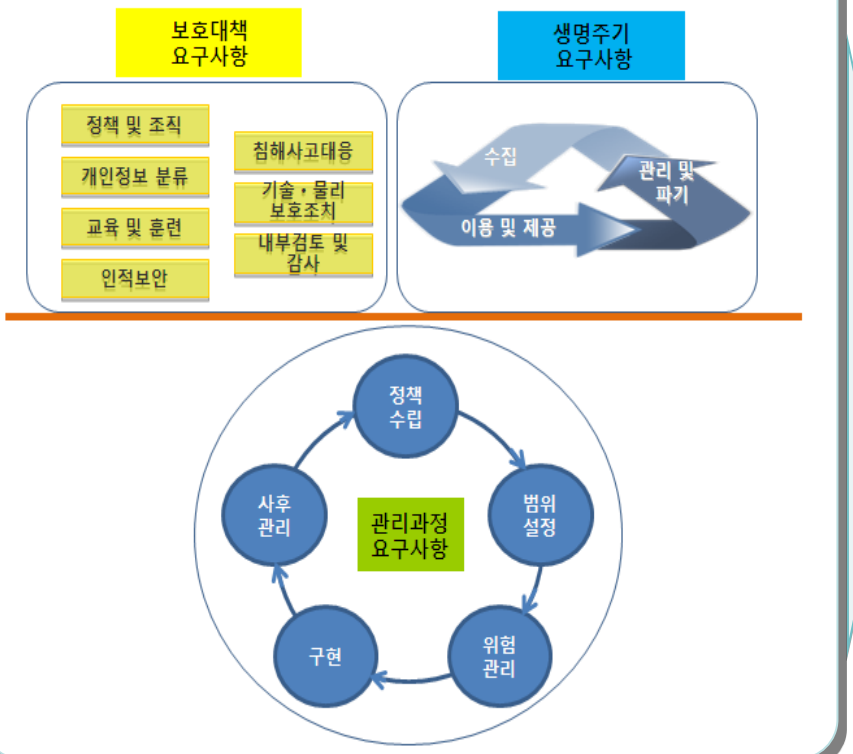
출처) 개인정보보호관리체계인증(PIMS) 컨설팅 소개자료, Infosec/SK C&C

PIMS 구성요소

개인정보보호 관리체계(PIMS))는 개인정보 보호를 체계적·지속적으로 관리하기 위한 **3**개 분야, **199**개 통제사항, **325**개 세부점검 항목으로 구성

PIMS 구성 및 점검항목

<PIMS의 구성>



<PIMS인증항목>

관리과정 요구사항

개인정보보호 활동을 체계적, 지속적으로 수행하고 있는지 기본 체계를 점검

보호대책 요구사항

개인정보를 안전하게 보호하기 위한 관리적.기술적 물리적 보호조치를 점검

생명주기 요구사항

법률에 명시되어 있는 개인 정보 생성에서 파기까지 생명주기 요구사항 점검

분야	세부분야	점검항목수	
		필수	선택
관리과정	1. 정책수립	5	0
	2. 범위설정	5	0
	3. 위험관리	6	1
	4. 구현	2	0
	5. 사후관리	4	0
소계	**5**	**22**	**1**
보호대책	1. 개인정보보호정책	11	0
	2. 개인정보보호조직	9	0
	3. 개인정보 분류	5	2
	4. 교육 및 훈련	7	0
	5. 인적보안	8	1
	6. 침해사고처리 및 대응절차	15	5
	7. 기술적 보호조치	106	19
	8. 물리적 보호조치	11	1
	9. 내부검토 및 감사	23	1
소계	**9**	**195**	**29**
생명주기	1. 수집	17	0
	2. 이용 및 제공	49	0
	3. 관리 및 파기	12	0
소계	**3**	**78**	**0**
합계	**17**	**295**	**30**

출처) 개인정보보호관리체계인증(PIMS) 컨설팅 소개자료, Infosec/SK C&C

의무기록 사용자별 권한

영상 의무기록의 사용자별 권한

(12.1 의무기록 보안에 대한 규정)

영상 의무기록의 작성. 열람 및 검색권한을 의미하며, 영상 의무기록은 환자의 진료 상태에 따라 외래. 입원으로 구분된다. 이에 대해 직종별. 업무별로 의무기록에 대하여 열람, 출력, 스캔/검수, 권한관리 등의 권한을 갖고, 권한관리자는 정기적으로 접근권한에 대해 관리한다.

(표1. 직종별 영상 의무기록 권한관리 참조)

가. 의사를 제외한 직종에서는 환자 개인정보 비밀유지를 위한 서약서(별첨 1)를 작성하고 권한을 부여받는다.

나. 간호사의 경우 진료목적으로 사용되는 외래진료, 입원진료 환자에 대한 의무기록 열람권한을 갖고, 간호부 팀장급 이상은 요청 시 진료 외 용도로 열람 가능하다.

다. 열람 권한을 위배하거나, 접근이 허락되지 않은 의무기록을 열람, 변조, 훼손시킨 자에 대한 경고 및 조치는 의무기록 관리위원회를 통해 처리한다.

의무기록 사용자별 권한

구 분				열람	출력	스캔/검수	권한관리	서약서	비고
진료	의사	수련의	진료, 수련, 연구	0	×	×	×	×	
		전공의		0	×	×	×	×	
		전문의		0	×	×	×	×	
간호	간호부	병동간호사	간호	0	×	×	×	0	재원중 환자만 검색가능
		외래간호사		0	×	×	×	0	외래 진료 환자만 검색 가능
		간호팀장급이상		0	×	×	×	0	요청 시 진료이외 용도로 검색 가능
진료지원	의료정보팀	의무기록사	권한관리	0	0	0	0	0	2개월 주기로 암호 변경
			정보분석	0	0	0	×	0	
			기타	0	×	×	×	0	
		일반업무원	스캔/검수	0	×	0	×	0	
			대출관리	0	0	0	0	0	
		기타	사본발급 및 열람	0	0	0	×	0	의무기록 사본 발급 신청된 경우만 출력 가능함
			정보분석	0	×	0	×	0	
			편집기타	0	×	0	×	0	
	영양팀	영양사	영양상담	0	×	×	×	0	
	약제팀	약사	복약상담	0	×	×	×	0	
	사회사업팀	사회복지사	환자상담	0	×	×	×	0	
	재활의학과	물리치료사	치료	0	×	×	×	0	
		작업치료사	치료	0	×	×	×	0	
		언어치료사	치료	0	×	×	×	0	
	기타진료지원	의료기사	검사시행 및 결과 확인	0	×	×	×	0	
행정	보험심사팀	행정직	보험심사	0	0	×	×	0	
	원무팀	행정직	법무	0	×	×	×	0	
		행정직	산재관리	0	×	×	×	0	
		행정직	진료비관리	0	×	×	×	0	
	전산운영팀	행정직	프로그램관리	0	×	×	×	0	
기타	교육수련팀	의대실습학생	수련 및 연구	0	×	×	×	0	아이디, 패스워드는 전산운영팀에서 관리

의무기록 사용자별 권한

(OCS / MIS)프로그램 사용자권한 신청서

요청부서	담 당	부서장	병 원 명 : 요청부서 : 요 청 자 : 요청일자 :	승인부서	담 당	부서장	전산운영	담 당	팀 장

구 분	세 부 사 항	비 고
요청메뉴		
요 청 사 유		
적용일자	2010년 월 일 부터	
기 타		

고려대학교 구로병원 전산운영팀

[별표 2] 정보시스템 사용권한

종합의료정보시스템 사용 신청서

요청부서	담 당	부서장

병 원 명 :
요청부서 : TEL :
요 청 자 :
요청일자 : 20 년 월 일

전산운영팀	담 당	팀 장

신청사유	□ 신규 ID 신청 □ 사용프로그램 메뉴 추가 신청		
직 종		사 번	
신규 ID	신규 ID 분리은 전산운영팀에서 분리 후 개별 통보	비밀번호	초기 비밀번호는 ID와 동일 각 사용시스템 초기 접속 후 변경
사용시스템	□OCS □MIS □PDSS □PORTAL □영상PACS □기타(다수선택가능)		
사용메뉴 추가신청			
주의사항	- 초기 접속 후 필히 비밀번호 변경		
기 타			

출처) 구로병원 OCS, 전산운영팀 공지사항

의무기록 사용자별 권한

환자 개인정보 비밀유지를 위한 서약서

목 적 : _____

소 속 부 서 : _____

사 용 자 명 : _____ 사 용 자 ID : _____

본인은 상기 목적을 위해 알게 된 환자의 개인에 관한 정보를 명시한 목적으로만 이용하며 보고서나 기타의 형태로 유출하지 않을 것이며, 본의의 불법공개나 사용, 노출로 인한 법적 처벌도 감수할 것과 비인가자의 불법적 사용을 막기 위해 본인의 비밀번호 관리 등에 주의를 기울이고 본인의 계정과 관련된 모든 사용에 대한 법적 책임을 질 것을 서약합니다.

관련근거 :

- 의료법 제19조(비밀누설의 금지) : 의료인은 이 법이나 다른 법령에 특별히 규정된 경우 외에는 의료 · 조산 또는 간호를 하면서 알게 된 다른 사람의 비밀을 누설하거나 발표하지 못한다.
  제88조(벌칙) : 3년 이하의 징역이나 1천만원 이하의 벌금에 처한다
- 의료법 제23조(전자의무기록) 제3항 : 누구든지 정당한 사유 없이 전자의무기록에 저장된 개인 정보를 탐지하거나 누출 · 변조 또는 훼손하여서는 아니 된다.
  제87조(벌칙) : 5년 이하의 징역이나 2천만원 이하의 벌금에 처한다

작 성 일 : 20 년 월 일

신 청 자 : _____ (서명)

소속팀장 : _____ (서명)

간호부장 : _____ (서명)

고려대학교 구로병원장 귀하

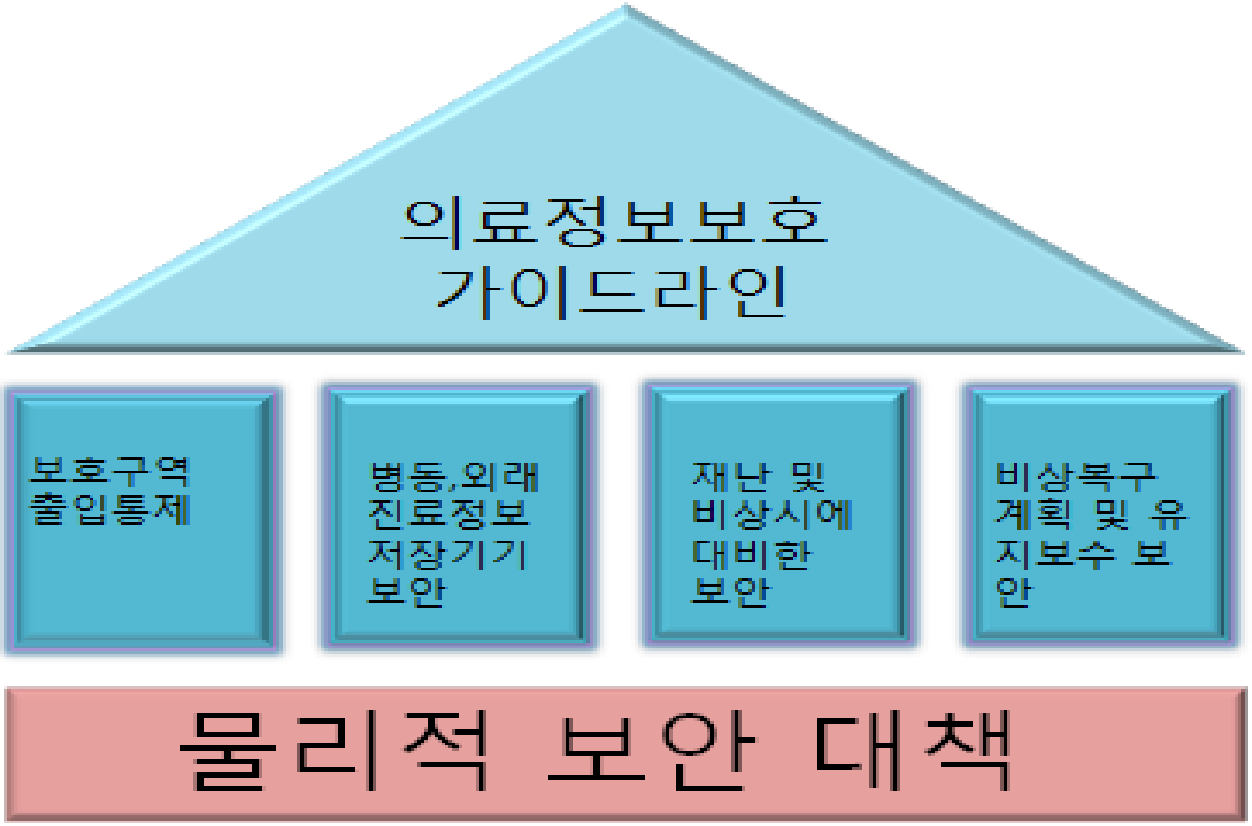
출처) 구로병원 OCS, 전산운영팀 공지사항

물리적보안의 정의

물리적 보안

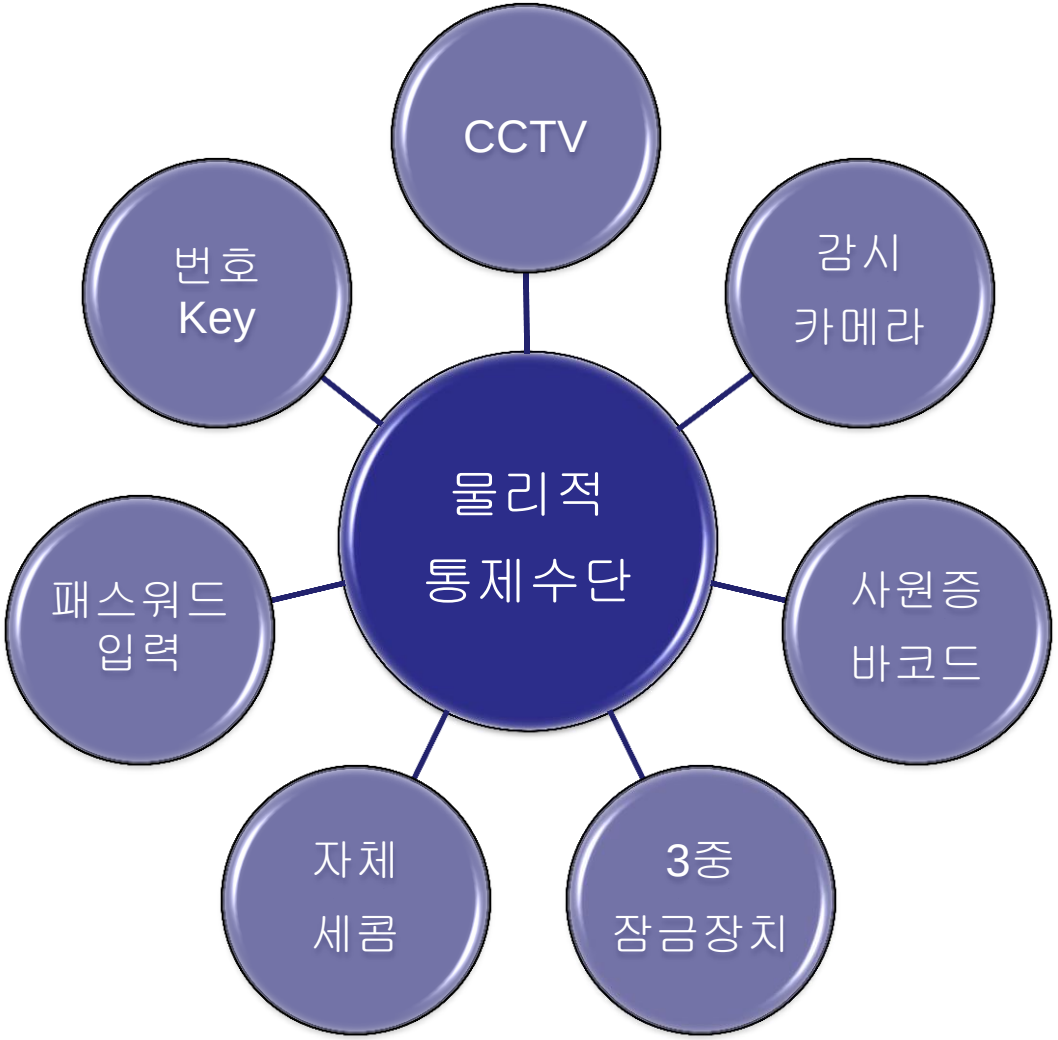
물리적 보안은 간과하기 쉽지만 중요한 보안영역이다.
출입통제, 시설물 관리, 안정적 전원 공급장치 등에 대한 사항을 말한다.
전산장비와 서버가 위치해 있는 전산센터가 주요 보호 대상이며 의료기관의 경우 각 병동, 외래 등 전산기기가 놓여있거나 사용되는 공간을 포함한다.

의료 정보 보호 대책- 물리적 보안



http://www.boannews.com/media/view.asp?page=1&idx=21019&search=&find=&kind=1 - 재구성

보호구역에 대한 출입통제



보호구역에 대한 출입통제-가이드라인

<<보호구역 시설 기준>>

- 개인정보가 포함된 전자 매체 장치를 설치하는 장소에 대한 물리적 기준

- 보호구역 경계를 명확하게 확정하여야 한다.
- 보호구역은 물리적으로 견고하여야 하고, 외부의 무단 침입을 차단할 수 있는 물리적 시설을 갖추어야 한다.

- 적정한 종류의 소화기와 소화설비를 소방법에 의거하여 적정 위치에 설치, 관리하여야 한다.
- 자연 재해에 대비한 비상대책이 수립되고, 이에 따른 직원들의 비상훈련이 정기적으로 이루어져야 한다.

<<보호구역 출입에 대한 통제기준>>

- 개인정보 보호구역은 인가된 사람만이 출입 가능하도록 출입통제 장치를 설치하여 보호하도록 하여야 한다.

- 개인정보 보관, 처리 공간에는 허가된 사람만 접근 허용

- 개인정보 보호구역의 출입허용을 식별하기 위한 별도 출입증(출입카드 등) 제공 및 패용
- 보호구역 출입자의 출입 시간을 기록 관리
- 상시 근무자가 없는 보호구역에 대한 잠금
- 보호구역에서 외부인력 투입 작업 시 감독자가 없는 작업 금지
- 물리적 출입통제 권한에 대한 주기적인 검토 및 불필요한 출입권한의 관리(출입증의 회수 등 포함)
- 반출, 반입되는 물품은 자산관리 정책에 따라 반출. 입 등록

병동, 외래 등에서의 진료정보저장 기기 보안

진료 정보저장 PC- 병동 및 외래에서 진료정보가 저장된 전산기기에 부적절한 접근을 차단할 수 있는가		
병동 및 외래의 PC 무방비 노출	기타 원내장소에서 진료정보가 저장된 전산기기에 무단 접근이나 도난	복사기, 스캐너 , 팩스 등 사용 후 노출

진료정보저장 기기 보안-가이드라인

<<자리비움시의 정보시스템 보안>>

- 모든 사용자는 자리를 비울 때 비 인가된 접근으로부터 의료정보시스템 및 데이터를 보호하기 위한 책임을 갖고 있다는 것을 인식하여야 하며, 이에 상응하는 조치(예: 로그아웃, 화면보호기 등)를 시행하여야 한다.

- 암호로 보호되는 화면보호기와 같은 적절한 잠금장치가 없을 경우, 활성화된 세션을 종료한다.

▷ 설명 및 예시

- 사용자는 정해진 작업을 마치고 자리를 비울 때, 비인가된 접근으로부터 의료정보시스템 및 데이터를 보호하기 위하여 로그아웃 하여야 한다.

- 컴퓨터 단말기에 대한 로그오프, 화면보호기 또는 키보드 잠금장치를 의미.

>사용자가 OCS 프로그램을 자신의 아이디로 열어둔 채로 잠시 자리를 비우는 때에는 키보드 잠금장치가 필요함[허가된 IC 카드를 꽂지 않으면 컴퓨터의 모든 기능이 잠기는 상태]. 이 상태에서 몇 분[=사용자가 지정한 시간]이 지나면 의료정보서비스를 실행하는 프로그램은 자동 종료되고 화면보호기 등이 작동됨.

재난 및 비상시에 대비한 보안

안전전원 공급	• 자체발전기, 이중전원선, 자동전압조정기
백업센터 장소	• 전산실, 병원건물, 건물 외부 등
비상계획	• 화재, 재해 등을 대비한 정보시스템 장소별 비상계획

재난 및 비상시 보안-가이드라인

<< 저장매체의 관리>>

- 정보 보안대상으로 관리되는 매체에 대해서는 사용 및 폐기 인가절차를 마련하여야 하며, 매체에 의한 불법적인 정보유출을 방지하기 위해 취약점 분석을 위한 점검 작업을 주기적으로 수행하여야 한다.

- 모든 매체는 매체의 보관 방식에 따라 안전한 보안 환경에서 보관되어져야 한다.

- 모든 저장 매체는 더 이상 사용되지 않을 경우 정식 절차에 따라 안전하게 폐기하여야 한다.

비상복구 계획 및 유지보수에 대한 보안

수립된 비상계획의 정기적인 모의 훈련

- 비상계획의 정기적인 모의 훈련실시
- 테스트 결과의 반영

시스템 장비의 유지 보수내역

- 관리 현황

정보 보호와 관련된 기사

누가,왜?농협전산망 마비 3가지 시나리오

[중앙일보] 입력 2011.04.22 02:06 / 수정 2011.04.22 09:26

1. 농협이 보안규정을 준수하지 않은 정황이 포착됐다. 규정상 서버 관리자와 농협 직원이 권한을 나눠 갖게 돼 있는데 실제로는 업무 편의를 위해 유지·보수를 맡은 협력업체나 하청업체 직원도 이 권한을 모두 가졌던 것으로 파악됐다는 것이다.

   ⇒ 관리적, 물리적 보안

2. 농협 내부 직원과 외부자의 공모에 의한 조직적 범죄 가능성이다. 상당수 전문가는 이번 사태가 내부 협조 없이는 불가능했을 것으로 보고 있다.

   ⇒ 관리적 보안

3. 세 번째는 전문 해커에 의한 사이버 테러 가능성이다

   누군가 농협 IT본부 보안실 내에서 e-메일이나 웹상의 가상 저장공간 등을 통해 스크립트를 내려 받아 노트북에 설치했을 가능성도 살펴보고 있다.

   ⇒ 물리적, 기술적 보안

누가 왜? 농협 전산망 마비 3가지 시나리오, 중앙일보, 2011.4.22

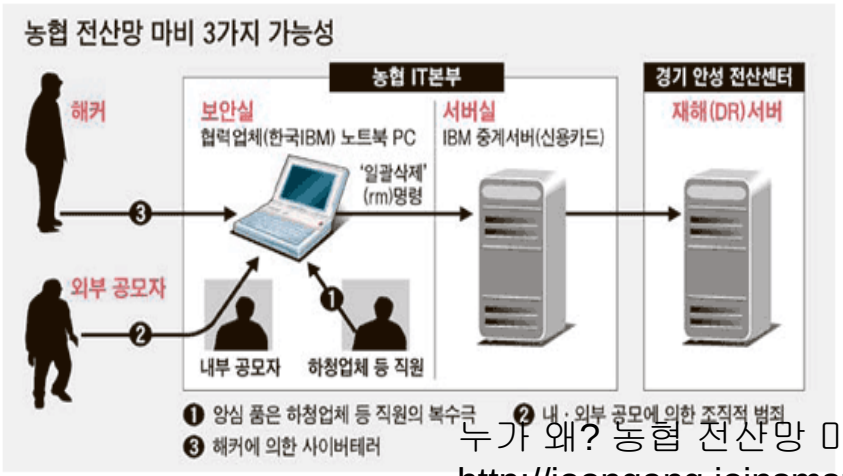
http://joongang.joinsmsn.com/article/aid/2011/04/22/5044347.html?cloc=olink|article|default

누가·왜? 농협 전산망 마비 3가지 시나리오

[중앙일보] 입력 2011.04.22 02:06 / 수정 2011.04.22 09:26

①앙심 품은 농협 하청업체 직원의 복수극?
②내부 협조 없이는 불가능…내외부 공모한 조직적 범죄
③외부 침입 흔적 발견…전문 해커의 단순 테러

농협 전산망 마비 사태가 22일로 발생 열흘째를 맞았다. 이 사건을 수사 중인 서울중앙지검 첨단범죄수사2부(부장 김영대)는 21일 삭제명령의 진원지인 협력업체 직원 노트북과 서버에 남아 있는 '디지털 족적(足跡)'에 대해 전문기관의 협조를 받아 분석 작업에 들어갔다. 그러나 수사에 착수한 지 일주일이 넘도록 농협 IT본부 서버에 대한 '삭제(rm) 명령'이 어떻게 내려졌는지 경로조차 파악하지 못하고 있다. 검찰 관계자는 "긴 터널에 들어왔다. (자료) 분석에만 2~3주는 걸릴 것"이라고 했다.



검찰은 누가, 어떻게, 왜 이런 범죄를 저질렀는지에 관해 현재까지 드러난 사실을 바탕으로 세 가지 가능성을 상정해놓고 있다. 우선 정보기술(IT) 업계의 고질적인 하청-재하청 구조에 앙심을 품은 전·현직 직원의 복수극일 가능성이 제기된다. 농협 서버에 내려진 삭제명령은 '최고접근(Super Root) 권한'을 가져야 가능하지만, 금융감독원 특별검사와 검찰 조사에서 농협이 보안규정을 준수하지 않은 정황이 포착됐다. 규정상 서버 관리자와 농협 직원이 권한을 나눠 갖게 돼 있는데 실제로는 업무 편의를 위해 유지·보수를 맡은 협력업체나 하청업체 직원도 이 권한을 모두 가졌던 것으로 파악됐다는 것이다. IT 업계에서는 현재 운용 중인 농협의 '신(新)시스템 프로젝트'가 복잡한 하청-재하청 구조로 진행됐고, 이 과정에서 하청업체들이 받는 압박이 심했다는 지적이 나오고 있다.

두 번째 시나리오는 농협 내부 직원과 외부자의 공모에 의한 조직적 범죄 가능성이다. 상당수 전문가는 이번 사태가 내부 협조 없이는 불가능했을 것으로 보고 있다.

'삭제명령'이 담긴 스크립트(명령어 조합으로 이뤄진 프로그램)가 단계적으로 실행돼 서버를 파괴했기 때문이다. 이 스크립트를 협력업체 직원 노트북에 심기 위해서는 내부자가 공모했거나, 최소한 농협 시스템을 잘 아는 인물이 개입됐을 가능성이 크다.

세 번째는 전문 해커에 의한 사이버 테러 가능성이다. 전산망 방화벽 내부에서 여러 차례 침입 흔적이 발견됐고, 정보를 빼내기 위한 '복사' 명령 없이 삭제명령만 내려졌다. 해커들은 일반적으로 자신의 실력을 과시하기 위해 특별한 흔적을 남기기 때문에 검찰의 분석 과정에서 이를 발견할 가능성도 있다. 그러나 최근 일어난 디도스(DDos·분산서비스거부) 공격과 같은 '묻지마 테러'라면 해커의 소행 여부를 밝히기가 쉽지 않을 것으로 보인다.

검찰은 당초 사고 발생 당시 '최고접근 권한'을 갖고 있던 인물들을 중심으로 수사망을 좁혀갔지만, 권한을 보유했는지 여부만으로는 용의자를 특정하기 어렵다고 판단했다. 결국 노트북과 서버에 어지럽게 남은 스크립트와 파일 등 '디지털 족적'을 분석해 경로를 파악하는 쪽으로 수사 방향을 선회했다.

검찰은 범인이 농협 전산망 방화벽을 우회하거나 뚫은 것은 아닌 것으로 보고 누군가 농협 IT본부 보안실 내에서 e-메일이나 웹상의 가상 저장공간 등을 통해 스크립트를 내려받아 노트북에 설치했을 가능성도 살펴보고 있다. 익명을 요구한 금융업계의 스토리지(저장장치) 전문가는 "해당 서버의 종류와 운영체제(OS), 사용된 명령어 조합을 살펴보면 이런 작업을 할 수 있는 이들을 좁혀갈 수 있을 것"이라고 말했다.

이동현 기자

누가 왜? 농협 전산망 마비 3가지 시나리오, 중앙일보, 2011.4.22
http://joongang.joinsmsn.com/article/aid/2011/04/22/5044347.html?cloc=olink|article|default

고대의료원 정보시스템 보안지침

제5장 물리적 보안

제15조 (통제구역)

① 중요정보가 보관되거나 처리되는 지역은 사전에 해당 기관장의 승인을 득하여 통제구역으로 지정한다.

② 다음 구역을 통제구역으로 지정하여 운영한다.

1. 정보시스템 운영 및 지원을 위한 **전산실**
2. 주전산기 및 전산기기들이 위치한 **기계실**
3. **백업 매체의 보관 장소**
4. 기타 정보자산의 보안 및 안전을 위해 통제가 요구되는 장소

③ 통제구역은 다음과 같이 운영한다.

1. 통제구역임을 나타내는 **표식을 부착**
2. **별도의 출입통제(시건 장치, 출입 제한 등) 장치**를 설치
3. 외부로부터의 물리적 침입 시도를 감지할 수 있는 **보안시설 설치**
4. 화재로부터 데이터의 손실을 최소화할 수 있는 **특수 방재설비설치**
5. 보안담당자에 의한 정기적인 보안점검

고대의료원 정보시스템 보안지침

제16조 (출입자 관리)

① 통제구역은 출입 자격자와 비자격자를 구분한다.

② 비자격자의 통제구역 출입허가는 다음에 의한다.

1. 근무시간 중에는 해당 통제구역의 **보안담당자의 승인**을 득하여야 한다
2. 근무시간 후에는 사전 출입허가 또는 당직자의 승인을 득한 경우에만 출입 가능하며 통제구역 출입 자격자가 반드시 동행토록 한다.

③ 근무시간 후 비자격자가 출입한 경우 당직자 또는 통제구역 근무자는 익일 아침 그 내용을 근무일지에 기재하여 보안담당자에게 보고하여야 한다.

④ 통제구역 출입 시 **사전 승인된 목적 이외의 물품(노트북, 카메라, 기억매체 등)은 반입할 수 없으며**, 이를 어길 경우 근무자는 해당물품을 압수하고 출입자를 통제 구역 밖으로 퇴실시켜야 하며, 해당 위반 사실을 즉시 보안담당자에게 보고하여야 한다.

고대의료원 정보시스템 보안지침

제17조 (장비 반·출입 관리)

① 의료원의 정보자산은 해당 부서장 및 보안담당자의 승인 없이 외부로 반출할 수 없다.

② 외부의 정보자산(개인 PC 및 노트북 등)은 해당 부서장 및 보안담당자의 승인 없이 의료원내로 반입할 수 없다.

③ PC 등의 반입/반출 시에는 H/W 사양뿐만이 아니라 S/W의 사양, 하드디스크 저장 정보를 해당 부서장이 직접 확인하고, 해당 기관 보안담당자에게 통보하여야 한다.

④ 반입/반출 된 물품 및 정보자산에 대한 보안책임은 반입/반출자와 해당 부서장 에게 있다.

정보보호를 위한 의료전문가의 역할

1. 의료정보의 분산저장

- 환자의 의료 정보를 다루는 시스템의 저장 용량을 제한한다. 예를 들어 최대 10만명까지 환자 레코드를 제한하여 저장하도록 한다. 이는 분산을 통하여 외부 침입이 발생하더라도 피해가 한정적으로 이루어 지도록 하기 위함이다.

2. 의료정보의 주기적 백업

- 시스템의 과부하로 반응시간이 느려질 수도 있고 좀더 심각한 문제로 시스템의 작동이 정지할 수도 있다. 이러한 문제에 대한 해결책으로 무정전 전원장치와 백업 하드웨어를 준비하는 것이다. 또한 시스템 문제가 발생할 경우 어떤 정보도 손실되지 않도록 의료자료를 주기적으로 백업해야 한다.

정보보호를 위한 의료전문가의 역할

3. 의료정보의 암호처리

- 저장 및 전송과정에서는 반드시 암호처리를 의무적으로 사용하여 사용자를 가장한 공격, 통신 도청 등에 대해서도 의료정보를 보호할 수 있도록 한다.

4. 의료종사자들에 대한 교육 강화

- 내부자에 대한 침해사례를 줄이기 위해서는 병원내의 정보보호 교육 및 물리적 보안을 수행하는 것이 중요하며, 또한 의무기록 자료를 불출을 감시하거나 환자의 개인정보를 저장, 조회, 출력 복사할 때 관리자의 승인 및 인증을 받도록 하는 것이 중요하다.

정보보호를 위한 의료전문가의 역할

5. 합리적인 의료정보 접근 통제 규칙 수립

- 의료정보에 대한 최대의 보안위협인 배부자의 오용 및 남용을 방지하기 위한 접근 통제를 적극적으로 실행하기 위하여, 최소한의 관련자만이 접근할 수 있도록 접근통제 원칙을 제정한다. 개인의 프라이버시 정보를 보험, 행정, 사법 등에서 접근하는데 있어 정치적 압력을 최대한 차단하기 위한 사회적 합의 도출이 필요하다.

6. 진료정보의 장기 보관을 위한 기술 개발

- 법적 보관 기간을 경과한 의료정보는 추후 있을지도 모를 법적 분쟁에 대비하여 계속하여 보관할 필요가 있다. 따라서 분산되어 있는 의료정보를 백업 보관하기 위한 자동화된 보관기술, 시스템 및 관리체계를 개발할 필요성이 있다.

정보보호를 위한 의료전문가의 역할

7. 보건의료 전산시스템 사용시 숙지사항

- 의료행위자는 환자의 사생활 문제를 보호하는데 부단히 주의를 기울여야 한다. 의료행위자는 개인정보 보호를 위하여 기관 혹은 조직이 새로운 그리고 기존의 보건의료 전산시스템과 관련되어 아래의 사항을 인지해야 한다.

- 비밀번호와 신원확인 코드의 사용은 기본이다.
- 정보의 수집과 기록에 대한 범위를 설정해 둘 필요가 있다.
- 데이터를 입력할 때는, 정보가 정확한지 확실히 할 필요가 있다.
- 사생활 보호, 기밀성, 시스템의 보안과 관련된 정책을 개발할 때 환자가 우선적인 관심사가 되어야 한다.
- 새로운 병원정보시스템을 구현할 때 일반 대중에게 알리는 것이 중요하다.
- 개인데이터를 시스템에 입력하기 전에 환자에게 전산의무 기록이 그 기관에서 사용된다는 것을 알려야 한다.

정보보호를 위한 의료전문가의 역할

- 연구에 정보를 사용할 때 동의를 구하는 것은 절대적으로 필요하다.
- 시스템과 그 통제는 정기적으로 점검되어야 할 필요가 있고 그에 따른 감사는 독립적인 다른 기관에 의해 실시되어야 한다.
- 데이터가 한 시스템에서 다른 시스템으로 전달되는 것을 통제하고 데이터의 사용을 조절하가 위한 데이터베이스 연계의 영역에서 정부의 법률제정이 필요하다.
- 환자의 사생활 보호와 기밀성 부분에 대한 직원교육은 필수적이다.

정보보안에서 생각해보아야 할 점

- 현재 간호사로서 의료정보보안에 대한 인식을 바로 하고 있는가?
- 병원에서의 보안에 대한 문제점은 무엇인가? 개선해야 할 점은 무엇인가?
- 병원에서 현실적인 정보보안방법에 대한 생각 해보기

참고문헌

- 전산시스템의 안전한 운영을 위한 운영체제 DB, 소프트웨어, 하드웨어 등을 보안기술을 이용하여 보호하는 행위 (안선주, 2005)
- 의료정보보안의 현황과 전망, 임채균, 2010
- 서울대학교 커뮤니티 : community.snu.ac.kr/bbs/servlet/DownLoad?SEQ=24626
- 의료기관개인정보보호 가이드라인 공청회, 2012. 9
- 정보시스템 보안 지침 , 총칙 – 고려대학교 의료원 규정
- 누가 왜? 농협 전산망 마비 3가지 시나리오, 중앙일보, 2011.4.22 http://joongang.joinsmsn.com/article/aid/2011/04/22/5044347.html?cloc=olink|article|default
- 개인정보보호관리체계인증(PIMS) 컨설팅 소개자료, Infosec/SK C&C
- 구로병원 OCS, 전산운영팀 공지사항,2010
- 의료정보 대책, 물리적 보안 http://www.boannews.com/media/view.asp?page=1&idx=21019&search=&find=&kind=1