

## 개인정보보호관리규정

제정 : 2012. 1. 1

### 제1장 총칙

제1조(목적) 이 규정은 상지대학교 부속한방병원(이하 “병원”이라 한다)이 처리하는 모든 개인정보가 분실,도난,유출,변조 또는 훼손되지 않도록 안전하고 체계적으로 관리하고 적법하게 함으로써 정보주체의 권리를 보호하기 위하여 필요한 사항을 규정함을 목적으로 한다.

제2조(적용범위)

- ① 병원에서 처리하는 환자정보, 환자보호자 및 대리인의 정보, 교직원 정보, 위탁업체 직원, 수련생 및 실습생 등 모든 개인정보에 적용한다.
- ② 병원의 개인정보를 처리하는 정보시스템, 문서, 기기, 시설물 등 모든 물적 자원에 적용한다.

제3조(용어정의) 이 규정에서 사용되는 용어의 정의는 다음 각 항과 같다.

- ① “개인정보”란 생존하는 개인에 관한 정보로서 해당 정보에 의하여 개인을 식별할 수 있는 정보를 말한다.
- ② “민감정보”란 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활, 유전정보, 범죄경력정보, 그밖의 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보를 말한다.
- ③ “고유식별정보”란 개인의 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호를 말한다.
- ④ “처리”란 개인정보의 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기 및 그 밖에 이와 유사한 일체의 행위를 말한다.
- ⑤ “정보주체”란 처리되는 정보에 의하여 식별되거나 식별될 수 있는 자로서 해당 정보의 주체가 되는 자를 말한다.
- ⑥ “개인정보파일”이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물을 말한다.
- ⑦ “개인정보처리자”란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 타인을 통하여 개인정보를 처리하는 자를 말한다.
- ⑧ “영상정보처리기기”란 일정한 공간에 지속적으로 설치되어 사람 또는 사물의

영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치를 말한다.

제4조(다른규정과과의 관계)

- ① 개인정보보호에 관하여는 다른 규정에 특별히 규정한 경우를 제외하고는 동 규정이 정하는 바에 의한다.
- ② 개인정보보호에 관한 지침을 제·개정하는 경우에는 동 규정에 부합 되도록 한다.

제2장 개인정보보호 조직

제5조(개인정보보호 조직체계)

- ① 개인정보보호와 관련한 정책 및 활동의 원칙, 의사결정 지원 등을 위해 “개인정보보호 위원회”를 둔다.
- ② 개인정보처리에 관한 업무의 총괄 관리를 위하여 “개인정보보호책임자”를 지정한다.
- ③ 개인정보보호책임자의 업무를 보좌하고 개인정보처리에 관한 실무관리 업무를 수행하는 “개인정보보호실무책임자”, “개인정보기술보안실무책임자”, “물리적 보안책임자”를 각각 지정한다.
- ④ 각 부서에서의 개인정보취급을 관리 및 감독하기 위하여 “개인정보취급관리 책임자”를 지정한다.
- ⑤ 병원의 교직원 및 위탁업체관리 직원, 교육생 등 개인정보를 취급하는 모든 사람은 “개인정보 취급자”로 지정한다.

제6조(책임자 지정)

- ① 개인정보보호책임자는 병원장이 지명하고 개인정보보호위원장을 겸한다.
- ② 개인정보보호실무책임자는 원무과장으로 지정하고 원무과를 개인정보보호 주관부서로 지정한다.
- ③ 개인정보기술보안실무책임자는 총무과장으로 지정하고 총무과를 개인정보기술보안 주관부서로 지정한다.
- ④ 물리적 보안책임자는 총무과장으로 지정하고 총무과를 물리적 보안 주관부서로 지정한다.
- ⑤ 각 부서의 장을 개인정보취급관리책임자로 지정한다.

제7조(개인정보보호책임자의 공개)

- ① 병원의 개인정보보호책임자는 홈페이지에 성명과 부서의 명칭,전화번호등 연락처를 공개한다.

- ② 개인정보보호와 관련한 고충 처리 상담을 위하여 담당자 성명, 부서의 명칭, 전화번호 등 연락처를 함께 게재한다.

제8조(개인정보보호책임자의 역할)

① 개인정보보호책임자는 개인정보보호에 관한 활동의 기획, 조정 및 관리등을 위해 다음 각 호의 업무를 수행한다.

- 1.개인정보 보호 계획의 수립 및 시행
- 2.개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
- 3.개인정보 처리와 관련한 불만의 처리 및 피해 구제
- 4.개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
- 5.개인정보 보호 교육계획의 수립 및 시행
- 6.개인정보파일의 보호 및 관리·감독
- 7.개인정보취급자 관리·감독
- 8.개인정보처리에 관한 안전조치 시행
- 9.기타 개인정보보호를 위해 필요한 사항

제9조(개인정보 보호 및 기술보안,물리적 보안 실무책임자의 역할)

① 개인정보 보호실무책임자는 개인정보보호에 관한 관리적 보호 조치 사항을 위해 다음 각 호의 업무를 수행한다.

- 1.개인정보 보호 수집, 이용, 제공, 파기 등 관리 업무
- 2.개인정보에 대한 접근 권한 및 규정 관리 업무
- 3.개인정보를 위한 교육 및 홍보에 관한 업무
- 4.개인정보취급현황 및 취급자 관리 업무
- 5.기타 개인정보 관리적 보호 업무

② 개인정보 기술보안실무책임자는 개인정보보호에 관한 기술적 보호 조치를 위해 다음 각 호의 업무를 수행한다.

- 1.정보시스템의 부당한 접근 및 외부 침입 등을 방지하기 위한 정보시스템의 구축, 관리 업무
- 2.정보의 정확성 및 최신성을 확보하기 위한 시스템 관리 업무
- 3.침해사고 예방, 복구 및 보호 등의 업무
- 4.정보보안에 관한 취급자 관리 정책 및 교육 업무
- 5.기타 개인정보 기술적 보호 조치에 관한 업무

③ 개인정보 물리적 보안실무책임자는 개인정보보호에 관한 물리적 보호조치를 위해 다음 각 호의 업무를 수행한다.

- 1.건물 전반적인 물리적 보안 정책의 수립 및 관리 업무
- 2.영상처리기기 설치 및 관리 업무
- 3.인적, 물적 동선관리 및 통신 보안관리 업무

4.기타 물리적 보호 조치에 관한 업무

제10조(개인정보취급관리책임자 및 개인정보취급자의 역할)

①개인정보취급관리책임자는 다음 각 호의 업무를 수행한다.

- 1.해당 부서의 개인정보 취급 현황 파악 및 정보자산 분류 및 관리 업무
- 2.해당 부서의 직원 및 위탁업체 직원 등의 모든 개인정보취급자의 업무에 따른 개인정보 보호 책임의 할당 및 관리·감독 업무
- 3.해당 부서의 개인정보보호 활동 관리 업무
- 4.기타 개인정보보호와 관련하여 위임 받은 업무

② 개인정보취급자는 다음 각 호의 업무를 수행한다.

- 1.개인정보보호관리규정 및 지침의 숙지 및 준수
- 2.개인정보보호 활동 및 교육 참여
- 3.보안서약서의 작성
- 4.개인정보 유출 및 보안사고 발생 시 신고 및 대응
- 5.기타 개인정보보호에 관하여 필요한 사항

**제3장 업무 위탁 및 외부자 보안관리**

제11조(업무위탁의 공개 및 고지)

- ① 개인정보보호책임자는 개인정보의 처리 업무를 위탁하는 경우에는 홈페이지에 공지하여야 하며, 병원 서비스 홍보 및 판매를 권유하는 업무를 위탁하는 경우는 정보주체에게 개인정보보호법시행령 31조에 따라 알려야 한다.
- ② 개인정보취급관리책임자는 개인정보의 처리업무를 위탁하는 경우, 개인정보보호책임자에게 보고하고 “개인정보업무 위탁업체 관리지침”에 따른다.
- ③ 업무위탁을 받은 수탁자는 개인정보의 처리현황, 개인정보파일 접근대 상자 및 접속현황 등을 기록하고 관리하여야 한다.

제12조(업무위탁 계약관리 및 개인정보보호 요구사항)

- ① 병원이 개인정보 처리 업무를 위탁하거나 용역업체와 계약하는 경우, 개인정보보호 요구사항 등이 포함된 “개인정보업무 위탁업체 관리지침”에 따른다.
- ② 개인정보 처리 업무 위탁 계약 담당자는 수탁자의 처리 업무의 지연, 처리 업무와 관련 없는 불필요한 개인정보의 요구, 처리기준의 불공정등의 문제점을 종합적으로 검토하여 이를 방지하기 위하여 필요한 조치를 마련하여야 한다.
- ③ 개인정보의 처리 업무를 위탁할 업체를 선정할 때에는 인력과 물적시설, 재정 부담능력, 기술 보유의 정도, 책임능력 등을 고려하여야 한다.

제13조(업무위탁 계약관리 및 용역업체 직원 등 관리)

- ① 업무위탁 및 용역업체 직원으로서 병원의 개인정보 처리를 하는 자는 병원의 “보안서약서”에 서명하여야 한다.
- ② 개인정보취급관리책임자는 업무위탁업체, 용역업체 직원 등에 대한 개인정보 처리실태점검 및 관리,감독을 하여야 한다.
- ③ 개인정보취급관리책임자는 업무위탁업체, 용역업체와의 계약 체결 시 해당 업무에 따라 접근하는 병원의 정보자산 및 개인정보 취급 현황에 대하여 개인정보보호책임자에게 보고 하여야 한다.
- ④ 개인정보보호책임자는 개인정보취급관리책임자가 위탁업체 및 용역업체 등의 관리·감독에 대한 현황을 년 1회 이상 점검하여야 한다.

제14조(외부자 보안 관리)

- ① 업무상 필요에 의해 일시적으로 병원의 개인정보를 처리하는 경우는 개인정보보호실무책임자의 사전 승인이 있어야 하며, 이 경우 개인정보 취급자로서의 책임과 의무를 다하여야 한다.
- ② 개인정보보호실무책임자는 외부자에 대해 “보안서약서”를 작성하도록 하여야 하며, 개인정보보호에 관한 관리·감독한다.

**제4장 개인정보보호 교육 및 인적자원의 관리**

제15조(교육계획의 수립 및 시행)

- ① 개인정보보호책임자는 병원의 정보보호에 대한 인식제고 및 실제 업무 중의 실수, 오용을 예방하기 위한 개인정보보호 교육계획을 수립하여 년 1회 이상 실시하여야 한다.
- ② 개인정보보호 교육의 실시는 전 교직원을 대상으로 하며, 외부 협력업체 등의 관련 외부자를 포함할 수 있다.

제16조(교육 및 훈련 내용)

- ① 교육은 대상자의 직위 및 담당하는 업무의 특성에 따라 구분하여 실시하여야 한다.
- ② 교육은 관련 규정 및 지침을 포함하여 대상자가 담당하는 업무의 특성에 따른 정보보호관련 내용을 포함하여야 한다.
- ③ 개인정보보호실무책임자는 전 교직원 및 외부 위탁업체 직원 등의 정보보호 생활화 및 인식제고를 위해 그룹웨어의 전자게시판, 정기간행물 등을 이용하여 정보보호에 대한 지속적인 교육 및 홍보를 실시하여야 한다.

제17조(교육결과 등에 대한 문서화)

- ① 개인정보보호실무책임자는 교육계획서 및 결과보고서를 작성하여 개인정보 보호책임자에게 보고하여야 한다.
- ② 개인정보보호실무책임자는 교육계획서 및 교육결과 보고서를 보관 및 관리하여야 한다.

제18조(교직원채용 및 인사이동시의 적격심사)

- ① 인사담당자는 병원의 교직원 및 계약직 직원 등의 채용 시 개인정보 취급에 따른 적격여부를 심사하여야 한다.
- ② 인사담당자는 인사이동을 포함하여 민감한 정보를 취급하거나 정보시스템에 접근권한을 가지고 직무를 수행하는 담당자는 강화된 방법으로 적격심사를 하여야 한다.

제19조(개인정보보안서약서의 징구)

- ① 인사담당자는 병원의 전 교직원의 신규채용, 퇴직, 인사이동에 따른 개인정보 취급 시 “개인정보보안서약서”를 받아야 하며, 개인정보보안서약서 징구 책임 및 절차 등은 “개인정보보안서약서 작성 및 관리 지침”에 따른다.
- ② 위탁업체 및 용역업체 직원 등 외부자로서 개인정보를 취급하는 자도 “개인정보보안서약서”를 받아야 한다.
- ③ 개인정보보호서약서의 내용 수정 및 신규서약서 개발은 개인정보보호위원회에서 승인을 받아야 한다.
- ④ 개인정보취급관리책임자는 작성된 개인정보보호서약서를 보관·관리한다.

제20조(준수관리 및 징계)

- ① 병원의 교직원 및 위탁업체 직원 등 개인정보취급자는 불법적 개인정보처리 및 개인정보보호법 등 관련 법령 등의 미준수로 인하여 민사상 또는 형사상의 법적문제를 야기 시키지 않도록 법적 요구사항을 준수해야 한다.
- ② 병원의 교직원 및 위탁업체 직원 등 개인정보취급자는 병원의 개인정보보호를 위한 관련 규정 및 지침 등을 숙지하고 이를 준수하여야 한다.
- ③ 병원은 개인정보보호법 등 관련 법령 및 병원내 규정 등을 위반하여 심각한 보안사고를 일으키거나 병원 이미지 및 경영상의 심각한 위해를 초래한 개인정보처리자에 대하여는 개인정보보호위원회 승인을 득한 후 징계위원회에 상정하여 징계처리를 할 수 있다. 특히, 심각한 보안사고를 일으켰다고 의심되는 개인정보처리자에 대해서는 개인정보보호위원회를 경유하여 경찰, 검찰 등 관련기관에 고발조치를 할 수 있다.

제5장 개인정보 수집,이용,제공 등

제21조(개인정보 수집,이용,제공 원칙)

- ① 병원의 업무를 목적으로 처리되는 개인정보는 개인정보보호법 제15조~20조에 의거하여 동 규정에서 명시한 경우를 제외하고는 개인정보를 임의로 수집, 이용 및 제공할 수 없다. 단, 개인정보보호위원회에서 심의 후 의결 받은 경우는 그러하지 아니하다.
- ② 병원이 처리하고자 하는 개인정보가 수집, 이용, 제공 등에 대하여 정보주체의 동의를 받아야 하는 경우 개인정보보호법 등의 요구사항에 의거 하여야 한다.
- ③ 병원이 처리하고자 하는 개인정보가 민감정보 및 고유식별정보로서 다른 법률에 특별한 규정이 없는 경우는 정보주체의 개별 동의를 받아야 한다.
- ④ 개인정보취급관리책임자는 수집, 이용, 제공한 개인정보 처리현황에 대하여 문서로 관리하여야 하며, 개인정보처리현황을 정보주체가 요구하는 경우 이에 응할 수 있도록 관리되어야 한다.
- ⑤ 개인정보취급관리책임자는 수집, 이용, 제공하고 있는 개인정보에 대해 개인정보보호위원회에 보고하여 처리 가능성 여부에 대한 심의를 거쳐 적법하게 처리하여야 한다.
- ⑥ 개인정보보호책임자는 개인정보취급관리책임자로부터 보고 받은 개인정보 수집,이용 제공 등 처리항목이 정보주체의 별도 동의가 필요한 경우 동의서를 제정 및 개정하여 적법하게 처리될 수 있도록 조치를 취하여야 한다.
- ⑦ 개인정보보호책임자는 개인정보의 수집, 이용, 제공 시 안전하게 관리될 수 있도록 필요한 관리적, 기술적, 물리적 보호조치를 강구하여야 한다.

제22조(개인정보 수집,이용,제공의 범위 및 방법)

- ① 진료를 위하여 수집, 이용, 제공하는 환자의 개인정보는 의료법, 의료법 시행규칙 등 관련 법률에 특히 규정된 경우를 제외하고는 정보주체의 동의를 받으며, 이용 및 제공 등에 관련한 사항은 “의무기록관리규정”에 따른다.
- ② 병원에서 채용한 교직원, 위탁업체 직원 등의 인사정보 중 근로기준법 등에 명시되어 있지 않은 개인정보 및 민감정보 등은 정보주체의 동의를 받은 후 개인정보를 수집하고, 수집하는 개인정보의 항목 등은 개인정보보호위원회에서 정한다.
- ③ 홈페이지 운영을 위하여 수집하는 개인정보는 정보주체의 동의를 받은 후 수집하고, 수집하는 개인정보의 항목 등은 “병원홈페이지 운영 지침”에 따른다.

제23조(개인정보의 보관 및 파기)

- ① 진료를 위하여 생성된 의무기록은 의료법에 따른 법적 보관연한까지 안전하게 보관 및 관리하며, 법적 보관연한이 경과되어도 정보주체의 동의를 득한 경

- 우 영구 보존할 수 있으며, 파기 시에는 “의무기록파기관리지침”에 따른다.
- ② 인사 정보 및 환자 이외의 외부자 등의 개인정보 보관연한은 동의서 획득 시 기재한 연한동안 안전하게 보관하며, 보관연한이 경과한 개인정보는 “개인정보파기관리지침”에 따른다.
  - ③ 개인정보취급자는 보존의무가 없는 개인정보의 이용 목적이 달성되어 그 개인 정보가 불필요하게 되었을 때에는 5일 이내에 그 개인정보를 파기 하여야 한다.
  - ④ 개인정보 파기시에는 파기관리대장을 작성하여야 하며 파기관리대장의 작성 방법 등은 “개인정보파기관리지침”에 따른다.
  - ⑤ 개인정보를 파기할 때에는 복구 또는 재생되지 않도록 조치한다.

## 제6장 정보주체의 권리보호 조치

### 제24조(동의 및 동의서 관리)

- ① 개인정보의 수집, 이용, 제공 등의 처리 시 법령에 의하여 동의를 받지않고 처리할 수 있는 경우를 제외하고는 정보주체의 동의를 받는다.
- ② 동의서의 내용 및 형식은 개인정보보호위원회에서 심의, 의결한다.
- ③ 만14세 미만의 아동은 법정대리인의 동의를 받아야 한다.
- ④ 만14세 미만의 아동이 진료를 받는 경우, 법정대리인의 동의 없이 진료를 우선 시행하고 진료 이외의 개별동이가 필요한 항목에 대한 동의를 받고자 하는 경우는 가능한 3일 이내에 법정대리인의 동의를 받아야 하며 이에 대한 관리는 원무과에 한다.
- ⑤ 동의서 관리 및 절차는 “동의서 지침”에 따른다.

### 제25조(정정 요청 및 처리)

- ① 정보주체 및 대리인(이하 “정보주체 등”)은 명백한 개인정보의 오류를 확인한 경우와 의무기록 내용 중 정보주체 등의 진술한 내용이 다르게 기재된 경우에 한해 정정을 요청할 수 있다.
- ② 의무기록 내용에 대한 정정 요청은 원무과에서 관리하며, 이 경우 “의무 기록 정정지침”에 따라 처리한다.
- ③ 의무기록 내용 이외의 명백한 개인정보의 오류에 대한 정정 요청은 총무과에서 관리하며, 이 경우 오류 사항을 입증할 수 있는 증빙서류를 확인하여 정정한다.
- ④ 정정처리 담당자는 정보주체 등이 요청에 의한 정정한 내용이 병원에서처리 되는 다른 파일 및 항목에서 이용되는지를 확인하여 동일한 내용이 기록되어

있는 경우 해당 내용을 같이 정정하여 정보가 일관성 있게 관리 한다.

- ⑤ 정정처리 담당자는 접수된 내용의 심의 결과를 신청자에게 서면으로 통보한다.

제26조(삭제 요청 및 처리)

- ① 정보주체 등은 의료법에 따라 보존되어야 하는 의무기록을 제외한 개인정보에 대해서는 삭제 요청을 할 수 있다.
- ② 제1항에 따른 삭제 요청 접수 및 처리 결과 통보는 총무과에서 관리한다.
- ③ 의료법에 따른 보존기간이 경과한 의무기록에 대한 삭제 요청에 대해서는 “의무기록 정정지침”에 따라 처리한다.

제27조(열람 및 사본발급 요청 및 처리)

- ① 정보주체 등은 해당 정보주체의 개인정보에 대하여 열람요청을 할 수 있으며, 담당자는 10일 이내에 열람요청에 응하여야 한다.
- ② 정보주체의 열람 요청에 응할 수 없는 정당한 사유가 있으면 열람은 열람을 연기하거나 거절할 수 있으며, 이 경우 담당자는 그 사유를 정보주체 등에게 알린다.
- ③ 정보주체 등이 열람 및 사본발급 하고자 하는 정보가 의무기록인 경우는 “의무기록 열람 및 사본발급 지침”에 따라 처리한다.

제28조(동의, 동의철회, 정정 및 열람 등의 이력관리)

- ① 개인정보보호실무책임자는 동의, 동의철회, 정정, 열람 등의 처리내역을 5년간 보관 관리한다.
- ② 개인정보보호실무책임자는 정보주체 등이 처리내역의 공개를 요청할 경우 그 내역을 제공한다.
- ③ 개인정보보호실무책임자는 해당 정보의 취급관리책임자에게 제1항에 따른 이력관리내역을 요청할 수 있으며, 요청을 받은 취급관리책임자는 이에 응하여야 한다.

제29조(개인정보의 유출통지)

- ① 개인정보보호책임자는 다음의 유출 사고가 발생한 경우 정보주체에게 5일 이내에 유출 사실을 알려야 한다.
  - 1.개인정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터 등을 분실하거나 도난당한 경우
  - 2.개인정보가 저장된 데이터베이스 등 개인정보처리시스템에 정상적인 권한이 없는 자가 접근한 경우
  - 3.개인정보처리자의 고의 또는 과실로 인해 개인정보가 포함된 파일 또는 종이 문서, 기타 저장매체가 권한이 없는 자에게 잘못 전달된 경우
  - 4.기타 권한이 없는 자에게 개인정보가 전달되거나 개인정보처리시스템 등에

접근 가능하게 된 경우

- ② 개인정보 유출 통지 항목 및 방법 등은 별도의 “개인정보유출통지지침”에 따른다.

### 제7장 개인정보처리 방침

#### 제30조(수립 및 공개)

- ① 개인정보보호위원회는 다음 각 호의 사항이 포함된 개인정보의 처리방침을 수립한다.
  - 1.개인정보의 처리 목적
  - 2.개인정보의 처리 및 보유 기간
  - 3.개인정보의 제3자 제공에 관한 사항
  - 4.개인정보처리의 위탁에 관한 사항
  - 5.정보주체의 권리·의무 및 그 행사방법에 관한 사항
  - 6.기타 개인정보의 처리에 관한 사항
- ② 개인정보보호책임자는 개인정보처리방침을 수립하거나 변경하는 경우에는 홈페이지 첫 화면 등에 정보주체가 쉽게 확인할 수 있도록 공개한다.

### 제8장 개인정보의 안전관리 조치

#### 제31조(개인정보의 안전성 확보)

- ① 개인정보처리자는 개인정보보호법 제29조에 따라 다음 각 호의 안전성 확보 조치를 하여야 한다.
  - 1.개인정보에 대한 접근 통제 및 접근 권한의 제한 조치
  - 2.개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치
  - 3.개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치
  - 4.개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치등 물리적 조치
- ② 제1항의 조치를 위한 지침은 병원장이 따로 정한다.

#### 제32조(영상정보처리기기의 설치 및 운영)

- ① 병원은 다음의 경우에 한하여 영상정보처리기기를 설치, 운영한다.

1. 법령에서 구체적으로 허용한 경우
  2. 범죄의 예방과 환자, 내원객, 교직원 등의 신체적 안전을 위한 경우
  3. 시설 안전 및 화재예방 등을 위하여 필요한 경우
- ② 영상정보처리기기의 설치 및 운영·관리에 관한 방침은 개인정보보호위원회에서 심의,의결하여 정한다.
- ③ 영상정보처리기기관리책임자는 개인정보보호책임자가 지명한다.

## 제9장 보안사고 관리

제33조(보안사고의 범위)병원은 다음의 경우를 보안사고로 정의하여 대응한다.

- ① 정보시스템 가동 및 서비스 중단
- ② 악성코드 유포
- ③ 정보시스템의 오용으로 인한 병원 시스템의 심각한 영향을 초래한 경우
- ④ 개인건강정보를 포함한 개인정보가 대량 유출된 경우

제34조(보안사고 발생 시 절차 및 조치)보안사고 발생 시는 다음과 같은 처리절차에 따른다.

- ① 개인정보처리자가 업무 수행 시 보안 침해사고를 탐지하였을 경우, 즉시개인 정보취급관리자에게 신고하고 보안담당자는 신고 접수 후 관련 책임자에게 보고한다.
- ② 보고 받은 관련 책임자는 사고원인을 파악하고 조치하며, 중대사안인 경우는 병원장에게 보고한다.

제35조(보안사고 관리)

- ① 개인정보처리자는 로그를 주기적으로 분석하여 비정상적인 행위나 징후가 파악되면 시스템을 점검하고 즉시 개인정보취급관리자에게 결과를 보고한다.
- ② 보안담당자는 보안사고 발생시 사고일시,내용,조치사항 등을 문서로 관리하며, 년 단위로 분석하여 개인정보보호위원회에 보고한다.
- ③ 보안담당자는 보안사고 재발 방지를 위하여 전 교직원에게 사고경위 및 조치사항 등을 공지한다.

## 부 칙

이 규정은 2012년 1월 1일부터 시행한다.