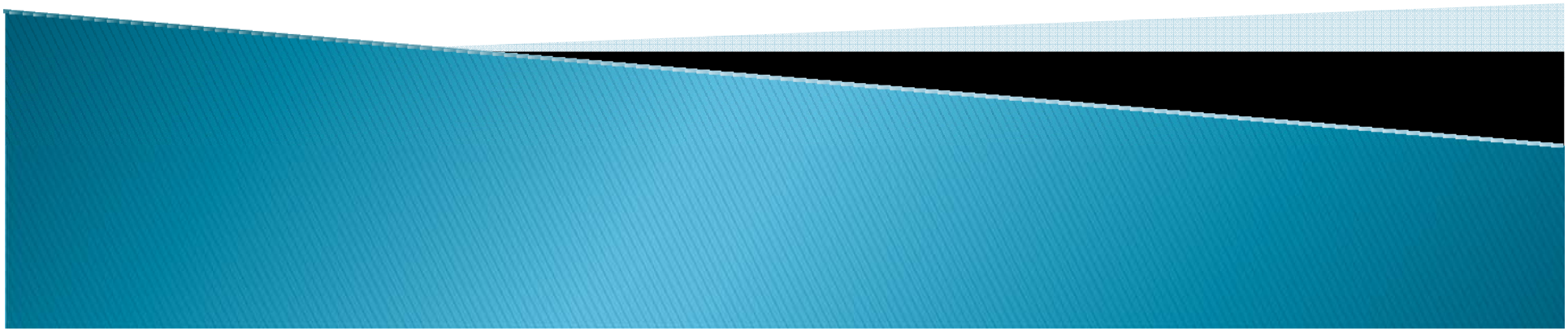
미국 의료기관의 HIPAA 적용에 따른 의료정보보호 사례

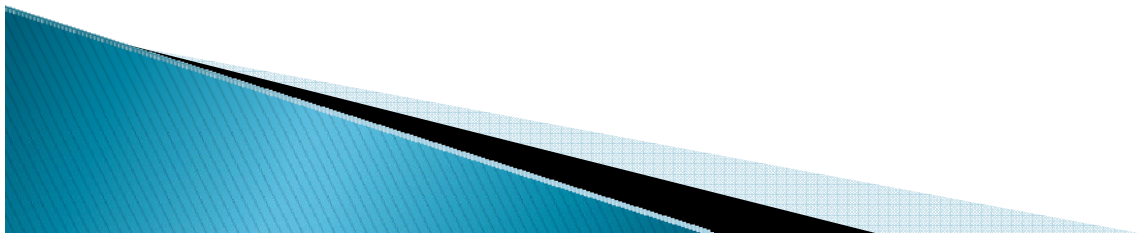
한양여자대학 보건행정과
임 현 숙



목 차

- 미국 시카고 일리노이 대학병원 의무기록 관리 규정 및 절차 (University of Illinois Medical Center at Chicago: Management Policy and Procedure)

- Practical Cases under the HIPAA Training Handbook



미국 시카고 일리노이 대학병원 의무기록 관리 규정 및 절차 예

I. 의무기록 정보의 공개(Release)

II. 환자명부에서 보호대상건강정보의 공개(Disclosure)

III. 보호대상건강정보의 비인가 공개(Unauthorized Disclosure)에 대한 설명 요청

IV. 보호대상건강정보의 이용 및 공개에 대한 제한 요청

V. 보호대상건강정보의 수정(Amendment) 요청

VI. 보호대상건강정보의 전달 (Communication) 제한

VII. 전화를 이용한 보호대상건강정보의 전달

VIII. 팩스를 이용한 보호대상건강정보의 전달

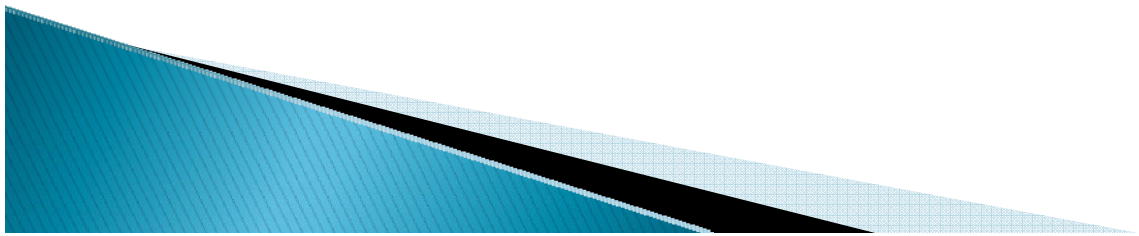
IX. 전자메일을 이용한 보호대상건강정보의 전달

X. 환자개인정보 보호 및 보안 불만사항(Complaints) 전달

XI. 보호대상건강정보의 파기(Destruction)

관련 정의 - 보호대상 건강 정보(PHI)

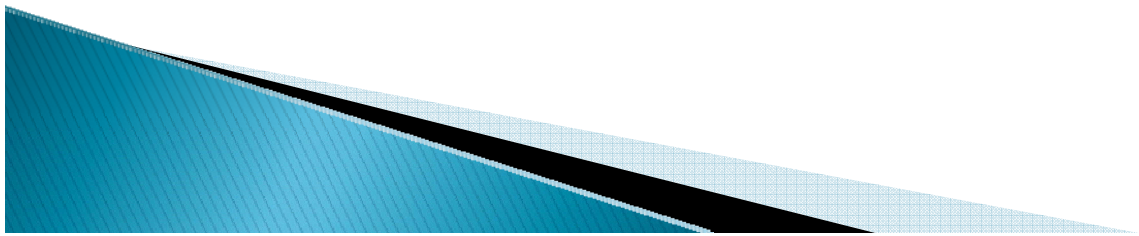
- 구두, 서술 또는 전자적인 매체를 포함한 어떠한 형태에서든지 유지되고 전달되는 개별적으로 식별 가능한 건강 정보
- 개별적으로 식별 가능한 건강정보는 개인의 건강 상태 또는 상황 즉, 개인에게 제공되는 의료서비스, 지불 또는 개인에 대한 보건의료 혜택 시행과 관련 있음
- 이 정보가 개인을 식별하는데 사용될 수 있다고 믿을 수 있는 합리적인 근거가 있는 곳에 있으면 이 정보는 보호대상 건강 정보라고 간주됨



관련 정의 – 최소 필수 항목

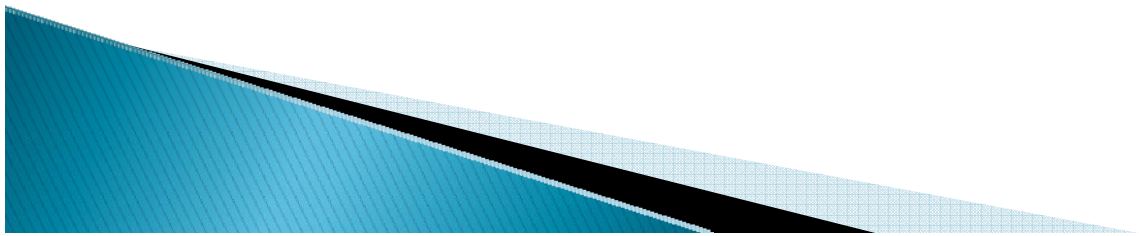
- 보호대상 건강 정보를 사용 또는 공개할 때,
- 다른 대상기관(covered entity)으로부터 보호대상 건강 정보를 요청 받을 때,

➡ 요청받은 기관은 이용, 공개, 또는 요청에 대한 의도된 목적을 이루기 위해서 최소 필수 항목의 보호대상 건강 정보로 제한하도록 합리적인 노력을 반드시 해야 함



관련 정의 – 최소 필수항목 요구에 대한 예외사항들

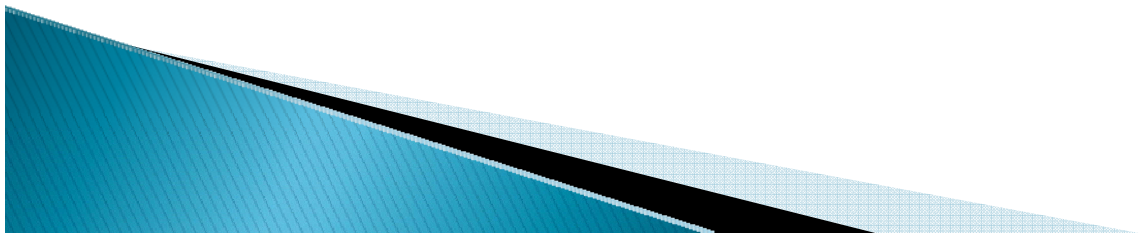
- 보건의료 서비스 제공자에게 치료 목적으로 요청 받거나 공개되는 경우
- 정보 주체인 당사자에게 공개하는 경우
- 개인이 요청하여 승인 하에 이루어진 사용 또는 공개
- 정보 공개가 법 집행 목적으로 요청될 때 보건복지부(Department of Health and Human Services, HHS)에 공개할 경우
- 기타 법적 요청에 따른 이용 및 공개



관련 정의 – 치료, 지불 및 보건의료 업무(TPO)

- **치료** – 의료기관에 의한 보건의료 서비스의 시행, 조율 및 관리와 관계됨
- **지불** – 의료기관이나 제 3자에 의해 수행되는 어떤 활동들을 포함하는데 건강보험 수혜 자격 여부 또는 건강 보험 보장 범위의 판정, 의료 필요상 환자에게 제공된 제반 서비스의 검토, 의료 서비스 활용에 대한 검토 등과 같이 건강보험 회사가 귀하에게 권장된 의료 서비스를 승인하거나 비용을 지불하기 전에 수행할 수도 있는 일부 조치 등이 포함됨
- **보건의료 업무** – 의료기관의 일반 관리 및 행정 기능을 포함하는 보건의료 서비스 제공자로서의 의료기관 기능들과 관련된 활동들 임

I. 의무기록정보의 공개(Release)



규정

- 본 규정은 ① 전체 의무기록의 공개 및 일부 공개에 대해서 설명하고 ② 정보 전달에 이용되는 모든 방법들(사진복사, 팩스, 모뎀, 문서, 구두, 및 영상의무기록과 전자의무기록을 출력한 사본)에 적용
- HIPPA 및 그 규정에 따라 의무기록 또는 의료 정보의 사본 제공을 위해서는 환자의 승인 필요
- 의료기관 소유 건물로부터 원본 의무기록을 이동시키기 위해서는 법원 명령 요구
- 의료기관은 건강정보관리부서(HIM Department)에 대해 의료 정보와 의무기록의 공개를 제한함.
- 단, 승인된 예외사항들에 대해서, 건강정보관리 책임자 또는 지명된 사람은 의무기록정보에 대한 모든 요청에 응해야 함.

규정- 예외사항들

1. 치료, 지불 및 보건의료 업무를 위한 의료정보 요청은 이 제한으로부터 면제됨
2. 환자들의 의무기록을 소유하고 있거나 소유할 수 있는 지역의 임상 센터는 보건복지부와 상의하여 그들 환자들에 대한 의무기록정보 요청에 응할 책임이 있음.
3. 업무 책임에 따라 전자의무기록에 접근하는 직원들은 그들이 고용되어 근무하는 동안 또는 전자의무기록에의 접근이 허락된 업무위치에서 일하는 동안 자기들의 의무기록의 검토 및 출력에 접근할 수 있다. 전자의무기록이 아닌 정보의 복사를 위해서, 직원들은 건강정보관리부서에 연락하도록 요청 받는다. 건강정보관리부서의 책임자는 의료기관 직원들에 의해 출력 및 공개된 정보로 취해진 행동들에 대해 책임이 없다.

- **주의:** 접근에 대한 이런 수준을 가진 직원들은 친구, 배우자, 또는 친척들의 의무기록에 접근하도록 허락되지 않는다. 문서화된 승인이 없이 친구, 배우자, 또는 친척 의무기록에의 접근은 환자 프라이버시 침해로 간주되고 징계 행동 대상이 된다.
- 다른 모든 직원들은 건강정보관리부서로부터 건강정보 요청서를 요구 받는다.

절차

1. 의료기관 의사들, 인턴, 전문의, 직원 및 학생들은 치료, 지불 및 보건의료 업무와 관련하여 정보를 공개할 수 있다. “최소 필수항목"(진료 관련 의사결정을 위해 필요한 정보에 한해서만) 규칙은 의료정보의 모든 공개에 적용된다. 모든 위반 또는 잠재적인 위반은 프라이버시 담당관에게 반드시 보고되어져야 한다.

⑴ 의무기록 복사에 대한 모든 소환장, 법원명령, 및 변호사의 요청은 반드시 건강정보관리부서로 전송되어져야 한다.

⑵ 건강정보관리부서로 의무기록 복사에 대한 모든 서면 요청서를 보내야 한다.

⑶ 의무기록의 어느 낱장이라도 원본은 어떤 환경, 어떤 때라도 환자, 조직, 또는 기관에게 절대 주어서는 안된다.

⑷ 전화로 정보를 공개하기 위해서는 MCMPP IM 4.07 보호대상건강정보의 전화 전달(Telephone Communication of PHI)을 참고하시오. 이런 형태의 공개는 단지 치료, 지불 및 보건의료 업무에 한해서만 행해져야만 한다.

⑸ 팩스로 정보를 공개하기 위해서는 MCMPP IM 4.08 보호대상건강정보의 팩스 전송(Fax Transmittal of PHI)을 참고하시오. 이런 형태의 공개는 단지 치료, 지불 및 보건의료 업무에 한해서만 행해져야만 한다.

⑹ 입원환자에 대해, 입원 중에 가능한 한 빨리 그러나 퇴원/전원 할 1일 이전에 의무기록의 복사 요청을 확인하고 건강정보관리부서에 알려야 한다

절차

2. 건강정보관리부서(HIM Department)

⑴ 정보 공개에 요구되는 서명된 서면 허가서를 받아야 한다.

⑵ HIPPA에서 요구하는 모든 항목들이 있는지 확인해야 한다.

⑶ 만약 요청이 있다면, 요청한지 30일 이내에 복사하기 이전에 환자가 기록을 세심하게 검토하도록 허락한다.

⑷ 복사와 관련된 요금을 요청자에게 알려주어야 한다.

⑸ 요청서 수령이 30일 이내이면 전자의무기록 또는 영상의무기록의 출력본 또는 사진복사물을 제공해야 한다. 만약 요청서가 30일 이내에 처리될 수 없다면, 30일 연장에 대한 서면 통보서를 요청자에게 제공해야 한다.

⑹ 요청날짜로부터 적어도 6년 동안 요청된 기록 명단을 보유해야 한다.

절차

3. 주치의/지명된 사람(Attending Physician/Designee)

⑴ 병원 입원환자를 위해, 요청서상의 환자 기록에 대한 검토 및 해석을 용이하게 해야 한다. 환자의 요청과 이와 연관된 견해/해석을 나타내는 경과기록을 작성해야 한다. 건강정보관리부서에 기록의 복사 요청을 의뢰해야 한다.

⑵ 의료 조사자, 공공보건, 및 법 집행 기관들에게 보고하도록 요구 받는 것과 관련된 모든 적용 가능한 의료기관 규정을 준수해야 한다.

절차

4. 의료이용 관리/퇴원 계획부서 직원(Utilization Management/Discharge Planning Staff)

⑴ 외부 의료 이용 조사 기관들의 모든 책임자들은 의무기록에의 접근을 위한 예약을 위해 의료이용 관리/퇴원 계획 직원에게 전화해야 한다.

⑵ 만약 입원 기록이 의료이용 관리 조사를 위해 필요하다면, 진료조정부서(Care Coordination Department)로 지명된 사람이 건강정보관리부서로부터 의무기록을 얻는데 책임이 있고 이것을 다시 건강정보관리부서로 돌려주는 것에 대한 책임도 있다.

⑶ 조사 문서는 의무기록에 보관될 것이다.

⑷ 이런 기관들에 의한 조사는 월요일에서 금요일까지 오전 8시부터 오후 4시 30분 사이에 허가가 될 것이다.

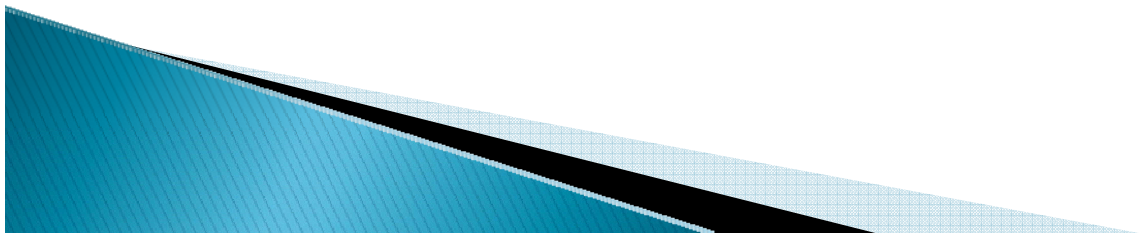
절차

5. 개인정보보호 담당관(Privacy Officer)

⑴ 보고된 위반 사례들에 대한 데이터베이스를 조사하고 유지해야 한다.

⑵ 건강 정보의 추가 항목에 대한 요청서를 처리해야 한다.

II. 환자명부에서 보호대상건강정보의 공개 (Disclosure)



규정

- 병원은 보호대상건강정보를 병원의 입원환자 명단을 보유하는 목적으로 사용 및 공개한다.
- 병원은 병원 명부에 대해 보호대상건강정보를 사용하거나 공개할 때 모든 적용 가능한 법과 법률 규정을 따른다.
- 병원은 환자가 병원 명부로부터 자신의 보호대상건강정보 제한을 요청하는 것을 허락한다.

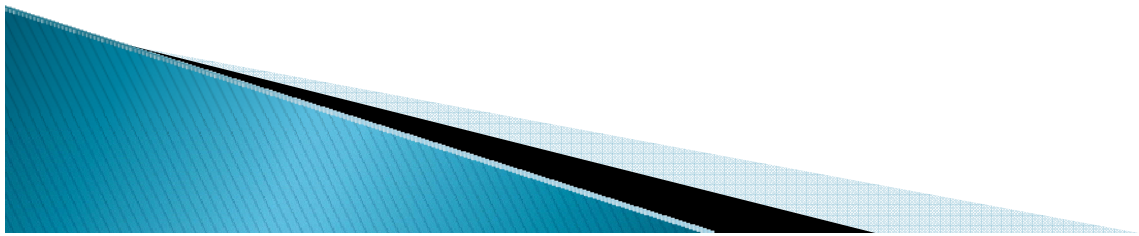
절차

1. 병원은 환자들의 보호대상건강정보가 명부에 포함될 수 있다는 것을 입원 시에 각 환자들에게 알린다.
2. 병원은 환자들의 보호대상건강정보가 병원 명부로부터 누군가에게 공개될 수도 있다는 것을 입원 시에 각 환자들에게 알린다.
3. 병원은 환자들에게 병원 명부 작성의 목적으로 그들의 보호대상건강정보가 이용 또는 공개되는 것을 제한하거나 금지할 수 있는 기회를 제공한다.
4. 만약 환자가 병원 명부로부터 자신의 보호대상건강정보 이용에 대한 제한을 요청한다면, 병원은 요청에 응하고 이를 위해 필요한 서식을 완성한다.

절차

5. 환자가 질병으로 움직일 수 없거나 응급 치료 상황에서는 특정 상황에 따라서만 개인의 보호대상건강정보를 이용 또는 공개한다.
6. 환자가 질병으로 움직일 수 없거나 응급 치료 상황에서, (실제 그렇게 하게 된다면) 지명된 보건의료 제공자는 개인에게 병원 명부 사용 목적에 대한 이용 또는 공개를 반대할 기회를 알리고 제공할 것이다.
7. 이 규정에 대한 위반 또는 잠재적인 위반을 알게 된다면 반드시 개인정보보호 담당관(312-355-5650) 또는 법률준수 고발체계(Compliance Hotline, 866-665-4296)에 곧바로 보고해야 한다.

III. 보호대상건강정보의 비인가 공개 (Unauthorized discolsure)에 대한 설명 요청



비인가 공개(Unauthorized Disclosure)

비일상적 목적으로 이루어진 공개 즉;

- 법의 요청; 공중보건 활동; 학대, 방치, 및 가정폭력의 희생자; 의료 감시 활동; 건강과 안전의 위협을 막고자 하는 경우; 법 집행 목적을 위해; (법률적) 사망자; 해부용 시신 장기, 눈, 또는 조직 기증; 안전을 위해; 근로자재해보상과 같은 특수한 정부 역할을 위해
- 이는 치료, 지불 및 보건의료 업무(TPO)에 근거하여 따르는 공개에서 제외된다.

규정

- 환자의 승인 없이 이루어진 보호대상건강정보의 모든 이용과 공개에 관한 데이터베이스를 유지한다.
- 환자들은 보호대상건강정보의 비승인된 공개에 대한 설명을 요청하도록 허락된다.

절차

1. 병원은 개인이 개인정보보호 담당관에게 문서로 공개에 대한 설명 요청서를 제출하도록 요구한다.
2. 개인정보보호부서 직원은 공개에 대한 설명 요청에 관한 응답, 처리, 수령에 관한 책임이 있다.
3. 또한 주 및 연방 정부에 대한 의무적인 보고 책임이 있는 부서들은 개인정보보호부서에게 이러한 요청된 공개를 보고한다.
4. 공개에 대한 설명 요청은 2003년 4월 14일 이전으로 앞설 수 없다.
5. 개인정보보호부서 직원은 요청 증명서를 받은 후 60일이 경과하지 전까지 개인에게 알린다.

절차

6. 병원이 조치를 하는 전체 기간은 30일 이내로 연장된다. 그리고 만약 연장이 필요하다면, 개인정보보호부서 직원은 병원이 공개에 대한 설명을 완료하기로 한 날짜와 연장에 대한 이유를 공식성명(서면)으로 개인에게 제공한다.
7. 조치 기간은 한번 이상 연장되지 않는다.
8. 공개에 대한 설명 보고서는 1년에 한번 무료로 제공된다. 추가적인 보고서는 요금을 받고 제공된다.
9. 공개에 대한 설명 요청은 요청이 발생한 날짜로부터 6년 동안 보유된다.

IV. 보호대상건강정보의 이용 및 공개에 대한 제한 요청

규정

- 각 개인들이 자신의 보호대상건강정보 이용 및 공개가 제한되도록 요청하는 것을 허용한다.

절차

1. 병원은 개인이 보호대상건강정보의 이용과 공개를 제한하기를 요청하는 것을 허용한다. (요청은 개인정보보호 담당관(312/355-5650)의 의해 조치되어 진다.
2. 그런 제한에 동의한 후에, 이 규정과 절차 내에서 특별히 언급된 것이 없다면 병원은 그 제한을 위반하지 않는다.
3. 만약 병원이 개인의 요청된 제한에 동의한 경우라도, 아래에 열거된 이용과 공개에 대해서는 제한 요청이 적용되지 않는다.

⑴ 자신의 보호대상건강정보에 접근하는 개인에 대해서;

⑵ 자신의 보호대상건강정보에 대한 설명을 요청하는 개인에 대해서;

⑶ 병원 환자 명부;

⑷ 동의, 승인, 또는 찬성/반대의 기회가 요청되지 않는 경우(예를 들면, 법원 명령에 의한 용도들; 의료 감시; 연구; 법 집행; 공공보건; 건강과 안전의 위협을 막고자 하는 경우; 해부용 시신 장기, 눈, 또는 조직 기증; 근로자재해보상; 학대, 방치 또는 가정폭력의 희생자들; 특수한 정부 기능들; 법에 의해 요청되는 경우)의 예들에 대해서.

절차

4. 병원은 아래에 열거된 상황에서 제한에 동의한 것을 종결시킬 수 있다:

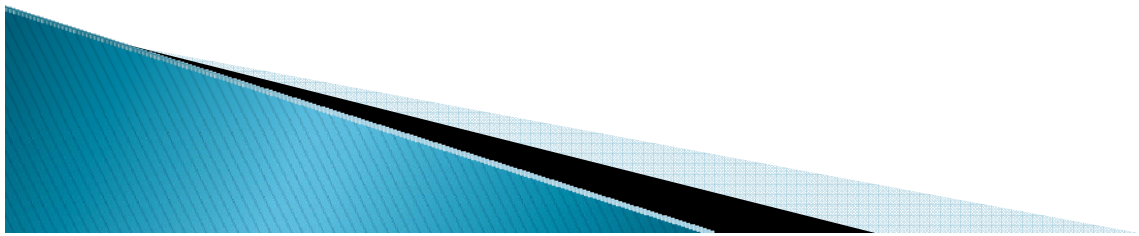
⑴ 개인이 서면(문서)으로 종결을 요청하거나 동의할 경우;

⑵ 개인이 구두로 종결에 동의하고 구두 동의가 문서화되는 경우; 또는

⑶ 병원이 개인에게 제한에 대한 동의가 종결됨을 알리는 경우. 이런 종결은 단지 개인에게 그렇게 됨을 통보한 후 받거나 생성된 보호대상건강정보와 관련해서만 효력이 있다.

5. 병원은 제한 동의를 만든 날 또는 제한이 사실상 지속되었던 날 둘 중 어느 것이든 늦은 날로부터 적어도 6년 동안은 제한을 문서로 만들어서 보유한다.

V. 보호대상건강정보의 수정(Amendament) 요청



규정

- 환자가 자신의 지정기록세트(정보가 지정기록세트에 보관되어 있는 한) 또는 보호대상건강정보 수정을 요청 하도록 한다.

절차

1. 보호대상건강정보에 대한 수정을 요청하는 모든 개인은 개인정보보호 담당관에게 서면으로 직접적으로 제출 한다.
2. 개인정보보호 부서 직원은 보호대상건강정보에 대한 수정 요청을 받고, 처리하고 응답하는 것에 대한 책임이 있다.
3. 개인은 반드시 수정 요청을 뒷받침할 이유를 문서로 작성해야 한다.
4. 요청은 검토를 위해 지명된 보건의료 전문인에게 위탁되는데 전문인은 개인정보보호 담당관에 의해 각 사례별로 선택된다.
5. 만약 수정 요청이 받아들여졌거나 혹은 거부되었다면 개인정보보호 부서 직원은 요청서 수령 후 60일 이내에 개인에게 알려준다.
6. 병원 조치에 대한 기간은 30일 이상 연장되지 않는다. 만약 연장이 필요하면, 개인정보보호 부서 직원은 개인에게 병원이 요청된 조치에 대한 예상 검토 완료 날짜와 기간 연장 이유를 서면 진술서를 제공한다.
7. 조치 기간은 한 번 이상 연장되지 않는다.

절차 – 보호대상건강정보에 수정 요청 승인

- 만약 수정 요청이 승인된다면, 개인정보보호 부서 직원은 필수 보건의료 전문인이 수정을 하도록 배치한다.
- 수정 요청 승인 하에, 개인정보보호 부서 직원은 아래의 임무들을 수행 한다:

1. 정보 수정을 공유해야 할 필요가 있는 관련된 사람에게 병원이 알려 주도록 개인의 확인과 동의를 얻어 적시에 개인에게 알린다.
2. 수정이 필요한 것으로 확인된 사람에게 적당한 시간 내에 수정을 제공하고 알리기 위한 합리적인 노력을 한다.
3. 수정된 정보에 의존하거나 의존이 예상될 수 있는 사람과 보호대상건강정보에 영향을 받는 병원이 알고 있는 사람에게 적당한 시간 내에 수정을 제공하고 알리기 위한 합리적인 노력을 한다.
4. 수정을 완료 할 때 개인정보보호 부서 직원은 최소한 지정기록세트에서 영향을 받는 정보를 확인하고 수정 위치에의 연계를 제공한다.

절차 – 보호대상건강정보에 수정 요청 거부

- 만약 요청된 보호대상건강정보 또는 기록이 아래에 해당하는 경우 일 때, 수정에 대한 개인의 요청은 거부될 수 있다:

1. 병원에서 생성된 것이 아님;
2. 지정기록세트의 일부분이 아님;
3. 보호대상건강정보에 접근할 개인의 권리에 대한 자격요건 검열이 용이하지 않음;
4. 정확하고 완전한 경우

- 전체 또는 부분적으로 수정이 거부되면, 개인정보보호 부서 직원은 개인이 (제한된) 시간 틀 내에 맞추어 서면 거부서를 제공한다.

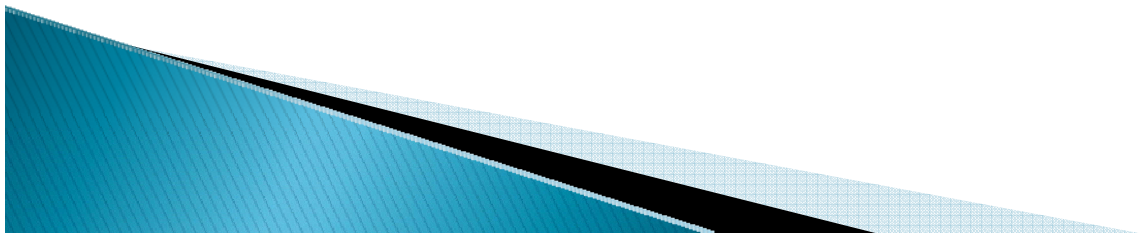
절차 – 보호대상건강정보에 수정 요청 거부

- 거부는 쉬운 용어가 사용된 문서로 되어야 하고 아래의 내용을 포함한다:

1. 거부에 대한 근거
2. 거부에 동의하지 않는 서면 진술서를 제출할 수 있는 개인의 권리
3. 개인이 어떻게 진술서를 제출할 수 있는지에 대한 설명
4. 이름, 직위, 그리고 불만을 접수하도록 지정된 담당자 또는 사무실 전화번호를 포함한 불만제기 절차에 준거하여 개인이 병원에 어떻게 불만을 제기할 수 있는지에 대한 설명;
5. 개인이 보건복지부에 대해 어떻게 불만을 제기할 수 있는지에 대한 설명

- 만약 개인이 불찬성 진술서를 제출한다면, 병원은 개인의 불찬성 진술서에 대한 서면으로 항변을 준비할 수 있다.
- 수정 요청은 요청이 접수된 날짜로부터 6년 동안 보유해야 한다.

VI. 보호대상건강정보의 전달 (Communication) 제한



규정

- 대체 수단을 사용하여 보호대상건강정보를 전달받고자 하는 개인의 합리적인 요청에 대한 편의를 도모하기 위해서 필요한 조치를 취한다.

절차

1. 병원은 개인이 개인정보보호 담당관에게 문서로 비밀연락(confidential communication)을 위한 요청서를 제출하도록 요구한다.
2. 병원은 비밀보장 전제하에 (정보를) 전달하는 조건으로 한 요청에 근거하는 한 개인에게 설명할 것을 요구하지 않는다.
3. 만약 어떻게든 처리될 수 있다면(연락 할 다른 방법 또는 대리 주소가 상세하다면) 병원은 어떻게 지불하는지에 대한 정보에 대한 연락 가능한 주소에 관한 조항을 조건으로 할 수 있다.
4. 대체 수단 또는 장소는 보호대상건강정보를 전달하기 전에 병원과 개인 양쪽 모두 만족할 수 있도록 개인별로 맞춰서 지정된다.
5. 전문가적인 판단을 이용하여 모든 관련 요소들을 고려하는 개인정보보호 담당관은 개인에게 보호대상건강정보를 전달한 대체 수단 또는 장소를 결정할 책임이 있다.

절차

6. 일단 이용 또는 공개가 적절하다고 판단다면, 기밀정보에의 적절한 접근 인가가 있는 직원이 적절한 승인 절차를 걸쳐 개인의 보호대상건강정보에 접근한다.
7. 요청된 보호대상건강정보는 비밀이 보장되고 안전한 방법으로 개인에게 전달된다. 이런 정보는 기밀정보에의 적절한 접근 인가를 가지고 있지 않는 직원들이나 다른 사람들에 의해 접근될 수 없다.
8. 개인정보보호부서 직원은 보호대상건강정보의 요청과 전달을 적절하게 문서화 한다.
9. 만일 보호대상건강정보를 요청한 개인 또는 대상기관의 신원과 법적 권한이 확인될 수 없을 경우, 개인정보보호부서 직원은 요청된 정보 공개를 삼가고 시기 적절한 방법으로 개인정보보호 담당관에게 이 사례를 보고한다.
10. 이 규정에 대한 위반 또는 잠재적인 위반을 알게 된다면 반드시 개인정보보호 담당관(312-355-5650) 또는 법률준수 고발체계(Compliance Hotline, 866-665-4296)에 곧바로 보고해야 한다.

VII. 전화를 이용한 보호대상건강정보 전달

정의 – 임상적으로 응급상황

- 진단, 치료, 또는 임상적 진찰과 더불어 의료진과 즉각적인 의사소통이 필요한, 즉 환자의 건강이 심각한 위험 상태에 있다는 전문 의료인의 결정.

규정

- 보호대상건강정보가 공개될 수 있는 곳에서 전화로 정보를 전달하는 것을 보호하기 위해 적절한 안전장치를 마련한다.
- 전화 상에서의 신원 결코 절대적으로 검증할 수 없기 때문에, 교수진, 의료진, 학생들 및 자원봉사자들은 전화로 정보를 전달할 때 충분한 주의를 기울여야 할 책임이 있다.
- TPO(치료, 지불, 보건의료 업무) 목적으로 필요한 정보를 긴급하게 즉각적으로 전송해야 하는 상황을 제외하고는 전화로 보호대상건강정보를 전달하는 것은 단념하는 것이 좋고 또한, 기타 당사자의 요구에 충족할 최소 필수 항목 정보로 제한된다.
- TPO(치료, 지불, 보건의료 업무)를 위해 개인의 일반적인 동의에 의해 승인되었거나 연방 또는 주 정부 법에서 요구하는 경우를 제외하고는, 어떤 방법으로든 보호대상건강정보를 전달하기 전에 적절하게 완성되고 서명이 되어 있는 허가서를 반드시 받아야 한다.

절차 – 환자에게서 전화가 걸려오는 것(Inbound Call)

1. 환자 개인 특성이 있는 테스트 질문들(예; 생년월일, 어머니의 미혼 시절 이름 등)과 통화의 성질(예; 약국 주소, 보험회사 가입자 번호)을 이용하여 전화를 건 사람의 신원을 확인한다.
2. 만약 통화의 성질이 긴급하지 않고 또, 전화 건 사람의 신원이 확인될 수 없다면, 전화로 어떠한 정보도 제공하지 않는다. 전화를 건 사람에게 팩스(MCMPP IM 4.08 Fax Transmittal of PHI) 또는 우편을 통해 정보를 요청할 것을 지시해야 한다.
3. 만약 통화의 성질이 임상적으로 긴급하고 또, 전화를 건 사람의 신원이 확인될 수 없을 경우, 보호대상건강정보를 포함하고 있는 어떠한 정보를 제공할 때 전문가적인 판단을 이용하고 환자의 의무기록에서 제공된 정보와 통화의 성질을 문서화 한다. 확실치 않은(의문스러운) 공개에 대해서는 개인정보보호 담당관에게 알린다(5-5650).
4. 어떠한 상황에서든, 전화를 건 사람의 요청에 충족할 최소 필수 정보만을 제공한다.

절차 – 환자에게 전화를 걸어주는 것(Outbound Call)

1. 전화를 걸기 전에 전화번호를 확인한다.
2. 통화의 성질과 환자 개인 특성이 있는 테스트 질문들을 사용하여 의도된 당사자의 신원을 확인한다.
3. 만약, 통화의 성질이 긴급하지 않고 의도된 당사자의 신원이 확인될 수 없다면, 또는 당사자와 통화할 수 없다면, 단지 전화를 회신할 의도된 당사자에게 필요한 최소 필수 정보가 승인될 때만을 일반적인 호출전화 메시지로 남긴다.
4. 만약 통화의 성질이 임상적으로 긴급하고 의도된 당사자의 신원이 확인될 수 없을 경우, 또는 당사자와 통화할 수 없을 경우, 환자에게 추후 연락을 위해 정보를 제공할 때 전문가적인 판단을 이용한다. 의무기록에서 환자와 연락할 어떠한 다른 전화번호로 환자에게 연락을 시도한 것을 문서화한다. 공개에 대해서 개인정보보호 담당관에게 알린다(5-5650).

절차 – 모든 전화

- 환자로부터 받은 서명이 있는 인증서 없이는, 어떤 당사자에게 TPO(치료, 지불, 보건의료 업무) 용도가 아닌 목적으로 보호대상건강정보를 전화로 전달하는 것은 금지된다.
- 인증서 없이 비의도적인 공개가 일어난 경우 개인정보보호 담당관에게 알린다(5-5650).

VIII. 팩스를 이용한 보호대상건강정보 전달

규정

- 보호대상건강정보를 팩스기기로 전송하는 것을 보호하기 위해 합리적인 안전장치를 마련한다. 또한, 팩스로 보호대상건강정보를 전송할 때 적절한 절차를 따르는 것을 책임지는 직원들을 보유한다.
- 병원 직원은 법, 직업적 윤리, 및 인가 조건의 요구에 따라 비밀보장이 되어야 하는 의료정보의 기밀성과 무결성을 보호한다.
- 팩스기기는 안전한 장소에서 보관된다. 환자 진료 공간들, 또는 보호대상건강정보를 수신하는 공간들과 직원을 두지 않는 공간에 있어서, 부서들은 업무 종료 시에 팩스기기가 꺼지는 것을 확실하게 해야 한다.
- 보호대상건강정보는 우편으로 발송된 사본이 치료, 지불 및 보건의료 업무(TPO) 용도로의 요구를 충족시키지 못할 경우에 대해서만 단지 외부 요청자에게 팩스로 전송될 수 있다.

규정

- 보호대상건강정보는 치료, 지불 및 보건의료 업무(TPO) 목적으로 내부적으로 팩스로 전송될 수 있다. 부서 책임자들은 내부적으로 팩스로 전송된 정보의 보존 및 파기를 포함해서, 팩스 전달 관리에 대한 모든 설비별(unit-specific) 표준을 규정하고 확립해야 한다.
- 전송되는 정보는 요청자의 요구에 충족하기 위한 최소 필수 항목으로 반드시 제한되어야 한다.
- TPO(치료, 지불, 보건의료 업무)를 위해 개인의 일반적인 동의에 의해 승인되었거나 연방 또는 주 정부 법에서 요구하는 경우를 제외하고는, 어떤 방법으로든 보호대상건강정보를 전달하기 전에 적절하게 완성되고 서명이 되어 있는 허가서를 반드시 받아야 한다.
- 기밀유지 표준안과 재공개(re-disclosure) 진술서를 포함하여 팩스 표지는 보호대상건강정보를 팩스로 전송하는 모든 것에 반드시 같이 보내야 한다.

규정

- 만약 법에 의해 요청되거나 예외적으로 건강정보관리부서에 의해 공개되지 않는다면, 아래에 열거한 의료정보 형태들은 연방 및/또는 주 정보 법률에 따라 보호되고 특별히 서면으로 작성된 환자 승인서 없이 팩스로 보내거나 복사를 해서는 안된다. (Release of Information Section 6-8715):

1. 환자와 정신치료사(psychotherapist) 또는 사회복지사 사이의 전달;
2. 성병 검사 결과 또는 방문 기록들(예외: 공공보건 기관에 감염관리 보고);
3. HIV 검사와 그 관련 정보(예외: 공공보건 기관에 감염관리 보고);
4. 약물 남용 재활 치료 기록;
5. 성 폭행 치료 기록; 또는
6. 아동/노인 학대 주장(진술) 및 치료 기록

- TPO(치료, 지불, 보건의료 업무)를 위한 절대적인 필요가 아니라면 10 페이지 이상 되는 정보에 대한 요청은 정기적인 우편 서비스로 처리할 것으로 권고된다.
- 환자 정보의 팩스 전송 및 관례적인 환자 정보 요청의 타당성에 대한 특정 질문은 건강정보관리부서에 접수되어 진다(6-2271).

절차 – 팩스를 통한 보호대상건강정보 전송

1. 모든 팩스 전송에 대해서 전송에 앞서 팩스번호 수신의 확인이 필요하다:

① 실수할 가능성을 최소화하기 위해 종종 사용되는 팩스 번호들을 미리 예정하여 세운다.

② 전하로 미리 번호를 확인한다.

③ 전송에 대한 원본 요청서 상의 팩스를 참고한다.

- 표준 겉표지 서식을 채워서 첨부하는데 아래 4가지를 포함한다:

① 전송 날짜

② 발신자의 이름, 부서, 기관명, 전화번호 및 팩스 번호

③ 수신자의 이름, 부서, 기관명, 전화번호 및 팩스 번호

④ 표지를 포함한 페이지 수

절차 – 팩스를 통한 보호대상건강정보 전송

2. 전송이 완료되었을 때, (가능하다면) 정보를 보호하기 위해 팩스 승인의 재검토가 의도된 수신 팩스번호로 발송되어야 한다.

3. 만약 팩스 전송이 잘못된 번호로 간 것이 확인되었다면:

① 실수로 팩스를 받은 수신자에게 알린다(전화로 알려야 하지만, 만약 전화번호를 알 수 없다면 팩스로 알린다). 수신자에게 받은 정보를 파기하도록 지시한다.

② 의도되지 않은 공개에 대해서는 개인정보보호 담당관에게 알린다.

- TPO(치료, 지불, 보건의료 업무) 목적 – TPO 목적으로 팩스를 보내는 부서는 전송 또는 확인 사본을 보유할 필요가 없다. 추후 참고용으로 사본을 유지하는 부서가 결정권을 가지고 있다.
- TPO(치료, 지불, 보건의료 업무) 목적이 아님 경우 – 환자로부터 받은 서명된 승인서 없이 외부 대상기관에게 비TPO 목적으로 의료정보를 팩스로 보내는 것은 금지된다. 승인 없이 무심코 한 공개가 발생한 경우, 개인정보보호 담당관에게 알린다.

절차 – 팩스를 통한 보호대상건강정보 수신

1. 가능한 한 빨리, 기계로 전송된 팩스를 치우고 의도된 수신자에게 전달한다.
   만약 수신자가 자리에 없다면, 팩스 서류 도착을 수신자에게 알리고 서류를 가져가도록 안전한 공간(장소)에 보관한다.
2. 만약 팩스가 잘못 수신되었다면, 즉시 발신자에게 알린다. 수신된 정보는 없애거나 또는 잘못 수신된 환자 정보에 대한 발신자의 지시에 따른다.

IX. 전자메일을 이용한 보호대상건강정보 전달

정의 – 컴퓨터 자원들(Computer Resources)

- 병원은 컴퓨터 네트워크를 갖추고 있다. 특히, 컴퓨터 자원들은 호스트 컴퓨터(host computers), 파일 서버(file servers), 애플리케이션 서버(application servers), 통신 서버(communication servers), 메일 서버(mail servers), 팩스 서버(fax servers), 웹 서버(Web servers), 단말장치(workstations), 독립형 컴퓨터(stand-alone computers), 휴대용 컴퓨터(laptops), 소프트웨어(software), 데이터 파일(data files), 모든 내부 및 외부 컴퓨터, 그리고 병원 컴퓨터 네트워크로부터 직접 또는 간접적으로 접근될 수 있는 통신 망(communication networks 예: 인터넷 상업적 온라인 서비스, 부가가치 통신망, 이메일 시스템)도 포함하나 이것에 국한하는 것은 아니다.

정의 – 사용자들(Users)

- 병원 컴퓨터 자원을 사용할 수 있는 직원들, 의료진들, 계약업자들, 학생들 및 자원봉사자들을 포함하나 여기에 국한하는 것은 아니다.

규정

- 전자메일은 병원 업무 처리에 있어 통합된 도구로 된다. 이 규정은 병원 컴퓨터 또는 네트워크에서 메일을 보내거나 받는 병원 전자 메일 시스템의 모든 사용 방법에 적용된다. 전자메일은 직원 업무 수행에 필요한 정보를 교환하고 상호간의 전달을 용이하게 하기 위한 업무 도구로서 이용되어야 한다.
- 환자 개인정보보호와 관련하여, TPO(치료, 지불 및 보건의료 업무)가 아닌 다른 목적을 위하여 전자메일로 보호대상건강정보를 전달하는 것은 환자로부터 특정 승인, 공개에 관한 증빙서류, 및 정보보호 담당관에게 통보할 것을 요구한다.

절차 – 사용자 의무(책임)

1. 사용자는 병원 전자 메일 시스템을 통해 생성된 정보를 읽고, 입력하고, 또는 갱신하거나 전송할 권한을 가진 사람이다.
2. 사용자는 적절하게, 효과적으로, 그리고 효율적으로 이메일을 사용하고 유지할 의무를 가진다.
3. 사용자는 전자적인 전달이 (기술에 달려 있긴 하지만) 다른 사람들에 의해서 전달되거나, 방해 받고, 출력되고, 저장될 수 있다는 것을 반드시 명심해야 한다. 그러므로 사용자는 문서로 된 기록에 적용되었던 것과 같거나 또는 더 능가하는 비밀유지 보호와 판단력을 활용해야 한다.
4. 전자메일은 긴급하거나 시간에 민감한 응답이 요구되는 경우에는 사용되어서는 안된다.
5. 병원 전자메일 계정과 암호는 승인된 사용자 이외에 다른 어느 누구에게도 드러내거나 공유해서는 안된다.

절차 – 금지된 사용들(1)

- 전자메일의 사용은 모든 적용 가능한 주 및 연방 법률들 그리고 병원 관리 규정 및 절차에 근거한다.
- 병원 전자메일의 금지된 용도는 다음의 예들을 포함하나 이것에 국한하는 것은 아니다. 다음의 금지된 용도에 대한 위반은 제제위원회(Sanctions Committee)에 의해 검토, 대처되어진다. 위반은 그것의 중대성에 달려있긴 하지만, 훈육에서 최고 해고까지를 포함한다.

1. 저작권 또는 특허법 소유자에 의한 적절한 승인이 없는 상태에서 저작권 및/또는 특허법에 의해 보호되는 서류, 소프트웨어 또는 기타 정보의 복사 또는 전송(저작권이 설정된 자료의 정당한 이용은 제외)
2. 협박, 명예훼손, 풍기문란, 모욕, 또는 괴롭힘 등을 전달하는데 관계하는 것; 이것은 비업무적인 이메일을 전달하는 것도 포함한다.
3. 대학 규정에 위배되는 용도에 대한 전자메일 시스템 사용

절차 – 금지된 사용들(2)

4. 정보에 대한 합법적인 업무 없이 사적인 소유물 또는 보호대상건강정보를 대상기관 내부 또는 외부의 개인에게 전송하는 것.
5. 해당 수신자로부터의 명백한 허가 없이 판매 목적으로 전자메일 시스템 사용
6. 고도로 비밀을 유지해야 하거나 민감한 정보의 전송(예: HIV감염 상태, 정신질환, 약물의존 및 산업재해보상 소송 등)
7. 명백한 법률 고문의 승인 없이 병원 내 또는 외부 법률 고문으로부터 온 전자메일 또는 메일 내용을 대상기관 외부의 개인에게 전달하는 것.
8. 전자적인 전달 상에 사용자의 신원이 부정확하거나, 분명치 않거나, 감추거나, 또는 다른 사람이 대신한 경우
9. 승인 또는 합법적인 업무 목적 없이 파일에 접근하거나 다른 사람에게 전달하는 것
10. 데이터에 인가되지 않은 접근을 시도 하거나 어떠한 전자 전달 시스템 상에서 보안 수단의 파손을 시도하는 것. 또는 적절한 승인 없이 전자 전달 및 전송의 방해를 시도하는 것.

절차

- 아래에 열거된 의료 정보 형태들은 연방 및/또는 주 법률에 의해 보호되고 만약 법에 의해 요청되거나 건강정보관리부서에 의해서 예외적으로 공개되지 않는다면 환자의 서면 승인서가 없이 공개되지 않을 수 있다. (Release of Information Section 6-6830)

① 환자와 정신치료사(psychotherapist) 또는 사회복지사 사이의 전달;

② 성병 검사 결과 또는 방문 기록들(예외: 공공보건 기관에 감염관리 보고);

③ HIV 검사와 그 관련 정보(예외: 공공보건 기관에 감염관리 보고);

④ 약물 남용 재활 치료 기록;

⑤ 성 폭행 치료 기록; 또는

⑥ 아동/노인 학대 주장(진술) 및 치료 기록

- 이상의 6가지는 포괄적인 것으로 간주되지 않는다. 전자메일의 적절한 이용에 대한 더 자세한 질문은 고용인 감독관(employee's supervisor), 보안 담당관, 및/또는 개인정보보호 담당관에게 바로 할 수 있다.

절차 – 전자메일에 대한 소유권 및 사용자 개인정보보호

- 전자메일의 사용은 병원 업무 처리과정의 한 부분이다. 병원 전자메일 시스템 내로 수신되거나 병원 내부에서 발생하고 전달되는 모든 메시지들은 병원의 소유물로 간주된다.
- 전자메일 시스템 사용자 모두는 그들이 전자메일 시스템을 사용하는 것과 관련하여 개인정보보호에 대한 기대를 가져서는 안된다는 것을 이해해야 한다.
- 병원은 병원 자산의 적절한 활용과 합법적인 업무 관심의 보호를 보장할 목적으로 전자메일 시스템에 접근할 권리를 가지고 보유한다.
- 그런 목적은 아래에 열거한 것들을 포함하지만 이것에 국한하지 않는다.

1. 잃어버린 메시지의 위치를 찾아내거나 갱신하는 것;
2. 직원이 근무지 밖에 있거나 활용할 수 없을 때 업무를 수행하는 것;
3. 메시지 유형을 분석함으로써 시스템 관리를 유지하고 필요하다면 수정을 수행하는 것;

절차- 전자메일에 대한 소유권 및 사용자 개인정보보호

4. 진행 중인 시스템의 가용성과 신뢰성을 보장하기 위해 전자 전달을 수집 또는 관리하는 것;

5. 협박, 명예훼손, 풍기문란, 모욕, 또는 괴롭힘 등으로 간주되는 전자메일을 시스템으로부터 영구히 제거하는 것;

6. 시스템 고장 및 다른 예기치 못한 응급상황으로 부터 복구; 그리고

7. 의심되는 보안 파손 또는 상당한 이유가 있는 규정 위반을 조사하는 것.

- 전자메일 정보는 때때로 정기적인 점검수행, 유지, 및 문제 해결에 종사하는 ITS 직원에게 보이게 된다. 이런 업무를 수행하도록 맡은 직원은 전자메일 내용을 의도적으로 읽거나, 다른 사람에게 공개해서는 안된다.
- 감독관들 / 관리자들은 직원 파일에 접근하기에 앞서 직원들이 메시지를 검토한 그들의 의도에 대하여 개인정보보호 담당관 및/또는 보안 담당관으로부터 반드시 승인을 받고 권고해야만 한다.

절차 – 전자메일의 비밀유지

- 병원 전자메일 시스템 사용자들은 시스템을 통하여 전송된 메시지를 전달, 출력 및 배포(회람)할 수용능력을 가지고 있다. 그러므로:

1. 사용자들은 문서화된 서류에 적용되는 것과 같거나 능가하는 수준의 비밀유지를 위한 보호를 하고 판단력을 활용해야 한다.
2. 전자메일이 비밀유지가 되어야 하고 민감한 정보 전달에 이용되었을 때, 정보의 기밀유지 보호 수단으로 특별한 조치들이 반드시 취해져야 한다. 이러나 보호수단은 아래와 같다:

① 비밀유지가 되어야 하고 민감하다고 간주되는 정보는 정보가 의도된 수신자 이외의 다른 사람에 의해 접근될 가능성을 감소시키는 이용 가능한 접근 통제를 활용하여 데이터 전송 동안 반드시 보호되어야 한다.

② 두드러지는 장소에서 비밀유지가 되어야 하고 민감한 성질의 정보에 대해 조회하는 표기 또는 플래그(flag)는 메시지에 부착되어야 한다.

③ 비밀유지가 되어야 하거나 민감한 정보는 합법적인 TPO 목적을 위해 다수의 수신자에 배포될 수 있다; 그러나, 최소 필수 항목 공개와 보장하고, 배포 명단 리스트의 이용은 금지된다.

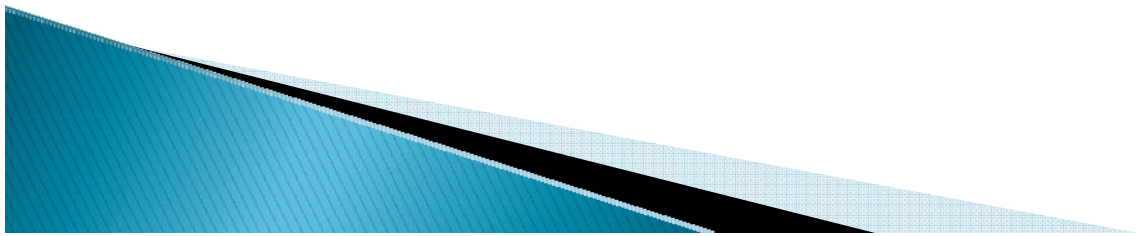
절차 - 전자메일함의 용량(크기) 및 전자 메일 보존

- 기술적 자원의 제한과 비용 때문에, 메일함 용량은 공동작업 서버(Exchange server) 상에서 아래의 용량으로 제한된다.
- 이것에 대한 예외는 직원관리 책임자(예: 간호 감독, 외래 감독 등)에게 요청하고 정보책임자(CIO)의 승인이 필요하다.

1. 직원 및 중간관리자 - 100 Meg 제한
2. 학장, 원장 및 부서 책임자 - 300 Meg 제한
3. 병원 지휘부(leadership staff) - 무제한

- 일반적으로, 전자메일은 non-vital한 일시적인 전달(의사소통)의 의미를 부여하고 주기적으로 폐기될 수 있다. 그러나, 전자메일 내용에 따라서는, 좀 더 형식적인 기록으로 간주될 수도 있고 병원의 기록 보존 일정에 준거하여 보존되어야 한다. 전자메일 테이프 백업(저장)은 업무복구(business recovery) 목적을 위해 규칙적으로 수행된다. 전자적으로 저장된 정보는 법적 검색 과정으로 채택되어 소환될 수 있다.

X. 환자개인정보 보호/보안 불만사항 전달



규정

- 환자, 직원, 학생 및 의료진은 수립되어 있는 공식적인 절차를 통해 불만사항을 모아둘 수 있다.
- 불만사항은 익명으로 될 수 있고 어떠한 앙갚음이나 보복도 없을 것이다.

절차 – 병원 직통전화(Hot Line)

1. 1년 365일 내내, 일주일 내내, 하루 24시간 내내 866-665-4296으로 전화
2. HIPAA와 관련된 개인정보보호 불만은 정보보호 담당관에게 위탁한다(312-355-5650).
3. HIPAA와 관련된 보안 불만은 정보보안 담당관에게 위임한다(312-996-0660).
4. 정보보호 담당관/정보보안 담당관은 적적하게 불만 처리를 해나간다.
5. 정보보호 담당관/정보보안 담당관은 적절하게 고객에게 해결사항을 전달한다.
6. HIPAA와 관련되지 않은 불만은 이행완료서(satisfaction form)를 작성하고 추후관리를 위해 고객 서비스부서(Guest Services)에 위임한다.
7. 불만은 적절한 서비스들에 의해 처리된다.

절차 – 정보보호 담당관(Privacy Officer)

1. 정규 업무 시간 동안에는 312-355-5650으로 전화를 하거나 아래 주소로 편지를 보낸다.

University of Illinois Medical Center at Chicago
Attention: Privacy Officer
Health Information Management Department
833 S. Wood Street M/C 772
Chicago, Illinois 60612

2. 정보보호 담당관은 불만 처리를 해나간다.
3. 정보보호 담당관은 고객에게 해결사항을 전달한다.
4. HIPAA와 관련되지 않은 불만은 추후관리를 위해 고객 서비스부서(Guest Services)에 위임한다.
5. 불만은 적절한 서비스에 의해 처리된다.

절차 – 정보보안 담당관(Security Officer)

1. 정규 업무 시간 동안에는 312-996-0660으로 전화를 하거나 아래 주소로 편지를 보낸다.

University of Illinois Medical Center at Chicago
Attention: Security Officer
Information Services Department
1740 West Taylor M/C 695
Chicago, Illinois 60612

2. 정보보안 담당관은 불만 처리를 해나간다.
3. 정보보안 담당관은 고객에게 해결사항을 전달한다.
4. HIPAA와 관련되지 않은 불만은 추후관리를 위해 고객 서비스부서(Guest Services)에 위임한다.
5. 불만은 적절한 서비스에 의해 처리된다.

절차 – 민권 담당국(Office for Civil Rights)

- 환자는 미국 보건복지부 민권 담당국(주소: 200 Independence Avenue, S.W., Room 509F, HHH Building, Washington, D.C. 20201)에 연락할 수 있다. 이 사무소에 불만을 제소할 때는 문서로만 가능할 수 있다.

XI. 보호대상건강정보의 파기

정의 – 파기(Destruction)

- 지정된 폐기함(disposal container)에 버리거나 또는 분쇄장비를 이용하여 보호대상건강정보를 포함하고 있는 모든 형태를 판독할 수 없는(읽을 수 없는) 상태로 만드는 것.

규정

- 병원 직원들, 교수진들, 학생들, 그리고 자원봉사자들은 보호대상건강정보를 포함하고 있는 어떤 문서든 무결성과 기밀성을 보호한다.
- 보호대상건강정보를 포함하고 있는 문서들은 안정한 장소에 보관되고 항상 직원의 관리 하에 있다.
- 보호대상건강정보를 포함하고 있는 문서들은 임상적, 업무적 또는 다른 사용 목적들이 합법적으로 요청 받도록 보유된다. 그리고 일리노이 주 법률에 따라 영구적으로 저장, 보관(축적) 또는 파괴된다.
- 담당부서 책임자(Department Director)는 이러한 같은 법률 규정에 근거하여 보호대상건강정보를 포함하고 있는 보관된 문서들을 폐기하기 위해서는 정기적인 계획표를 확립해야 할 것이다.

규정

- 문서들은 종이조각으로 만드는 파쇄기(“confetti")를 이용하여 현장에서 파쇄 될 수 있다. 만약 파쇄기를 현장에서 작동할 수 없다면, 보호대상건강정보를 포함하고 있는 모든 매체는 반드시 ”파쇄(Shred-It)" 보관소(쓰레기통)에 넣어 놓고 매각자(vendor)가 이것들을 회수할 수 있을 때까지 보안이 철저한 장소에 보관해야 한다.
- 담당부서는 ”파쇄(Shred-It)" 보관소의 위치를 배정하기 위해 반드시 시설관리 책임자에게 연락해야 한다.
- 의무기록 원본 문서와 관련된 규정에 대해 참조하고 기타 조직관련 기록에 대한 규정은 참조한다.

절차 – 부서별 저장 표준 수립

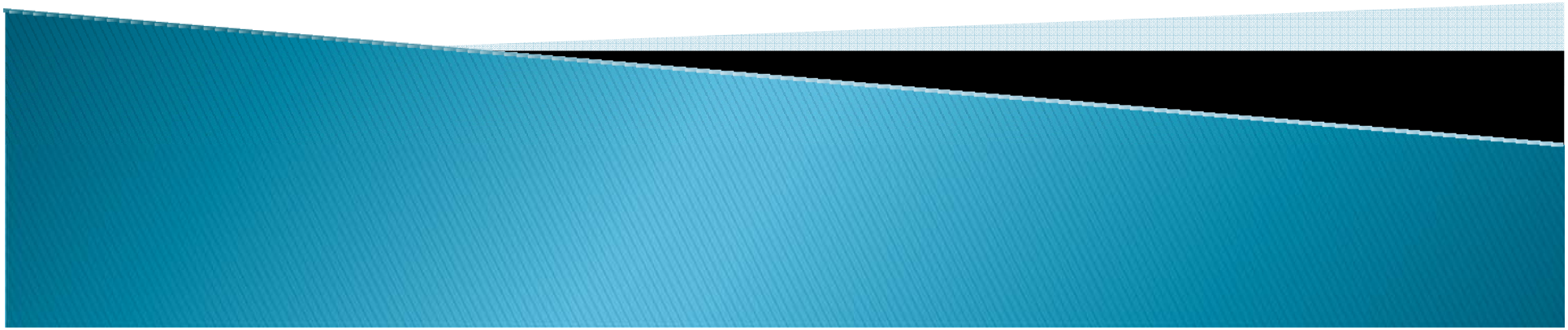
- 부서 책임자들 또는 지명된 사람들은:

1. 부서별 현장 보관 및 파쇄 용량을 평가한다.
2. 적절한 보관 또는 파쇄 장비가 조달되는 것을 보장한다.
3. 보관 및 파쇄 장비 사용에 대한 부서별 지침서를 개발한다.
4. 모든 의료진, 교수진, 학생들 및 자원봉사자들이 장비 사용에 대한 훈련을 받도록 보장한다.
5. 보호대상건강정보를 포함하고 있는 문서들의 적절한 파기 기준에 준수하는지를 감독한다.

절차 - 보호대상건강정보를 포함하고 있는 문서들의 파기

1. 현행업무에 활용되지 않는 비활용(non-current)문서들을 확인한다.
2. (MCMPP IM 2.01 Documentation - Minimal Content of Patient Record)에 따라서 어떠한 원본 의무기록 문서라도 보건정보관리자에게 보낸다.
3. (MCMPP IM 2.04 Records Retention and Disposal-Archival Deposit of Organizational Records)에 따라서 문서보관소의 기록을 준비하고 대학 기록물보관소에 보낸다.
4. 허가된 보관소 매수자(storage vendor)에게 부서별 규정들과 절차에 의해 정해진 대로 현장 보관을 위한 기록을 준비하고 보낸다.
5. 파쇄하는 방법으로 다른 모든 문서들을 파기한다(만약, 이용 가능한 현장이 있다면). 만약 현장에서 파쇄할 수 없다면, 문서가 지정된 안전한 장소/저장소에서 파쇄되도록 놓아 두거나 부서 일정에 따라 지정된 파쇄 장소로 수송하도록 배열하거나 수송한다.

II. Practical Cases under the HIPAA training

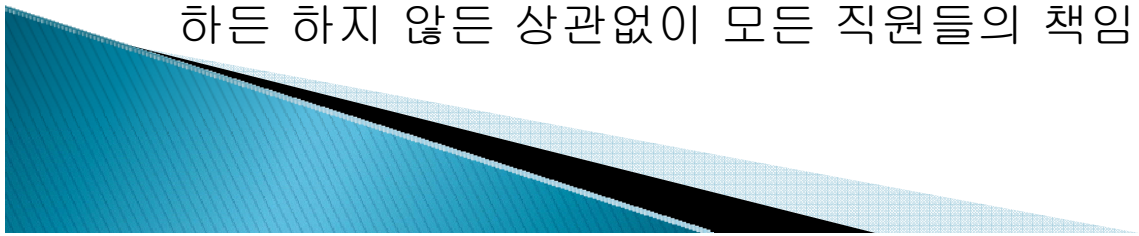


Case #1

Q. 동생의 친한 친구가 일하는 병원에서 수술을 받았다. 동생이 친구의 컨디션에 대해서 물었다. 아는 간호사에게 이것에 대해 물어볼 수 있는가? 그 친구의 의무기록을 볼 수 있는가?

A. 명확하게 대답은 "아니오"이다.

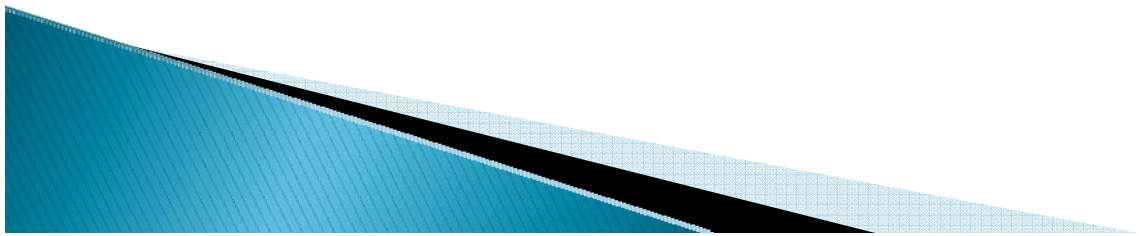
- 아무리 당신과 동생이 좋은 의도를 갖고 있다 할지라도 그 친구의 건강에 대한 개인적인 정보에 대한 접근권한은 없다.
- 일과 관계없이 환자의 정보를 보는 것은 면직의 사유가 될 수 있고, 법적 결과를 가져올 수 있다. 따라서, 알게 된 기밀정보를 공유하거나 발설하면, 고의든 아니든 해고될 것이다.
- 이 규정은 모든 고용자에게 적용된다. 기밀정보의 보호는 환자를 직접 관리하든 하지 않든 상관없이 모든 직원들의 책임이다.



Case #2

Q. 어떤 사람이 컴퓨터로 작업하기 위해 병원에 왔다며, 문을 열어달라고 하고, 시스템으로 가는 길을 알려달라고 한다. 당신은 어떻게 대답할 것인가?

A. 가장 좋은 대답은 이 사람이 조직의 누구와 연락 하였는지 물어보는 것이다. 그리고 그 사람을 찾는다. 수리공을 적절한 작업구역으로 데려갈 수 있다. 이 수리공이 누구와 연락했는지 말하지 않는다면, 감독자 또는 프라이버시 관리자에게 알린다.

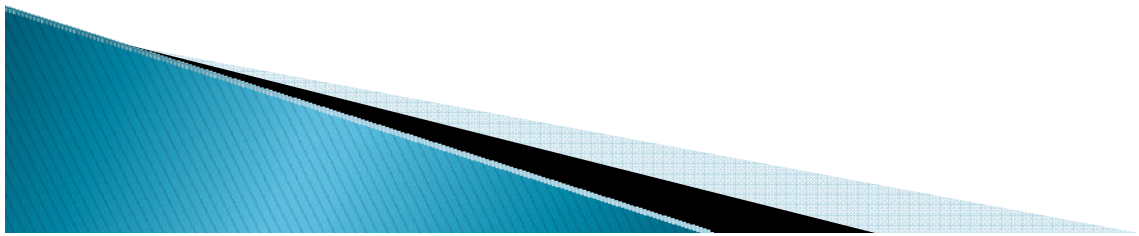


Case #3

Q. 업무 중에 환자의 이름을 보았는데, 아는 사람이라는 것을 알게 되었다. 그의 상태가 어떤지 알아보기 위해 그에게 전화해야 하는가?

A. 아니오.

기록에 있는 이름을 우연히 보게 되어, 친구의 상태를 알게 된다면 그에게 전화해서는 안 되고, 당신이 무엇을 알아냈는지 누구에게든 언급해서는 안 된다. 왜냐하면 친구는 다른 사람이 수술에 관해서 알게 되는 것을 원하지 않을 것이고, 프라이버시를 지키는 것은 그의 권리이기 때문이다.



Case #4

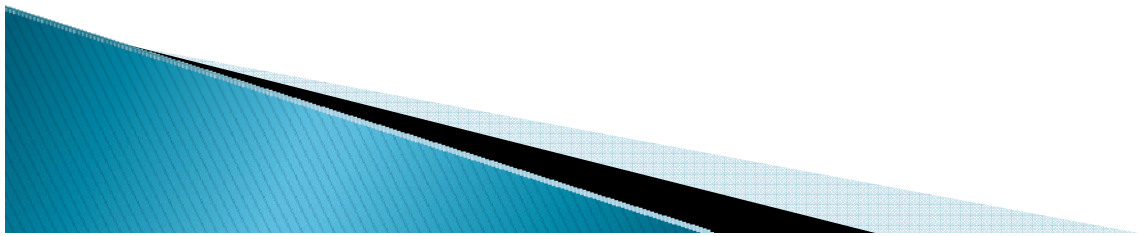
Q. 개인정보를 포함한 문서를 처분하는 저장고가 넘치고 있다.

여기에는 환자의 성명 목록과 의무기록 번호를 가지고 있다.

이 목록을 공개된 쓰레기통에 버릴 수 있는가?

A. 아니오.

환자의 정보를 포함하는 종이는 찢어서 파기되거나 이를 적절하게 폐기하는 업체로 전달되기 위해 잠금 저장고에 버려야 한다.

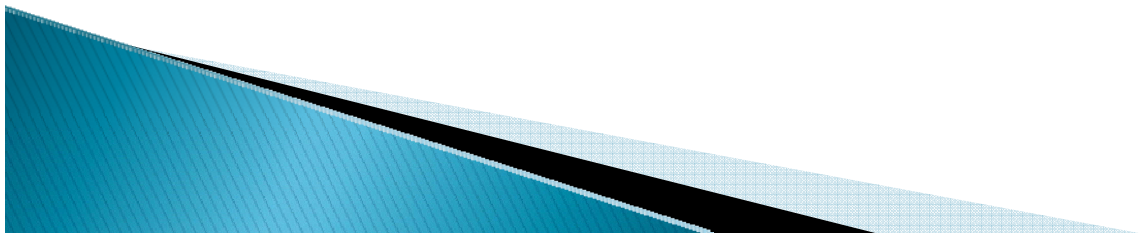


Case #5

Q. 의사가 HIM 사무실에 전화하여 환자에 대한 리포트를 사무실로 보내겠다고 한다. 하지만, 사무실은 닫혀있고, 내일 아침까지 팩스를 받을 사람이 없다. 어떻게 해야 하는가?

A. 기계가 잠긴 방안에 있다는 것이 확인되지 않는다면, 사람이 없는 기계로 팩스를 보내면 안 된다.

팩스기계가 밖에 있다면, 정규 업무시간에 사무실에 있는 직원이 팩스를 기다려 즉시 수취할 수 있다.



Case #6

Q. 동료 Transcriptionist가 시스템에 접근하는데 어려움을 겪고 있다. 그는 접근 시도를 위해 당신에게 로그인 이름과 패스워드를 요구한다. 당신을 이것들을 공유할 수 있는가?

A. 아니오.

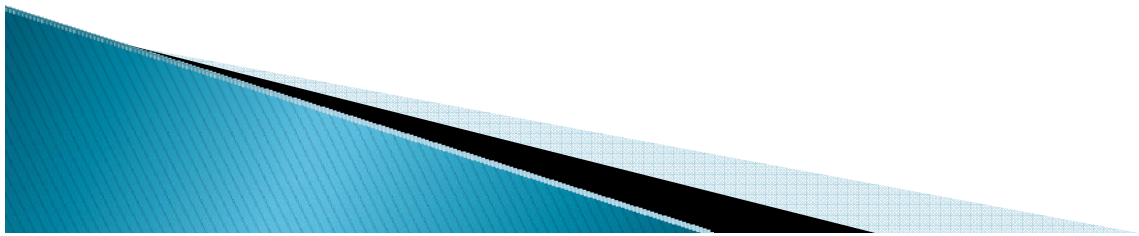
- HIPAA 보안 표준은 각각의 직원들이 컴퓨터 시스템에 저장되어 있는 정보에 접근하기 위한 개인 패스워드의 사용을 요구한다. 시설은 시스템에 들어가기 위해 사용하는 로그인 이름과 패스워드를 기본으로 한 기록의 추적을 유지한다. 만약 다른 사람에게 당신의 이름과 패스워드를 사용하도록 허락하는 것은 HIPAA의 규정을 위반하는 것이고 그들이 부적절하게 환자정보에 대한 접근을 하는 것에 대한 책임이 있다.
- 직원들은 시스템에 접근하기 위한 고유의 로그인 이름과 패스워드를 사용하여 시스템보안을 유지해야 한다. 직원은 비밀번호를 공유할 수 없고, 병원 정책과 절차를 기본으로 정규적으로 패스워드를 변경해야 한다.

Case #7

Q. 컴퓨터 기록 시스템을 위한 패스워드를 90일마다 변경해야 하므로, 그것을 기억하는 것이 힘들 수 있다. 패스워드를 종이에 메모하여 책상서랍에 붙여도 되는가?

A. 절대로 안 된다.

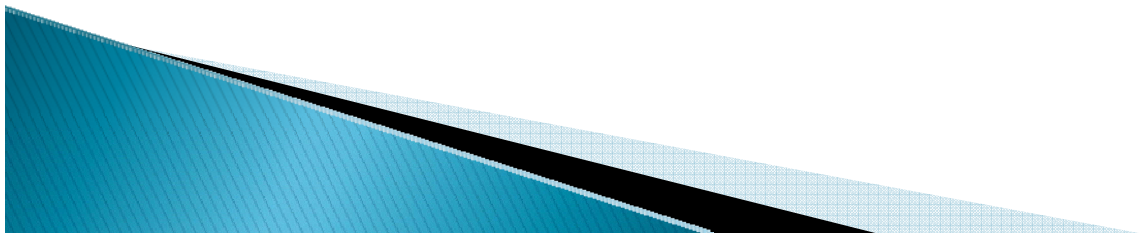
- 책상 서랍이 잠겨 있을지라도, 항상 서랍을 열기 때문에 다른 사람이 당신의 패스워드를 볼 수 있는 기회가 있다. 즉, 패스워드를 적어두면 안된다.
- 패스워드를 기억하기 어렵다면, 패스워드를 떠올리기 위한 팁을 얻기 위해 정보시스템부서의 직원에게 물어본다. 하지만 기억하는 것이 좋다.



Case #8

Q. 지역의 비영리 단체 소속 연구자가 암 치료에 관한 연구를 하고 있어 지난 해에 유방암으로 치료받은 모든 환자들의 기록을 보기 원한다. 이 사람에게 정보를 공개할 수 있는가?

A. 아니오. 연구자가 이 기록을 보기 위해서는 신상정보를 제거해서 연구자가 환자가 누구인지 알 수 없게 할 것이라며 각 환자들에게 인증을 받아야 한다. 연구자는 신상정보 제거 없이 기록의 공개를 허가하는 기관심의위원회(IRB)와 프라이버시 위원회로부터 면제(waiver)를 받아야 한다.

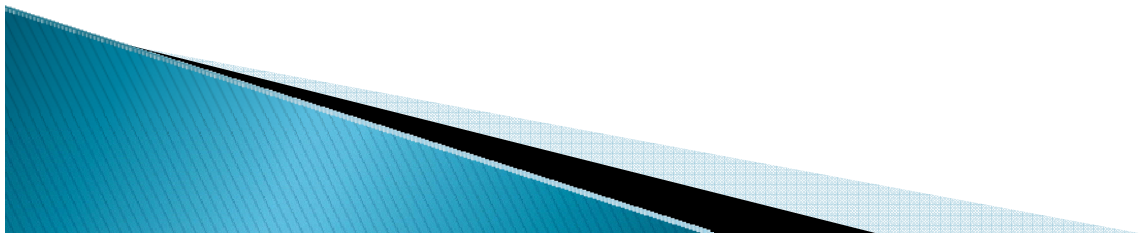


Case #9

Q. 환자는 자신의 정보가 공개된 것에 대한 설명 요구 권한이 있으므로 3일간의 입원기간 동안 자신의 기록을 본 의사와 간호사 명단을 보고자 한다. 환자에게 이 리스트를 줄 수 있는가?

A. 아니오.

- 정보 공개에 대한 설명 요구에는 치료 목적을 위한 기록의 사용을 포함하지 않아도 된다.
- 만약, 환자가 직원이 그의 의무기록을 부적절하게 보았다고 의심하면, 프라이버시 관리자와 불만을 처리하는 담당자에게 불만사항을 제시할 수 있다.



Case #10

Q. 환자가 병원의 디렉터리에 그의 이름과 정보가 포함되지 않기를 요구한다. 한 여자가 이름으로 환자를 찾아달라고 요구하면서, 자신이 그 환자의 엄마라고 하며, 이를 증명하기 위해서 자신의 운전 면허증을 보여준다. 이 엄마에게 당신을 뭐라고 말해 줄 수 있는가?

A. 엄마가 관리제공자에게 알려지지 않았고, 입원 기간 동안 환자의 치료에 적극적으로 관여되지 않았다면, 그녀에게 아무것도 알려주어서는 안 되며, 심지어 환자의 위치도 알려주어서는 안 된다.

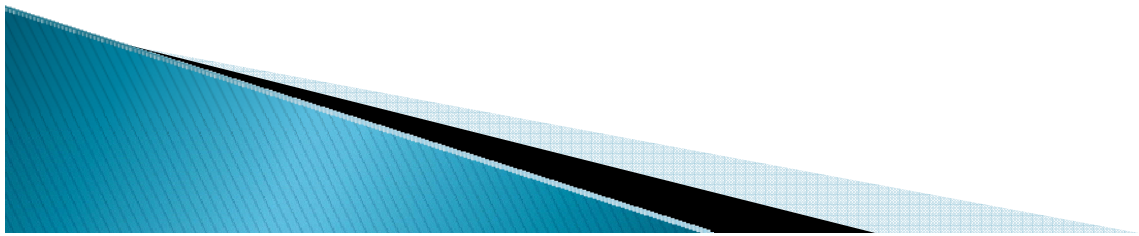
- 만약 환자가 그의 이름이 디렉터리에 포함되지 않기를 요구한다면, 병원직원은 환자와의 개인적 관계와 상관없이 그 누구에게도 그에 관한 정보를 주어서는 안 된다.
- 고객의 관계에 관한 문제를 피하기 위해, 엄마에게 프라이버시 실행 알림 사본을 제공할 수 있다. 환자의 프라이버시는 아주 중요하다는 것을 설명하고, 환자가 기밀성에 대해서 요구하면, 그 요구를 지켜야 한다.

Case #11

Q. 병원에서 정신 상담을 받고 당뇨 치료를 받은 환자가 자신의 의무기록 사본을 요구한다. 환자에게 접근 권한을 제공하기 전에 정신 상담에 관한 내용은 문서에서 제거해야 하는가?

A. 아니오.

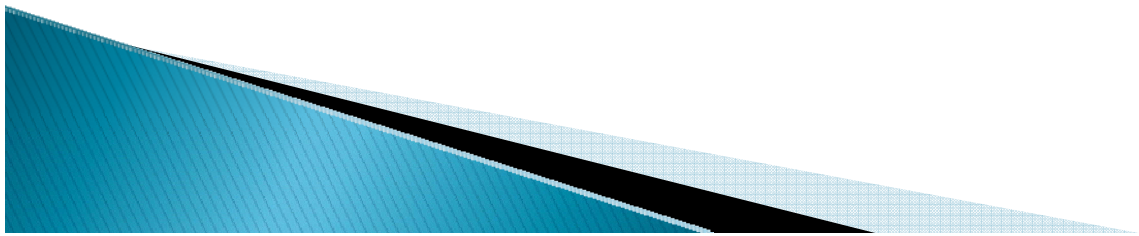
- 특별한 처리는 HIPAA에서 신중하게 정의된 정신기록에만 적용된다. 이 기록은 환자의 다른 의무기록과 분리되어 유지되어야 한다.
- 환자는 자신의 정신과 치료, 의약품 처방전, 감시, 치료의 유형과 횟수, 임상적 검사의 결과, 예후, 경과를 포함하는 자신의 기록을 볼 권한이 있다.



Case #12

Q. 붐비는 레스토랑에서 자리를 기다리면서, 환자의 진단에 관한 질문에 의사가 답을 했는지 확인하고 싶어 한다. PDA를 가지고 있고 의사의 답을 볼 수 있는 병원의 시스템에 로그인 할 수 있다. 당신은 어떻게 하겠는가?

A. 시설의 정책과 보안 메커니즘이 허가한다면, 시스템에 로그인 할 수 있고, 원하는 정보를 찾을 수 있지만, 레스토랑 한 가운데에서는 안 된다. 다른 사람이 없는 자가용, 빈 공간과 같은 개인적인 공간으로 이동하여 정보를 볼 수 있다.



Case #13

환자가 오빠에게 자신의 PHI를 공개하지 않을 것을 병원에 요구한다. 환자는 요구를 서면으로 제출하였고, 병원도 동의했다. 후에, 병원에서 환자는 신부전 말기로 판명되었다. 환자의 오빠는 병원을 방문하여 간호사에게 동생의 상태에 대한 가장 최근의 정보를 요구한다.

Q. 간호사는 오빠에게 환자의 어떤 PHI를 공개할 수 있는가?

A. 아무것도 공개해서는 안 된다.

- 환자는 병원 직원들에게 자신의 PHI 공개를 제한하도록 요구할 권리가 있다. 만약 환자가 가족에게 자신의 PHI를 절대로 공개하지 말 것을 병원에 요청하고, 병원이 이러한 제한을 수락한다면, 어느 때이건 어떤 형태이건 해당 환자의 PHI를 가족에게 공개하면 안 된다.

Case #14

실험실에서 일하는 사람이 자신이 교회에서 알게 된 사람의 이름이 붙여진 표본을 받게 되었다. 그는 환자 결과에서 의학적 문제가 있다는 것을 알게 되었다. 그는 교회에 다니는 다른 사람에게 이 정보를 말했고, 그 사람은 기도회에 이에 대해 말했다. 순식간에 수백 명의 사람들이 환자의 질병에 대해서 알게 되었다.

Q. 이것은 용인되는 공개인가?

A. 아니오. 만약 환자기록을 비즈니스가 아닌 이유로 보았다면 면직과 법적 처벌을 받을 수 있다. 마찬가지로 정당한 이유로 기록을 보았지만 이를 알 권한이 없는 사람에게 알렸다면, 조직의 정책과 법률을 위반한 것이 된다.

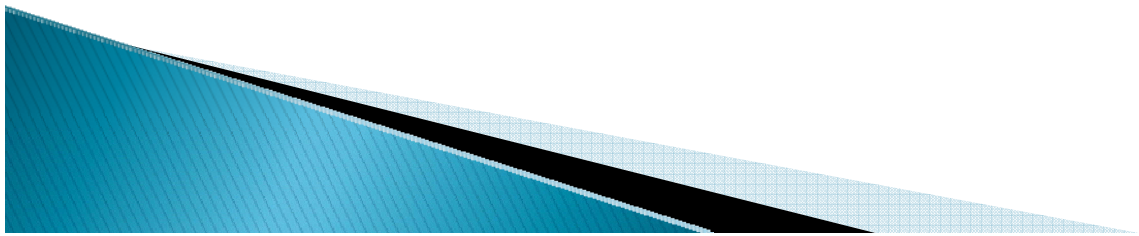
- 이 규정은 조직에 있는 모든 사람(직원, 의사, 간호사, 자원봉사자 포함)에게 적용된다는 것을 명심해야 한다. 만약 의사 또는 간호사가 환자에 대한 기밀정보를 치료목적이 아닌 이유로 본다면, 해고되거나 병원에서 일할 수 있는 특권을 잃게 된다. 의사 또는 간호사가 정보를 알 권한이 없는 외부의 사람과 정보를 공유한다면 해고되거나 병원에서 일할 수 있는 특권을 잃게 된다. 게다가 이는 법적 결과를 초래하고 면허가 정지/취소될 수도 있다.

Case #15

쓰레기통에서 환자의 이름과 주소가 있는 리스트를 발견하였다.

Q. 이것을 어떻게 처리해야 하는가?

A. 가장 좋은 방법은 리스트를 쓰레기통에서 빼서 관리자에게 주는 것이다. 관리자는 이를 병원의 프라이버시 또는 정보보안 관리자에게 보고할 것이고 이들은 왜 PHI가 부적절하게 처리되었는지를 밝혀내는 노력을 할 것이다.



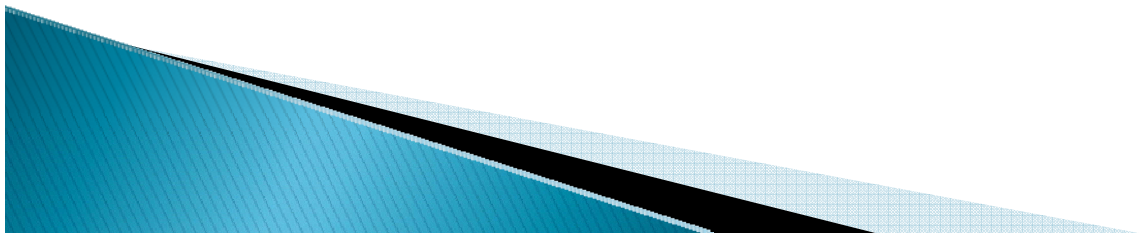
Case #16

환자를 치료한 후에, 간호사가 차트를 열려있는 차트 홀더에 두었다.

Q.이것은 HIPAA의 프라이버시 규정 위반인가?

A. 아니오.

- HIPAA 프라이버시 규정은 병원이 환자의 프라이버시를 보호하기 위하여 잠금 챠트 홀더를 사용할 것을 요구하지 않는다. 하지만 차트 홀더에 차트를 보관하는 것은 환자의 이름을 쉽게 볼 수 없게 하므로 좋은 생각이다.

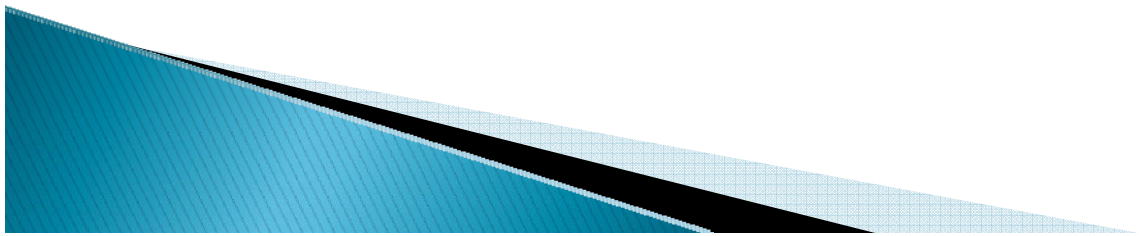


Case #17

한 직원이 휴가 중이고, 그의 동료가 그를 대신해서 일한다. 휴가를 떠난 직원은 자신의 노트북을 잠가서 캐비닛에 두었지만, 동료에게 캐비닛 열쇠와 노트북 패스워드를 알려 주어 동료가 일을 할 수 있었다.

Q. 휴가간 직원이 잘못한 것이 있는가?

A. **그렇다.** 직원은 그의 동료와 패스워드를 공유해서는 안 된다. 만약 동료가 필수적인 기록에 접근할 수 없거나 애플리케이션에 필요 항목을 삽입할 수 없다면, 그 동료의 사용자 ID와 패스워드를 사용하여 정보에 접근해야 한다. 최상의 방법은 이 상황을 담당자와 상의하여 동료에게 확장된 접근권한을 임시적, 영구적으로 주는 것이다.

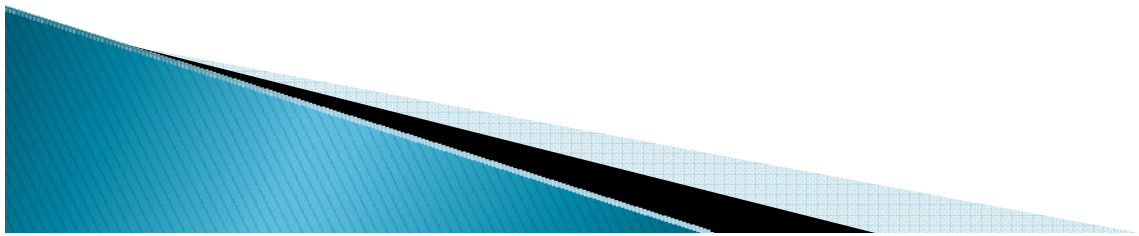


Case #18

당신은 출장으로 비행 중이다. 공항에 도착했을 때, 비행이 지연되었음을 깨달았고, 붐비는 터미널에 앉아 노트북으로 일을 시작하였다. 몇몇 환자의 기록에 대한 접근을 하고, 그 기록을 열람하였다. 컴퓨터 스크린은 다른 사람의 시야 내에 있고, 옆에 앉은 사람이 이를 볼 수 있다.

Q. 이것이 잘못되었는가?

A. **그렇다.** 환자의 PHI 기밀성을 보호하기 위해 더 주의를 기울여야 한다. 예를 들어, 자리를 변경하거나, 위치를 바꿔 다른 사람이 스크린을 볼 수 없도록 노트북 스크린을 보호해야 한다. 만약 이것이 불가능하다면, 환자의 PHI를 포함하지 않은 문서로 작업하는 것이 좋을 것이다.



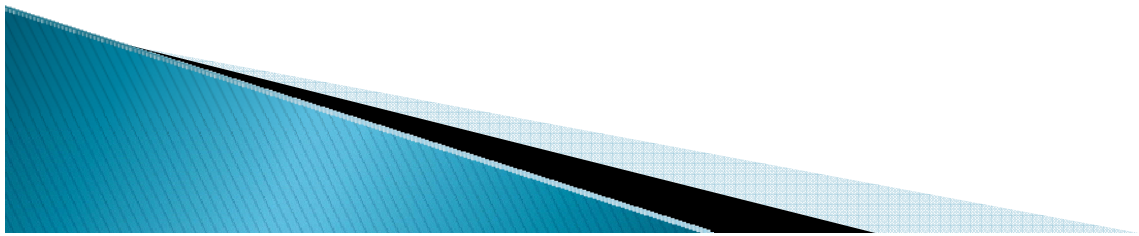
Case #19

한 직원이 그가 신뢰하는 부하직원에게 패스워드를 알려주었다. 그 부하직원은 그가 자리를 비웠을 때 그의 전자메일 메시지만 확인할 수 있다.

Q. 이를 용인할 수 있는가?

A. 아니오. 이것은 **보안위반**이다.

- 직원이 전자메일 메시지에서 어떠한 기밀적인 것이 있을 것이라고 생각하지 않았을지라도 모든 패스워드는 비밀로 지켜져야 한다.
- 직원은 그의 부하직원이 얼마나 신뢰할 수 있는 지와 상관없이 패스워드를 공유하면 안 된다.

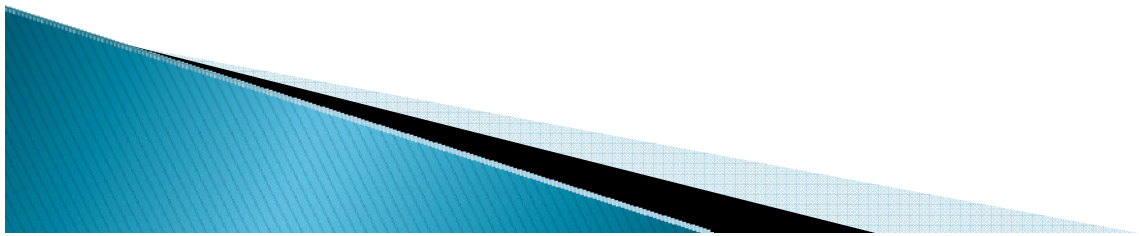


Case #20

친구들과 동료들이 컴퓨터에 인터넷 메신저(IM)를 설치하고, 당신의 컴퓨터에도 설치하기를 원한다. 안전하게 보이는 사이트를 찾아서 소프트웨어를 다운로드하고 설치하였다.

Q. 이것이 잘못되었는가?

A. **그렇다.** 절대로 인증되지 않은 프로그램이나 소프트웨어를 컴퓨터에 설치하면 안 된다. 업무용 컴퓨터는 업무만을 위한 것이다. 컴퓨터에 있는 모든 것은 IT 부서에서 승인되어야 한다. IM과 같은 소프트웨어는 새로운 보안 위험을 생성하고, 조직에서 금지하고 있다.



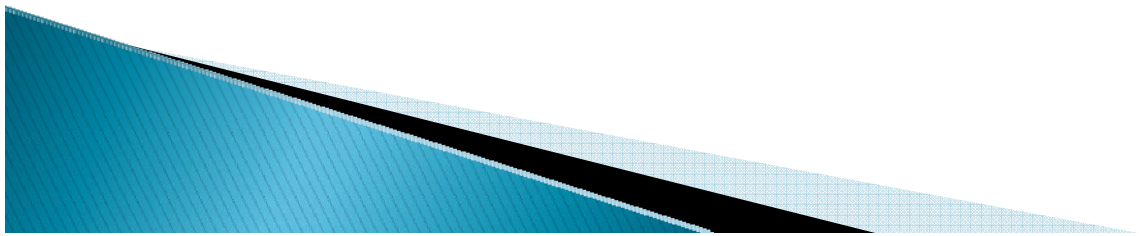
Case #21

동료가 패스워드를 잊어버려 환자 데이터에 접근할 수 없어 더 이상 업무를 할 수 없다. 이를 안타깝게 여긴 당신은 내일 아침 일찍 떠나고 ID와 패스워드를 사용하지 않으므로 동료에게 ID와 패스워드를 주었다. 불행하게도, ID를 사용하는 동안에 병원에서 치료받고 있는 친구의 기록을 동료가 뽑았다.

Q. 당신은 책임이 있는가?

A. 부분적으로 책임이 있고, 처벌 받을 것이다.

- 이 시스템에는 기록을 보는 사람을 보여주는 log audit가 있어서 위반에 대한 책임이 있다.
- 동료는 그의 잘못된 행위에 대한 책임이 있을 것이다. 하지만 이는 당신이 동료에게 ID와 패스워드를 제공하지 않았다면 일어나지 않았을 것이다.



Case #22

병실의 호출을 받아 노크를 하고 안으로 들어갔다. 병실에서는 간호사들이 환자의 상태와 투약에 대해서 얘기 중이었다.

Q. 무엇을 해야 하는가? 업무를 수행해도 되냐고 물어봐야 하는가? 또는 나중에 다시 와야 하는가?

A. 업무가 환자관리에 중요한 것이라면, 업무를 해도 되는지 물어본다. 그렇지 않다면 업무를 하기 위해 병실 왔고, 15~20분 뒤에 다시 오겠다고 설명한다. 이것이 그들의 의논하는 것을 엿듣지 않고 환자의 프라이버시를 보호하는 것이다.

- 일부 환자들이 상담하는 동안 당신이 있는 것이 괜찮다고 말할지라도, 환자는 당신이 병실에 있는 동안에 증상에 관한 정보를 공유하는 것에 불편해 한다는 것을 명심해야 한다. 일부 환자는 나가달라고 요구하는 것을 불편해 할 수도 있다. 일부 간호사는 그들이 환자와 치료에 관한 얘기를 하는 동안에 심지어 당신이 병실에 있으면 안 된다는 사실을 잊어버린다.
- 환자의 관리를 방해하지 않기 위해 나중에 다시 온다고 그들에게 말하는 것이 프라이버시 유지 실행의 좋은 보기이다.

Case #23

신문에서 어떤 유명한 사람이 병원에 왔다고 보도하였고, 이것이 사실인지 알고 싶어 한다.

Q. 이 사람에 관해 주위에 물어보거나 기록을 찾을 수 있는가?

A. 명백하게 대답은 '아니오'이다. 호기심을 만족시키기 위해 정보를 열람하는 것은 허가 되지 않는다. 만약 업무가 아닌 이유로 환자의 기록을 보면, 이는 면직의 사유가 되거나 가능한 법적 결과를 초래한다. 이 법률은 의무기록에 대한 접근 권한이 없는 사람뿐만 아니라 모든 사람들에게 적용된다는 것을 명심한다.

- 환자의 기밀정보를 보호하는 것은 환자를 직접적으로 관리하는가에 상관없이 자원봉사자를 포함한 전 인력이 공유하는 책임이라는 것을 이해하는 것은 중요하다.

Case #24

친구가 병원에 있는 그의 여자친구를 걱정하고 있다. 그가 당신에게 뭔가 알아낼 수 없느냐고 물어본다.

Q. 친구를 위해서 정보를 찾아봐야 하는가?

A. 답변은 '아니오'이다. 환자가 자신의 정보를 디렉터리에 두는 것을 동의한다면 환자의 위치, 일반적 상황을 알 수 있는 안내 데스크로 친구를 데려간다.

- 업무를 할 때가 아니고는 환자 기밀정보를 찾아낼 수 없다는 것을 명심한다. 환자정보를 사용할 수 있을 때라도 이를 다른 사람에게 알리면 안 된다. 환자정보의 기밀성을 유지하는 것은 단순히 병원 업무의 우선순위가 아니라 법률이다.

Case #25

사무실에 있는 낡은 컴퓨터를 발견하였고, 이것이 더 이상 사용되지 않는다고 확신한다.

Q. 다른 업무 수행에 사용하기 위해 이 컴퓨터를 가져가도 되는가?

A. 가장 좋은 방법은 관리자에게 물어보는 것이다. 인증 받지 않고 시설의 소유물을 제거하는 것은 도난으로 간주되므로, 승인 없이 시설의 외부로 컴퓨터를 가지고 가면 안 된다.

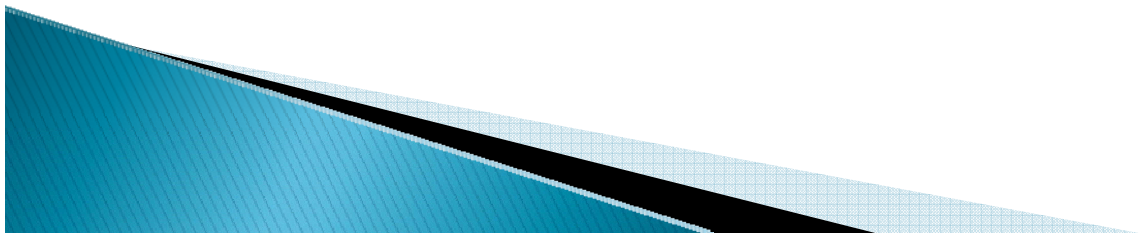
- 하지만, 업무를 위해서 컴퓨터를 사용할 목적을 가지고 있을지라도, 관리자가 이 컴퓨터에 환자정보가 없다는 것을 확인하도록 요구해야 하고, 만약 환자정보가 있다면 적절하게 제거되어야 하도록 요구해야 한다.

Case #26

몇 년간 병원은 병원서비스를 제공하기 위해 환자가 퇴원한 후 우편물을 보냈다. 우편물을 보내는 업체에서 우편물 발송을 위한 환자의 이름과 주소가 포함된 컴퓨터 디스크를 잃어버렸다고 한다. 그들은 이름과 주소 리스트를 전자메일로 보내달라고 한다.

Q. 병원은 이미 환자들에게 우편물을 받을 것이라고 통보한 사실을 알고 있다. 그러므로 요구한 정보를 메일로 보내줄 수 있는가?

A. 아니오. 가장 좋은 생각은 정보를 디스켓으로 오프라인으로 보내는 것이다. 이것을 어떻게 보낼지에 대해 관리자 또는 보안 관리자와 확인해야 한다. 병원은 계약한 운송인이 이를 전달하도록 요구할 것이다.



Case #27

의사가 환자의 집에 전화하여 환자의 아내에게 메시지를 남겼다. “남편의 전립선염 처방을 위해 전화하였고, 약이 언제 준비되는지 약국에 전화하면 알 수 있을 것이라고 전해주십시오”

Q. 의사가 잘못한 것이 있는가?

A. 그렇다. 의사는 전화로 환자의 가족 또는 자동응답기에 메시지를 남기는 것을 주의해야 한다. 환자는 그들에게 메시지를 남기지 않도록 요구할 것이다. 일부 환자는 그들의 PHI를 가족과 공유하는 것을 제한할 것이다. 메시지를 남기는 경우, 정보의 양과 유형을 한정해야 할 것이다. 만약 조직의 정책이 메시지 남기는 것을 허가한다면, 위 시나리오에 있는 메시지는 다음과 같이 더 비밀로 지켜져야 할 것이다. : “약국에 가서 처방약을 가져가라고 남편에게 전해주세요” 하지만 이러한 정보도 기밀 PHI라는 것을 명심해야 한다.

Case #28

두 명의 의사가 엘리베이터에서 환자의 치료에 대해 의논하고 있었다. 대화 중, 환자의 이름을 언급하였다.

Q. 이것은 HIPAA 위반인가? 환자의 프라이버시를 보호하기 위해서 의사들은 어떠한 단계를 거쳐야 하는가?

A. 그렇다. 이것은 HIPAA 위반이다. 의사들은 다른 사람이 있는 엘리베이터에서 이름으로 환자를 확인하면 안 된다. 환자의 이름을 말하지 않더라도, 사람을 확인할 수 있다. 가급적이면, 의사들은 환자에 대한 의논을 엘리베이터와 같은 공공장소에서 하면 안 되고, 대신 비밀스러운 장소에서 대화를 해야 한다. 만약 이것이 실제적이지 못하다면, 의사들은 그들의 목소리를 작게 하여 다른 사람이 들을 수 없도록 해야 한다.

Case #29

최근에 신장결석 환자를 치료하였고, 1차 진료를 했던 의사가 환자의 기록을 팩스로 보내달라고 요청한다. 환자 등록 시스템에 따라 그 의사가 실제 1차 의료제공자임을 확인하였고, 환자의 인증 없이 그의 기록을 팩스로 보내주었다.

Q. 잘못한 것이 있는가?

A. HIPAA의 관점에서는 잘못된 것이 없다. HIPAA 프라이버시 규정은 공급자에게 치료를 목적으로 한 PHI의 공유를 요구하지 않는다.

- 하지만, 가끔 환자는 네트워크상이 아닌 관리 또는 그들의 PCP가 포함되지 않은 관리를 추구한다. 먼저 환자와 함께 확인해야 한다. 그 후, 팩스번호를 여러 번 확인하고, 다른 사람이 환자의 정보를 볼 수 없도록 팩스를 보낸다는 것을 확인해야 한다.

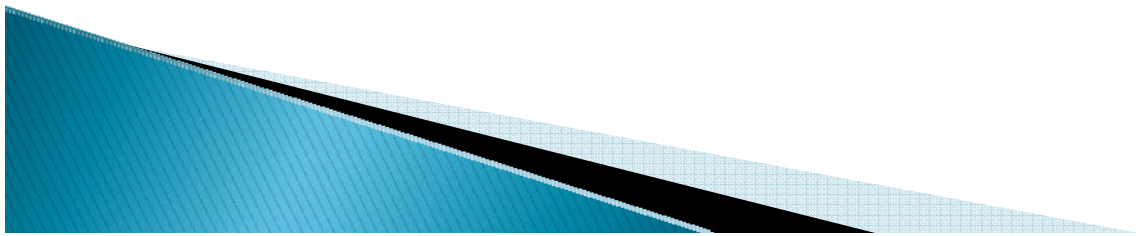
Case #30

병원은 의사에게 병원 컴퓨터 데이터베이스에 접근할 수 있는 패스워드를 만들도록 요구하였다. 의사는 패스워드로 자신의 이름을 사용하였다.

Q. 이것은 용인할 수 있는가?

A. 아니오. 쉽게 추측할 수 없는 패스워드를 선택하는 것이 중요하다.

- 이는 스포츠 팀 이름, 개인 이름, 생년월일을 사용하면 안 된다는 것을 의미한다. 단어, 이름과 같은 일반적 패스워드는 피한다. 대신 시스템이 지원한다면, 문자와 숫자의 조합, 6자리 이상으로 구성, 대문자와 소문자의 조합한 패스워드를 사용한다.

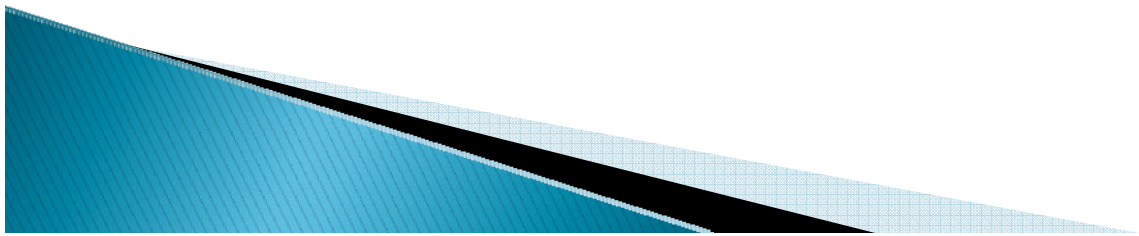


Case #31

의사들이 스케줄과 검사 결과를 확인하기 위해 복도에 있는 컴퓨터를 공유한다. 한 의사가 시스템이 타임아웃 된다는 것을 알고, 로그오프를 하지 않고 자리를 떠났다. 하지만 그 사이에 환자의 정보는 지나가는 사람이 볼 수 있다.

Q. 이것은 용인할 수 있는가?

A. 아니오. 의사는 그 자리를 떠날 때 로그오프 해야 한다. 게다가 프라이버시를 위해 스크린의 위치에 대한 결정을 점검해야 한다. 대안으로 모니터에 있는 정보를 보호하기 위해 스크린커버 또는 필터가 사용되어야 할 것이다.

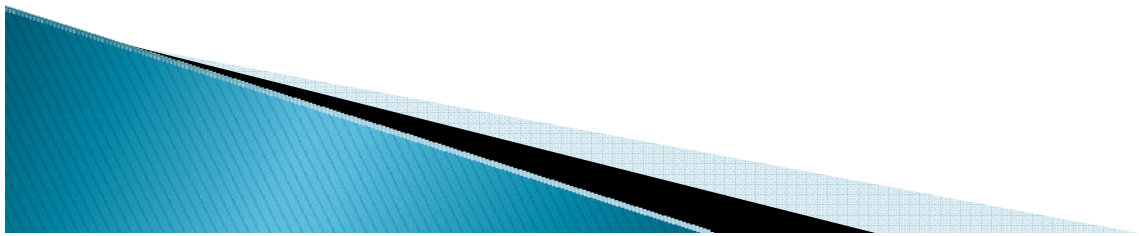


Case #32

의사가 자동차로 이동 중이고, 일부 환자 케이스를 검토하기 위해 노트북을 가지고 간다. 목적지로 가는 동안에 노트북을 옆 좌석에 두었다. 가스 충전을 위해 차를 멈췄고, 창문이 열린 채로 차 밖으로 나가서 커피 한 잔을 사고, 가스비를 지불했다.

Q. 노트북을 안전하게 유지했는가?

A. 아니오. 노트북을 차에 방치해두면 안 된다. 대신, 노트북을 안전을 위해 이것을 가지고 다니거나 트렁크에 넣어 다른 사람이 보지 못하도록 해야 한다. 게다가 노트북은 패스워드로 보호되어야 하고, PHI가 있는 파일도 암호화되어야 한다. 노트북과 이동에 관한 조직의 정책을 확인한다.



Case #33

병원이 의사에게 장기간의 휴가 동안 가져갈 수 있도록 휴대용 컴퓨터를 주었다. 휴가 중 이메일을 확인하기 위해 빌린 컴퓨터에 소프트웨어를 다운받았고, 개인 이메일에 접근하기 위해 집에 있는 컴퓨터에 연결을 하였다.

Q. 잘못한 것이 있는가?

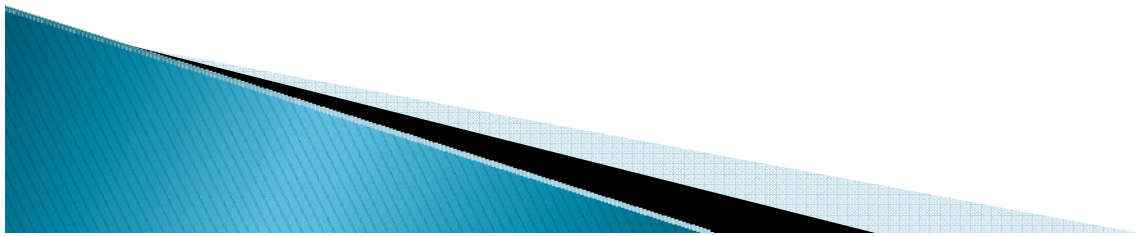
A. **그렇다.** 컴퓨터 바이러스, 보안 위반으로부터 휴대용 컴퓨터를 보호하기 위해, 의사는 컴퓨터를 비즈니스 목적으로만 사용해야 한다. 또한 의사는 인증되지 않은 소프트웨어를 다운로드하고, 병원에서 인증하지 않은 서비스에 연결함으로써 휴대용 컴퓨터를 손상시켰다. 게다가 의사가 병원 네트워크에 컴퓨터를 연결하였다면, 자신도 모르게 네트워크에 바이러스가 확산되거나 인증되지 않은 개체가 제공되었을 것이다. 휴대용 컴퓨터에 관한 정책과 원거리에서 조직이 네트워크에 접근하는 것에 관한 정책을 확인한다.

Case #34

환자기록을 다루는 직원의 컴퓨터 모니터가 접수처로 향해 있고, 환자들이 이를 볼 수 있다. 하지만, 화면 보호기가 매 20분마다 작동한다.

Q. 스크린에 나타나는 환자의 PHI를 보호하기 위해 충분한 조치를 취하고 있는가?

A. 아니오. 직원은 모니터의 방향을 바꿔야 하고, 병원은 작업 구역을 다시 배치하여 환자가 볼 수 없도록 해야 한다. 대안으로 직원은 스크린 커버로 모니터를 가려야 한다.

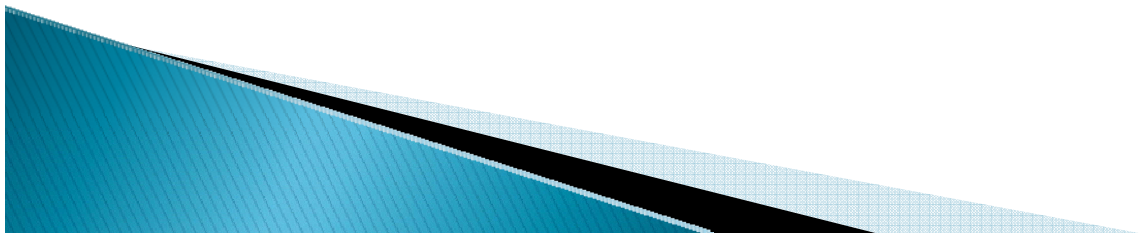


Case #35

모든 컴퓨터는 자동적으로 로그오프 된다. 이는 사용자가 5분간 사용하지 않으면 로그오프 하도록 설정되었다. 근무 중 업무상 5분 이상의 통화를 자주 하기 때문에, 종종 자동적으로 로그오프 된다. 이러한 불편함을 피하기 위해서 로그오프 기능을 억제하였다.

Q. 잘못하였는가?

A. 그렇다. 인증 없이 자동 로그오프 기능을 억제하면 안 된다. 이를 억제하면, 환자의 PHI에 대한 인증되지 않은 접근의 위험을 증가시킨다.

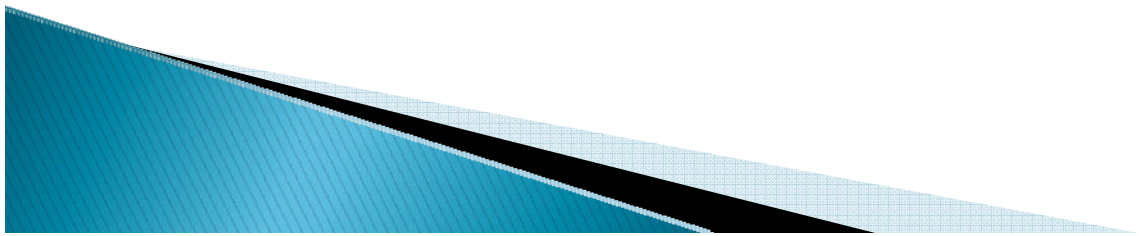


Case #36 – 임상실험

의사가 천식 임상실험을 위해 환자들을 등록하였다. 치료 방법이 마음에 들지 않아 환자는 연구에 참여하지 않겠다는 것을 서면으로 밝혔다. 의사는 부분적으로 완성된 보고서(CRF)를 스폰서에게 제출하였다.

Q. 의사는 무엇을 별도로 해야 하는가?

A. HIPAA는 실험 참가자가 서면으로 취소를 한 후에는 부가적인 PHI 사용 또는 공개를 금지한다. 그러므로 의사는 연구의 완전성을 보존하기 위해 필요한 경우에만 이 보고서를 스폰서에게 보내야 한다.(이것은 일반적으로 단일 센터에서는 발생하지 않지만 다중 센터에서는 종종 발생한다.)

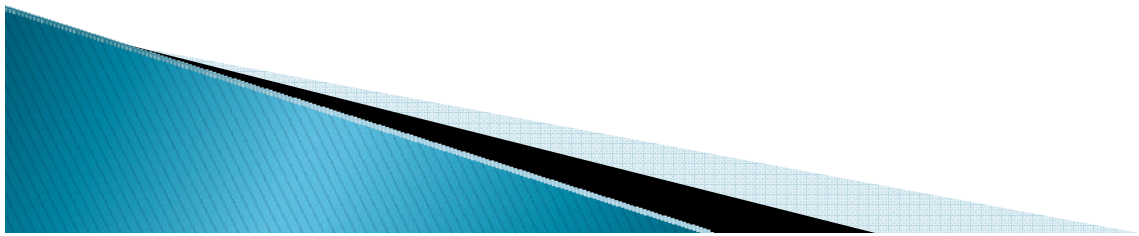


Case #37 – 임상실험

한 의사가 실험에 참가하고 있고, 실험대상자는 병원에서 모집하였다. 추후 정보는 의사의 사무실에서 얻어졌다.

Q. 연구를 위한 PHI를 얻을 때, 서로 다른 두 조직-병원과 사무실-로부터 두 개의 인증을 받아야 하는가?

A. 아니오. 독립적이든 통합적이든 하나의 인증이 두 개체를 포함한다, 하지만, 의사는 HIIPAA의 기록보유 요구사항을 만족하기 위해 사본을 각각 사무실과 병원의 기록실에 두어야 한다.

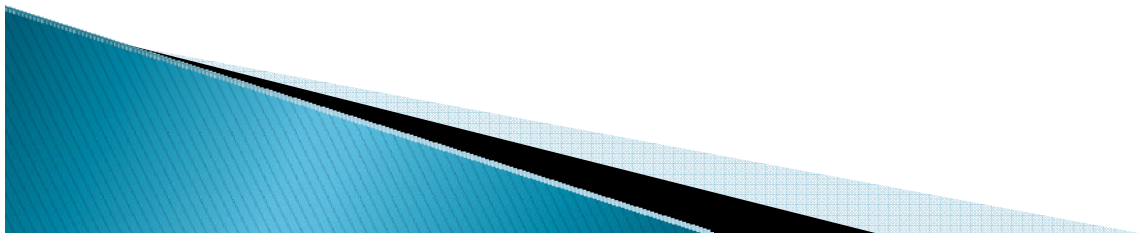


Case #38 – 임상실험

의사는 환자에게 울혈성 심부전 신약에 관한 연구를 수행하고 있다. 이 연구의 임상실험 코디네이터는 병원에서 고용하였다. 이 사람은 연구 전 검토의 일환으로 전날 ICU 입원기록을 검토하며 사전차단을 수행하였다. 임상시험 스폰서인 ABC제약회사의 감독자는 병원을 방문하여 사전차단 된 케이스에 대한 사이트 지불을 결정하기 위해 사전차단 기록 열람을 요구하였다.

Q. 코디네이터는 감독자에게 기록을 보여줄 수 있는가?

A. 아니오. HIPAA는 연구 전 검토가 완료될 때 공개를 허가한다. 감독자 검토는 그들의 목적이 사전차단을 도와주는 경우에만 허가된다.



Case #39 – 임상실험

의사는 울혈성 심부전 환자에 대한 신약 연구를 수행하고 있다. 의사는 실험을 하고 있고, 병원에서 특권을 가지고 있다. 의사는 연구 이전 검토의 일부로 전날 ICU 입원기록을 검토하며 사전차단을 스스로 수행하였다.

Q. 연구에 등록하지 않았지만 환자가 요구하면 병원은 의사가 검토하고 있는 기록의 목록에 있는 환자에게 알려줘야 하는가?

A. **그렇다.** 병원에서 연구를 목적으로 공개를 할 때, 병원은 (비록 의사를 만난 적이 있을지라도) 환자가 요구하면 그들에게 알려줘야 한다. (만약 공개가 50명 이상의 정보에 관련되어 있다면, 어떤 사람의 PHI가 공개되는지에 대한 연구 목록을 만들어야 한다.)