개인정보 보호 및 보안 규정

관리번호	W-12.4	**제정일**	2013년 02월 15일
승인책임자	병원장	**최근개정일**	2016년 10월 31일
검토책임자	규정관리위원장	**시행일**	2016년 12월 01일
주무부서	원무과, 전산팀, 심사과	**검토주기**	3년
관련근거	의료기관인증기준12.4	**검토예정일**	2019년 10월 30일

Ⅰ. 목적

진료 및 그 외 모든 업무 처리 과정에서 얻어진 개인정보가 훼손, 멸실, 변경, 위조, 유출되지 않도록 하기 위해 필요한 개인정보 보호 및 보안에 관한 구체적인 사항을 정함을 목적으로 한다.

Ⅱ. 적용범위

1. 이 규정은 병원에서 처리하는 환자 정보, 환자 보호자 및 대리인의 정보, 직원 정보 등 모든 개인정보에 적용한다.
2. 병원의 모든 직원과 병원에서 처리하는 개인정보를 취급하는 위탁업체 직원, 실습생 등 병원의 개인정보를 취급하는 모든 자들에게 적용한다.
3. 병원의 개인정보를 처리하는 정보시스템, 문서, 기기, 시설물 등 모든 물적 자원에 적용한다.

Ⅲ. 정의

1. '개인정보' 라 함은 생존하는 개인에 관한 정보로서 성명/주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호/문자/음성/음향 및 영상 등의 정보(해당 정보만으로 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말한다.
2. '정보주체' 라 함은 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
3. '개인정보보호 책임자'라 함은 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지거나 업무처리를 최종적으로 결정하는 자를 말한다.
4. '개인정보 실무담당자'라 함은 개인정보보호 책임자를 보좌하여 개인정보보호·보안 업무에 대한 실무를 총괄하고 관리하는 자를 말한다.
5. '개인정보처리자'라 함은 사업장 내에서 컴퓨터를 이용하여 개인정보자료를 추출·가공 하고 이를 입·출력하는 업무의 담당자 또는 시스템 관리자를 말한다.
6. '개인정보취급자'라 함은 사업장 내에서 고객의 개인정보를 수집, 보관, 처리, 이용, 제공, 관리 또는 파기 등의 업무를 하는 자를 말한다.
7. '개인정보처리시스템'이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스 시스템을 말한다.

Ⅳ. 정책

1. 모든 직원 및 위탁업체 직원, 실습생은 개인정보 보호 및 보안규정을 준수하고 개인정보 보호 및 보안서약서를 작성한다.[별첨 1]

2. 개인정보보호 및 보안에 관하여는 관계 법령, 정관에 특별히 정한 것을 제외하고는 이 정책이 정하는 바에 의하며 다음에 적용한다.
   1) 개인정보 취급관리 및 책임
   2) 개인정보보호 정책 및 관련 법률과의 부합성
   3) 교육 · 훈련 지침
   4) 개인정보보호 및 보안 감사
   5) 개인정보 외부위탁관리 지침
   6) 정보자산관리 지침
   7) 물리적 보안 지침
   8) 시스템개발 보안지침
   9) 접근통제관리 지침
   10) PC 및 개인용 휴대 단말기 관리 지침
   11) 전산운영관리 지침
   12) 침해사고관리 지침

Ⅴ. 절차

1. 개인정보 취급관리 및 책임
   1) 개인건강정보 수집, 이용 및 제공
      (1) 병원에 내원한 환자의 개인건강정보 수집 및 이용을 위하여 '개인정보 수집 및 이용 동의서'를 받는다.
      (2) 병원은 정보주체 또는 대리인의 동의가 있는 경우, 동의한 목적 내에서 개인건강정보를 이용하거나 제공할 수 있다.
      (3) 병원은 정보주체 또는 대리인의 동의가 있다 해도 제3자의 생명, 신체, 재산 및 기타 권리 이익을 해칠 우려가 있는 경우, 병원의 적정한 업무수행에 명백한 지장을 끼칠 우려가 있는 경우, 다른 법령에 위반하는 경우에는 개인건강정보의 전부 또는 일부에 대하여 이용을 거부할 수 있다.
      (4) 환자의 개인건강정보 제공 시 주민등록번호, 전화번호 등, 식별이 가능한 정보는 제공하지 않는다.
   2) 관련부서 운용 및 책임자 지정
      (1) 개인정보를 보호하고 관련 정책 심의 등 정보보호 활동을 총괄 및 관리하기 위하여 개인정보 보호 위원회 내의 개인정보 보호 인력을 구성한다.
      (2) 정보보호 및 보안업무를 관리하기 위하여 각 부서별 실무담당자를 지정하여 해당 업무를 수행한다.(Ⅵ장 참조)
2. 개인정보보호 정책 및 관련 법률과의 부합성
   1) 개인정보 보호책임자는 윌스기념병원의 개인정보 보호를 위한 전반적인 사항을 포함하여 내부관리계획을 수립한다.[별첨 2]
   2) 개인정보 보호책임자는 개인정보 보호를 위한 내부관리계획의 수립 시 개인정보 보호와 관련한 법령 및 관련 규정, 개인정보보호 가이드라인(의료기관 편, 2015년 4월) 을 준수하도록 내부관리계획을 수립한다.
   3) 개인정보 보호책임자는 개인정보 보호담당자가 수립한 내부관리계획의 타당성을 검토하여 개인정보 보호를 위한 내부관리계획을 수립한다.

4) 개인정보 보호담당자는 개인정보 보호 관련 법령의 제·개정 사항 등을 반영하기 위하여 연 1회 개인정보보호 및 보안 규정, 지침, 내부관리계획의 타당성과 개정 필요성을 검토한다.
5) 개인정보보호 실무담당자는 모든 항목의 타당성을 검토한 후 개정할 필요가 있다고 판단되는 경우 개인정보보호 및 보안 규정은 개인정보보호위원회 승인을 위해 보고하여 검토를 요청하며 내부관리계획은 개정안을 작성하여 개인정보보호 책임자에게 보고하고 결재를 득한 후 직원에게 공표한다.

3. 교육 · 훈련 지침
1) 개인정보 보호책임자는 정보주체 정보보호에 대한 직원들의 인식제고를 위해 노력해야 하며, 개인정보의 오·남용 또는 유출 등을 적극 예방하기 위해 임·직원을 대상으로 매년 정기적으로 연2회 이상의 개인정보 보호 교육을 실시한다.
2) 같은 목적으로 신규직원 대상으로 입사 시 1회 [W-9.2 직원교육관리규정 참조] 개인정보 보호 교육을 실시한다.
3) 교육 방법은 집체 교육뿐만 아니라, 인터넷 교육, 전단지 교육 등 다양한 방법을 활용하여 실시하고, 필요한 경우 외부 전문기관이나 전문요원에 위탁하여 교육을 실시한다.
4) 개인정보 보호에 대한 중요한 전파 사례가 있거나 개인정보 보호 업무와 관련하여 변경된 사항이 있는 경우, 개인정보 보호책임자는 부서 회의 등을 통해 수시 교육을 실시할 수 있다.
5) 개인정보보호 실무담당자는 교육계획서 및 교육결과보고서를 작성하여 개인정보보호 책임자에게 보고하여 보관 및 관리한다.

4. 개인정보 보호 및 보안 감사
1) 개인정보보호 및 보안 감사
(1) 개인정보보호 및 보안 감사는 개인정보보호와 보안 관리체계의 적합성 및 운용상황 등의 점검을 통해 실시하며, 개인정보보호와 보안에 대한 안전성 및 신뢰성을 확보 한다.
(2) 각 PC 백신프로그램 자동업데이트는 매일 업데이트 되도록 설정하며 매주 금요일 자동 업데이트 설정 확인 하도록 원내 메신저를 통하여 공지하며 전체점검은 분기별로 한다.
(3) 각 PC DLP 프로그램은 매월 자체 감사하며 점검 결과를 개인정보보호 책임자에게 보고한다.
(4) 통신 점검은 보안실무담당자가 매월 위탁업체에서 보고서 받아 점검 결과를 개인정보보호 책임자에게 보고한다.
(5) EMR 시스템 점검은 보안실무담당자가 분기별로 위탁업체에서 보고서 받아 점검 결과를 개인정보보호 책임자에게 보고한다.
(6) PACS 시스템 점검은 보안실무담당자가 분기별로 위탁업체에서 보고서 받아 점검 결과를 개인정보보호 책임자에게 보고한다.
(7) 개인정보보호 실무담당자 또는 보안실무 담당자는 규정 위반 사례의 사안에 따라 개인정보보호위원회에 보고하여 징계를 요청할 수 있다.

2) 규정 위반 시 징계
(1) 모든 직원 및 위탁업체 직원이 개인정보보호 및 보안 규정 위반 사례를 인지한 경우 개인정보보호 실무담당자 또는 보안 실무담당자에게 보고한다.
(2) 보고를 받은 개인정보보호 실무책임자 또는 보안실무 담당자는 규정 위반 사례에 따라 담당자를 지정하여 규정 위반 사례를 조사하고 개인정보보호위원회에 보고하며 병원 인사위원회에 상정하고 병원 인사규정에 따라 제재조치를 취한다.
(3) 불법적인 사용으로 인해 발생한 문제에 대한 법적 책임은 불법 사용자 자신에게 있다. 불

법 사용자라 함은 다음과 같다.

① 본인에게 부여된 접근 권한을 위배한 자.

② 접근이 허락되지 않은 환자의 의무기록 및 의료정보를 조회, 변조, 훼손시킨 자.

③ 업무권한 범위내서라도 업무이외의 용도로 환자의 의무기록 및 의료정보에 접근하여 그 내용을 탐지한 자.

5. 개인정보 외부위탁관리 지침

1) 개인정보 처리업무 위탁은 문서[별첨 3]에 의해야 하며 아래와 같은 내용을 포함한 “개인정보처리 위탁 특수조건”을 계약서에 첨부 하도록 한다.

(1) 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항.

(2) 개인정보의 기술적·관리적 보호조치에 관한 사항.

(3) 위탁업무의 목적 및 범위.

(4) 재 위탁 제한에 관한 사항.

(5) 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항.

(6) 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항.

(7) 개인정보보호법 제26조제2항에 따른 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항.

2) 개인정보 처리업무를 위탁하는 경우에는 위탁에 관한 사항을 ‘개인정보처리 방침’에 포함하며 정보주체가 언제든지 쉽게 확인가능 하도록 위탁업무내용과 수탁자를 인터넷 홈페이지에 공개하도록 한다.

3) 개인정보 위탁업체에 대한 관리 및 감독은 위탁관리 부서에서 연 1회 이상 점검하며 관련 서류나 보고서등을 보안실무 담당자에게 제출하며 보안실무 담당자는 개인정보보호 책임자에게 보고 후 관리한다.

6. 정보자산관리 지침

정보자산이란 병원에서 의료 및 일반 업무로 인하여 발생되어 보관, 관리되는 모든 정보를 말하며 보안 및 관리대상이 된다.

1) 환자 및 직원에 관련한 인적 정보

2) 환자의 진료기록

3) 업무상 발생한 문서파일

4) CCTV 기록자료

5) 전산기록 등

7. 물리적 보안 지침

1) 보안실무 담당자는 서버실, 의무기록보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다.

2) 서버실에는 보안실무 담당자가 출입을 허가한 직원 및 외부업체만이 전산실 직원과 동행할 수 있다. 서버실 출입 시에는 허가된 직원의 지문 인식 장치로 서버실 입·출입 로그를 저장하며 등록되지 않은 자는 출입을 할 수 없다. 출입을 허가한 직원 및 외부업체는 출입증 명패를 착용한다.

3) 보안실무 담당자는 통제구역의 물리적 출입통제 권한 및 불필요한 출입권한을 매년 1회 이상 검토한 후 개인정보보호 책임자에게 보고한다.[별첨 4]

4) 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.

5) 개인정보처리자는 물리적 접근방지를 위한 별도의 보호시설에 출입하거나 개인정보를 열람하는 경우, 그 출입자에 대한 출입사실 및 열람 내용에 관한 관리대장을 작성하도록 하여야 한다.

8. 시스템 개발 보안지침
   1) 정보시스템 개발 시 분석, 설계, 구현, 시험 단계별 필요한 정보보안 활동을 수행하도록 한다.
   2) 정보시스템 의무기록의 생성, 수정, 삭제에 관한 발생 일시, 처리자, 원본 등을 저장하고 이전 정보가 손상되지 않도록 이력 관리를 하여야 한다.
   3) 인가되지 않은 사람의 프로그램 소스 및 라이브러리에 대한 접근은 통제 되어야하며 프로그램 수정 및 배포에 관한 상세 이력관리를 한다.
9. 접근통제관리 지침
   1) 정보시스템 접근통제
      (1) 방화벽 또는 침입방지 시스템 설치
         ① 인터넷망과 접속 시 방화벽 및 침입방지 시스템을 통해 접근통제를 수행하며, 필요시 침입탐지 시스템 등을 활용하여 접근을 모니터링 한다.
         ② 인가된 사용자만이 네트워크에 접근할 수 있도록 접근통제를 실시하고 업무상 불필요한 인터넷사이트를 차단한다.
         ③ 원칙적으로 인터넷 등 외부 망을 통해 내부 시스템을 관리하는 것을 금지하고 있으며, 부득이하게 접근하기 위해서는 보안실무 담당자에게 요청하고 개인정보보호 책임자에게 승인 후 접근을 허가한다.
      (2) 보안 프로그램 설치 및 운영 등
         ① 보안실무 담당자는 바이러스 등의 악성 소프트웨어로부터 정보시스템을 보호하기 위해 악성소프트웨어를 탐지, 대응하는 프로그램을 관리한다.
         ② 단말기의 악성 소프트웨어의 침투 여부 점검 및 치료를 위하여 백신 소프트웨어를 설치한다.
         ③ 단말기의 보안업데이트가 자동으로 실행되도록 설정한다.
   2) 정보시스템 접근권한
      (1) 보안실무 담당자는 서버의 보안 관리를 위해 직무분리 및 접근 권한 통제 등을 위한 담당자 지정, 책임 및 절차 등을 포함한 정책을 수립하고 시행한다.
         ① 정보시스템에 대한 접근자 계정은 매년 1회 이상 점검하여 비활동성 계정 추출 및 권한의 적절성 여부 검토 등의 계정보호 조치를 수행한다.
         ② 정보시스템에 대한 접근자 계정의 접근기록은 매년 1회 이상 점검하고 관리한다.
      (2) 보안실무 담당자는 정보시스템에 대한 접근을 통제하기 위하여 관리자와 사용자의 계정관리 정책을 수립하고 시행한다.
         ① 정보시스템 사용자 계정은 입사 시 전산권한신청서[별첨 5]를 작성하여 별도 계정을 부여받으며 전자서명법에 의거하여 의료인은 공인된 기관으로부터 전자 공인인증서를 교부 받아 본인의 전자서명이 필요한 상황에서 사용하도록 한다.
         ② 정보시스템의 사용자에 대해서는 업무수행에 필요한 권한만을 부여하고 사용자 인증과정을 통해 접근이 가능하도록 한다.
         ③ 직원의 직종 및 업무에 따른 개별적 정보시스템 접근권한은 입사 시 담당자별 메뉴 권한을 부여하고 인사이동에 따라 변경되도록 한다. 퇴사 시에는 정보시스템 접근이 불가하도록 권한을 불용처리 한다.

(3) 비밀번호는 영문, 숫자, 특수문자조합으로 8자리 이상 설정하고 3개월마다 변경하도록 한다.
① 정보시스템에 사용되는 비밀번호는 암호화하여 저장하고, 비밀번호 분실 시 사용자 확인 후 공용 비밀번호로 초기화 세팅하여 개별 사용자가 자신의 비밀번호를 재설정 하도록 조치한다.
② 보안실무 담당자는 정보시스템의 사용자 계정과 비밀번호의 미승인 사용을 막고 미승인 된 사용시도를 즉각적이고 긴급히 찾아내어 개인정보보호 책임자에게 보고하여야 한다.
(4) 보안실무 담당자는 정보시스템이 1분 동안 사용되지 않을 경우 화면보호기가 실행되도록 하며 재접근 시 로그오프 되어 비밀번호 입력 후 사용하도록 조치를 취한다.
(5) 개인정보처리시스템 접속기록 위 · 변조 방지
① 개인정보처리시스템에 접속한 기록이 위 · 변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관한다.
② 개인정보처리시스템의 접속기록에 대한 정기적인 점검 및 분석 등을 토대로 개인정보 취급자에 의한 개인정보 오남용 방지 및 불법적인 접근 방지를 위한 대책 마련을 한다.
(6) 정보시스템의 비정상적인 접속기록이 발견되었을 시 보안실무 담당자는 개인정보보호 책임자에게 보고하여 필요한 조치를 취한다.

10. PC 및 개인용 휴대 단말기 관리 지침

1) PC 관리 지침

(1) 개인정보처리자는 업무 용도로만 시스템을 사용하고 개인정보처리시스템 또는 업무용 컴퓨터에 악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 한다.
(2) 개인정보처리자는 보안 프로그램의 자동 업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 적용하여야 한다.
(3) 각 층에 설치되는 PC는 각 층별 관리책임자를 지정한다.
(4) 개인정보처리자는 악성 프로그램관련 경보가 발령된 경우 또는 사용 중인 응용프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 적용하여야 한다.
(5) 개인정보처리자는 컴퓨터에 환자정보를 노출 시킨 채 장시간 이석하지 말아야 하고, 컴퓨터 모니터는 사람들이 지나가는 곳으로부터 방향이 전환되어 있어야 하며 자리를 이동할 시에는 로그아웃한다.
(6) 개인정보처리자는 화면 보호 기능을 1분 후 자동 잠금으로 되도록 설정한다.
(7) 병동복도에 설치되어 있는 PC사용자는 컴퓨터 스크린이 노출되지 않도록 주의하며 스크린 세이버 기능을 10초 후 자동 잠금으로 되도록 설정하며 이석 시 반드시 로그아웃하고 설정스크린을 내리도록 한다.
(8) 보안실무 담당자는 PC 폐기 또는 반출시 반드시 복구·재생되지 않도록 물리적으로 포맷하여 개인정보 등을 영구 삭제하여야 한다.

2) 개인용 휴대 단말기 관리 지침

(1) 휴대용 단말기는 병원 망 연결을 할 수 없도록 하며 필요시 정보보안 담당자에게 허가 후 사용하도록 하며 개인정보보안 담당자는 사전 악성코드 점검을 실시하여야 하고 병원의 보안통제프로그램을 설치하여야 하며 반출시 개인정보 등의 정보자산을 물리적으로 완전히 제거한다.

11. 전산운영관리 지침

1) 정보시스템 운영은 문서화된 지침과 절차에 따라 운영되고 관리되어야 한다.
2) 각 정보시스템에 대한 변경이 발생할 경우 아래와 같은 사항에 대한 통제 대책이 수립 되어야 한다.
   (1) 변경이 정보보호에 미치는 영향에 대한 분석
   (2) 변경에 대한 승인절차
   (3) 변경이 성공적으로 수행되지 않았을 경우에 복구하는 절차
   (4) 변경에 대한 상위 관리자의 확인
3) 운영 중인 정보시스템에 대하여 침해사고가 발생할 경우 신속하게 대응하기 위하여 다음의 사항을 포함하는 지침이 수립되어야 한다.
   (1) 침해사고 신고방법
   (2) 침해사고 발생 시 신속하게 복구할 수 있는 방법
   (3) 침해사고 원인을 분석하고 재발을 방지하기 위한 방법
   (4) 해당 침해사고 처리 후 상위 관리자에게 보고하는 내용 및 방법
4) 운영 중인 정보시스템은 개발 및 테스트시스템과 분리된 환경에서 운영되어야 한다.
5) 개발환경에서의 시험을 위하여 운영 중인 데이터가 개발 환경으로 복사될 경우 시험 데이터는 운영데이터와 동일한 수준으로 보호하고 통제한다.
6) 본원의 모든 서버는 보안실무담당자를 선정하여 운영한다.
7) 본원의 보안실무담당자는 시스템의 안정화를 위해 점검 및 예방 활동을 수행하고, 주기적으로 보안점검 및 분석을 실시하여 문제점 발견 시 이를 개인정보보호 책임자와 협의하여 적절한 통제대책을 강구한다.

12. 침해사고관리 지침
1) 침해사고의 범위에는 정보시스템 가동 및 서비스 중단, 악성코드 유포, 정보시스템의 오용으로 인한 병원정보시스템에 심각한 영향을 초래한 경우, 개인건강정보를 포함한 개인정보가 대량 유출된 경우 등이 있다.
2) 침해사고가 발생된 경우 보안실무 담당자는 지체 없이 개인정보보호 책임자에게 사실을 보고한다.
3) 개인정보에 관한 권리 또는 이익의 침해를 받은 자 또는 침해사고를 탐지한 자는 개인정보침해사실신고서[별첨 6]를 작성하여 개인정보 실무담당자에게 그 침해사실을 신고한다.
4) 개인정보 실무담당자는 신고 접수 후 개인정보보호 책임자에게 보고한다.
5) 개인정보보호 책임자는 사고 원인을 파악하고 중대사안인 경우는 병원장에게 보고하여 조치한 후 그 처리결과를 처리결과통지서[별첨 7]에 의하여 신고인에게 통지한다.
6) 개인정보 실무담당자는 보안사고 발생 시 사고 일자 및 사고 내용과 사고처리 등의 내용을 상세히 작성하여 사고일지를 문서화하여 관리, 보관한다.
7) 규정 위반 사례 관리
   개인정보보호 및 보안 규정이나 절차를 위반하여 병원의 이미지에 좋지 않은 영향을 끼친 직원에 대해서는 개인정보보호위원회의 심의 후 인사위원회에 상정하여 징계처리 한다. 특히 심각한 보안 사고를 일으켰다고 의심되는 직원에 대해서는 개인정보보호위원회 협의 후 경찰, 검찰 등 관련기관에 고발조치를 한다.
8) 침해사고로 인하여 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사실을 알린다.
   (1) 유출된 개인정보의 항목

(2) 유출된 시점과 그 경위
(3) 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
(4) 개인정보처리자의 대응조치 및 피해 구제절차
(5) 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

9) 침해사고로 개인정보가 유출된 경우 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 취한다.

10) 개인정보 유출 등의 신고
(1) 1만명 이상의 개인정보가 유출된 경우에는 본 계획 제18조에 따른 통지 및 조치결과를 지체 없이 행정자치부장관 또는 대통령령으로 정하는 전문기관(한국정보화진흥원, 한국인터넷진흥원)에 신고한다. 이 경우 행정자치부장관 또는 전문기관은 피해 확산방지, 피해 복구 등을 위한 기술을 지원할 수 있다.
(2) 개인정보 유출에 따른 통지의 시기, 방법, 절차 등에 관하여 필요한 사항은 아래와 같다.
① 윌스기념병원은 개인정보가 유출되었음을 알게 되었을 때에는 서면 등의 방법으로 지체 없이 제18조 각 호의 사항을 정보주체에게 알린다. 다만, 유출된 개인정보의 확산 및 추가 유출을 방지하기 위하여 접속경로의 차단, 취약점점검·보완, 유출된 개인정보의 삭제 등 긴급한 조치가 필요한 경우에는 그 조치를 한 후 지체 없이 정보주체에게 알린다.
② 윌스기념병원은 구체적인 유출 내용(시점 및 경위)을 확인하지 못한 경우에는 먼저 개인정보가 유출된 사실과 유출이 확인된 사항만을 서면 등의 방법으로 먼저 알리고 나중에 확인되는 사항을 추가로 알린다.
③ 1만명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 서면 등의 방법과 함께 인터넷 홈페이지에 정보주체가 알아보기 쉽도록 정보를 (유출된 개인정보의 항목, 유출된 시점과 그 경위, 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보, ○○○의 대응조치 및 피해 구제절차, 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처) 7일 이상 게재한다.

Ⅵ. 담당자 지정 (개인 정보 보호 조직도)

구분	직책	소속	역할
위원장	개인정보보호 총괄책임자	행정부원장	1. 개인정보보호에 관한 업무 및 활동에 관한 사항을 총괄 2. 개인정보 보호 계획의 수립 및 시행 3. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선 4. 개인정보 처리와 관련한 불만의 처리 및 피해 구제 5. 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축 6. 개인정보 보호 교육 계획의 수립 및 시행 7. 개인정보파일의 보호 및 관리·감독 8. 개인정보취급자 관리, 감독 9. 개인정보처리에 관한 안전조치 시행 10. 그 밖에 개인정보의 적절한 처리를 위하여 대통령령으로 정한 업무
간사	개인정보보호 관리책임자	진료지원과장	1. 개인정보 보호를 위한 각종 활동계획의 수립 2. 개인정보 보호 관련 정책 및 규정 수립의 지원 3. 개인정보 보호 관련 교육 및 훈련 4. 관련법령 및 규범 등에 대한 문서화 및 유지관리 5. 환자의 개인정보 보호 관련 불만 및 고충처리 관련 업무
위원	원내 층별 관리적보안 담당자	원무과장 전산주임 PA 실장 6병동수간호사 7병동수간호사 심사팀장	1. 개인정보보호 및 보안 규정과 지침의 숙지 및 준수 2. 개인정보보호 활동 및 교육 참여 3. 개인정보보호 및 보안서약서의 작성 4. 개인정보유출 및 보안사고 발생 시 신고 및 대응 5. 기타 개인정보보호에 관하여 필요한 업무
실무	IT 보안 관리자	전산주임	1. 외부로부터의 침입, 접근 및 해킹 등으로부터 개인정보보호시스템을 보호하여 개인정보가 유출되지 않도록 하는 업무 2. 기관의 개인정보시스템을 관련 법률과 기관의 개인정보보호 규정에 적합 하도록 관리 하는 업무
	물리적 보안 관리자	관리과장	1. 허가받지 않은 인원의 출입통제, 출입통제 보안장치를 관리하는 업무 2. CCTV등 영상물에 대한 개인정보 장치를 관리하는 업무

Ⅶ. 개인정보 보호를 위한 보안체계

1. 접근통제구역의 지정 및 출입통제

1) 종이서류 보관 장소 및 접근통제 방법

구분	보관 장소	접근통제방법
종이서류	별관(피부과)3층	번호키패드로 인증
전자차트	본관8층 서버실	번호, 지문 등으로 인증, 24시간 CCTV 녹화

2) 정보시스템 접근 통제

시스템	도입제품	역할
통합보안관리	SonicWall	허가 받지 않은 외부접속차단

DB접근제어	SeNeapp	허가 받은 외부접속에 대한 감사
정보유출방지	GuardZone	내부 개인정보 유출 차단
개인정보 암호화	PI.-FILTER	각 PC 개인정보 암호화
E.M.R 개인정보 암호화	MEDI+SECURE	E.M.R DB 암호화
백신	V3	내부 침입 악성 코드 차단

2. 정보시스템 접근권한
   1) 직원의 직종 및 업무에 따라서 개별적으로 전산담당자가 정보시스템 접근권한을 부여한다.
   2) 모든 사용자에게 별도 계정을 부여하며, 적절한 인증기술(아이디/패스워드, 공인인증서)을 통하여 정보시스템 접근한다.
   3) 인사이동 및 퇴직 등으로 인한 접근권한은 즉시 실행하며 해당 기록에 대한 장부를 남겨둔다.
   4) 의무기록 담당자가 정기적으로 각 직원에 대한 의무기록 접근권한을 검토하여 개인정보 담당자에게 전달하며, 최종 확인 후 정보시스템에 해당 사항에 대하여 반영한다.
   5) 개인정보에 대하여 규정위반 사례 발견 시, 절차에 따라 처리한다.
3. 의료행위와 관련된 정보시스템 접속기록 보관, 관리
   1) 접속이력의 기록
      (1) 사용자 ID, 날짜 및 시간, 접근권한은 접속기록에 포함한다.
      (2) 허용된 권한 외의 접근, 비정상적으로 많은 데이터 다운로드 등 비정상적인 접근 기록에 대한 이력을 관리한다.
   2) 기록의 관리
      (1) 개인정보의 쓰기, 삭제, 출력에 대한 접근기록을 관리하며 [W-12.1(1) 의료정보의무기록의 개인정보 취급관리 및 책임]에 따른다.
      (2) 의료정보시스템에 접속한 기록을 최소 6개월 이상 보관 · 관리한다.
      (3) 의료정보시스템의 입 · 출력 및 수정사항, 데이터 접근내역 등을 자동으로 기록, 저장하여 관리하여 접속이력 정보는 변경할 수 없어야 한다.
      (4) 의무기록사는 접근현황에 대해 주기적인 모니터링을 실시해 월1회 보안 실무담당자에게 자료를 제출하고 보안 실무담당자는 개인정보보호 책임자에게 보고하고 연1회 이상 재검토한다.
      (5) 접속이력에 대한 위반사례가 있을 경우 보안 실무담당자는 개인정보보호 책임자에게 보고하고 필요한 조치를 취한다.

Ⅷ. 참고

1. 개인정보보호법(2015년) 및 동법 시행령(2015년), 시행규칙 (2014년)
2. 개인정보보호 가이드라인(보건복지부, 행정자치부)- 의료기관편 (2015년)

[별첨]

별첨1. 정보보호 및 소프트웨어 서약서
별첨2. 내부관리 계획
별첨3. 개인정보처리위탁계약서
별첨4. 통제구역출입관리대장
별첨5. 전산권한신청서
별첨6. 개인정보침해사실 신고서
별첨7. 처리결과 통지서

입안자	규정관리위원장	
승인책임자	병원장	
서명일		

[별첨 1] 정보보호 및 소프트웨어 서약서

정보 보호 서약서

성 명 :
주민등록번호 :

본인은 윌스기념병원(이하 “병원”라 함)을 근무함에 있어 아래 사항을 충분히 숙지하고, 성실히 준수할 것을 서약합니다.

1. 병원에 재직한 기간 중 독자적으로 또는 다른 사람과 함께 취득한 기술정보(발명, 특허, 개발, 생산 등 제반 기술) 및 경영정보(재무, 관리, 기획, 영업, 인사 등 제반 정보)등 모든 영업비밀은 전적으로 회사의 소유이며, 회사가 사용하거나 처분할 권리가 있음을 인정합니다.
2. 어떠한 장소에 어떠한 방법으로도 병원의 영업비밀, 자산, 개인정보를 보유하거나 병원 외부로 유출하지 않음을 확인합니다.
3. 재직기간 중 취득한 병원의 모든 영업비밀(경영 및 기술정보) 및 개인정보는 퇴사 후에도 병원의 업무 인수.인계와 관련 없는 어떠한 병원내외 제3자에게 누설하지 않겠습니다.
4. 퇴직 후 3년간 병원의 영업비밀을 이용하여 창업하거나 경쟁관계에 있는 병원, 또는 기타 제3자를 위하여 영업비밀을 누설하거나 사용하지 않겠습니다.
5. 병원의 영업비밀 보호 및 개인정보 보호를 위한 노력에 적극 협조할 뿐만 아니라, 그에 따른 법적.도덕적 의무를 성실히 이행하겠습니다.
6. 의료정보는 본원에서 정하는 의무기록 관리 규정에 따라 열람, 복사할 것이며 적정한 절차 없이 의무기록(또는 전자의무기록)에 저장된 정보를 무단으로 열람,복사,누출하지 않겠습니다.

본인은 위의 사항을 충분히 숙지하여 이를 성실히 준수할 것이며 만일 이를 위반하였을 경우 부정경쟁방지, 영업비밀에 관한 법률, 개인정보보호법 등 관련 법령에 따라 민.형사상의 책임뿐만 아니라 제반 손해 배상의 책임 등 불이익을 감수할 것이며, 회사에 끼친 손해에 대해 지체 없이 변상.복구할 것을 서약합니다.

20 년 월 일

서 약 자 : (서 명)

윌스기념병원장 귀하

[별첨 2] 내부관리 계획

윌스기념병원
개인정보 내부관리 계획 개정안

	개인정보보호 실무담당자	개인정보보호 책임자	병원장
결제			
날짜			

검토일 : 년 월 일

승인일 : 년 월 일

윌스기념병원장

윌스기념병원
개인정보 내부관리 계획

목 차

제1장 총칙

제1조(목적)

개인정보 보호 내부관리계획은 개인정보보호법 제29조(안전조치의무) 내부관리계획의 수립 및 시행 의무에 따라 제정된 것으로 윌스기념병원이 취급하는 개인정보를 체계적으로 관리하여 개인정보가 분실, 도난, 누출, 변조, 훼손, 오·남용 등이 되지 아니하도록 함을 목적으로 한다.

제2조(적용범위)

본 계획은 홈페이지 등의 온라인을 통하여 수집, 이용, 제공 또는 관리되는 개인정보뿐만 아니라 오프라인(서면, 전화, 팩스 등)을 통해 수집, 이용, 제공 또는 관리되는 개인정보에 대해서도 적용되며, 이러한 개인정보를 취급하는 내부 임직원 및 외부업체 직원에 대해 적용된다.

제3조(용어 정의)

1. “개인정보”라 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.
2. “처리”란 개인정보의 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.
3. “정보주체”란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
4. “개인정보처리자”란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
5. “개인정보 보호책임자”란 개인정보의 처리에 관한 업무를 총괄해서 책임지는 자로서 영 제32조제2항제1호 및 제2호에 해당하는 자를 말한다.
6. “개인정보 보호담당자”란 개인정보책임자가 업무를 수행함에 있어 보조적인 역할을 하는 자를 말하며 개인정보 보호 책임자가 일정 요건의 자격을 갖춘 이를 지정한다.
7. "개인정보취급자”란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 임직원, 위탁업체 직원, 학생 등을 말한다.

8. “개인정보처리시스템”이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다.
9. “영상정보처리기기”란 폐쇄회로텔레비전(CCTV), 네트워크카메라 등 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 일체의 장치를 말한다.
10. “개인영상정보”라 함은 영상정보처리기기에 의하여 촬영·처리되는 영상정보 중 개인의 초상, 행동 등 사생활과 관련된 영상으로서 해당 개인의 동일성 여부를 식별할 수 있는 정보를 말한다.
11. “영상정보처리기기 운영자”라 함은 개인정보보호법 제25조제1항 각호에 따라 영상정보처리기기를 설치·운영하는 자를 말한다.

제2장(내부관리계획의 수립 및 시행)

제4조(내부관리계획의 수립 및 승인)

① 개인정보 보호책임자는 윌스기념병원의 개인정보 보호를 위한 전반적인 사항을 포함하여 내부관리계획을 수립하여야 한다.

② 개인정보 보호책임자는 개인정보 보호를 위한 내부관리계획의 수립 시 개인정보 보호와 관련한 법령 및 관련 규정을 준수하도록 내부관리계획을 수립하여야 한다.

③ 개인정보 보호책임자는 개인정보 보호담당자가 수립한 내부관리계획의 타당성을 검토하여 개인정보 보호를 위한 내부관리계획을 승인하여야 한다.

④ 개인정보 보호담당자는 개인정보 보호 관련 법령의 제·개정 사항 등을 반영하기 위하여 매년 11월말까지 내부관리계획의 타당성과 개정 필요성을 검토하여야 한다.

⑤ 개인정보 보호담당자는 모든 항목의 타당성을 검토한 후 개정할 필요가 있다고 판단되는 경우 12월말까지 내부관리계획의 개정안을 작성하여 개인정보 보호책임자에게 보고하고 개인정보 보호책임자의 승인을 받아야 한다.

제5조(내부관리계획의 공표)

① 개인정보 보호책임자는 전조에 따라 승인한 내부관리계획을 매년 1월말까지 윌스기념병원 전 임직원에게 공표한다.

② 내부관리계획은 임직원이 언제든지 열람할 수 있게 사내통신망의 게시판을 통하여 게시하며, 변경사항이 있는 경우에는 이를 공지하여야 한다.

제3장 개인정보 보호책임자의 의무와 책임

제6조(개인정보 보호책임자의 지정)

① 윌스기념병원은 개인정보보호법 시행령 제32조제2항1호에 따라 해당하는 지위에 있는 자를 개인정보 보호책임자로 임명한다.

1. 사업주 또는 대표자
2. 개인정보 처리 관련 업무를 담당하는 부서의 장 또는 개인정보 보호에 관한 소양이 있는 사람

제7조(개인정보 보호책임자의 의무와 책임)

① 개인정보 보호책임자는 정보주체의 개인정보 보호를 위하여 다음 각 호의 업무를 수행한다.

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

② 개인정보 보호책임자는 업무를 수행함에 있어서 필요한 경우 개인정보 처리 현황, 처리 체계 등에 대하여 수시로 조사하거나 관계 당사자로부터 보고를 받을 수 있

다.

③ 개인정보 보호책임자는 개인정보 보호와 관련하여 이법 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 하며, 필요하면 소속 기관 또는 단체의 장에게 개선조치를 보고하여야 한다.

제8조(개인정보취급자의 범위 및 의무와 책임)

① 개인정보취급자의 범위는 다음과 같다.

1. 윌스기념병원 내에서 정보주체의 개인정보를 처리하는 업무를 수행하는 자를 말하며, 직원외 위탁업체 직원, 학생 등 포함될 수 있다.

② 개인정보취급자의 의무와 책임

1. 내부관리계획의 준수 및 이행
2. 개인정보의 기술적·관리적 보호조치 기준 이행
3. 업무상 알게 된 개인정보를 제3자에게 제공하지 않음

제4장 개인정보의 기술적·관리적 보호조치

제9조(개인정보취급자 접근권한 관리 및 인증)

① 개인정보처리자는 개인정보처리시스템에 대한 접근권한을 업무수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.

② 개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여야 하며, 또한 비밀유지의무 등에 대한 서약서를 받아야 한다.

③ 개인정보처리자는 제1항, 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.

④ 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자 계정을 발급하는 경우, 개인정보취급자 별로 한 개의 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

⑤ 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스

템에 접속하려는 경우에는 가상사설망 또는 전용선 등 안전한 접속수단을 적용하여야 한다.

제10조(비밀번호 관리)

① 개인정보처리자는 개인정보취급자 또는 정보주체가 생일, 주민등록번호, 전화번호 등 추측하기 쉬운 숫자나 개인관련 정보를 패스워드로 이용하지 않도록 비밀번호 작성규칙을 수립하고, 이를 적용 및 운용하여야 한다.

② 개인정보처리자는 비밀번호에 적정한 기간의 유효기간(분기별 1회 이상)을 설정하여야 한다.

제11조(접근통제)

① 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 시스템을 설치·운영하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol)주소 등으로 제한하여 인가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지

② 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 업무용 컴퓨터에 조치를 취하여야 한다.

제12조(개인정보의 암호화)

① 개인정보처리자는 주민등록번호, 비밀번호, 바이오정보에 대해서는 안전한 암호 알고리즘으로 암호화하여 저장하여야 한다. 단, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

② 개인정보처리자는 정보주체의 개인정보를 정보통신망을 통하여 송·수신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

③ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

④ 개인정보처리자 또는 개인정보취급자는 정보주체의 개인정보를 업무용 컴퓨터(PC)

에 저장할 때에는 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화 저장하여야 한다.

제13조(접속기록의 위·변조 방지)

① 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 최소 6개월 이상 보관하여야 한다.

② 개인정보처리자는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.

제14조(보안프로그램 설치 및 운영)

① 개인정보처리자는 개인정보처리시스템 또는 업무용 컴퓨터에 악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 한다.

② 보안 프로그램의 자동 업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 적용하여야 한다.

③ 악성 프로그램관련 경보가 발령된 경우 또는 사용 중인 응용프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 적용하여야 한다.

제15조(물리적 접근제한)

① 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다.

② 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.

③ 개인정보처리자는 물리적 접근방지를 위한 별도의 보호시설에 출입하거나 개인정보를 열람하는 경우, 그 출입자에 대한 출입사실 및 열람 내용에 관한 관리대장을 작성하도록 하여야 한다.

제5장 개인정보 보호 교육

제16조(개인정보 보호 교육 계획의 수립)

① 개인정보 보호책임자는 다음 각 호의 사항을 포함하는 연간 개인정보 보호 교육계획을 매년 11월말까지 수립한다.

1. 교육목적 및 대상
2. 교육내용
3. 교육 일정 및 방법

② 개인정보 보호책임자는 수립한 개인정보 보호 교육 계획을 실시한 이후에 교육의 성과와 개선 필요성을 검토하여 차년도 교육계획 수립에 반영하여야 한다.

제17조(개인정보 보호 교육의 실시)

① 개인정보 보호책임자는 정보주체 정보보호에 대한 직원들의 인식제고를 위해 노력해야 하며, 개인정보의 오·남용 또는 유출 등을 적극 예방하기 위해 임·직원을 대상으로 매년 정기적으로 연2회 이상의 개인정보 보호 교육을 실시한다.

② 신규직원들 대상으로 입사일 3개월 이내 교육을 실시한다.

③ 교육 방법은 집체 교육뿐만 아니라, 인터넷 교육, 그룹웨어 교육 등 다양한 방법을 활용하여 실시하고, 필요한 경우 외부 전문기관이나 전문요원에 위탁하여 교육을 실시한다.

④ 개인정보 보호에 대한 중요한 전파 사례가 있거나 개인정보 보호 업무와 관련하여 변경된 사항이 있는 경우, 개인정보 보호책임자는 부서 회의 등을 통해 수시 교육을 실시할 수 있다.

제6장 개인정보 침해대응 및 피해구제

제18조 (개인정보 유출 등의 통지)

① 윌스기념병원은 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사실을 알려야 한다.

1. 유출된 개인정보의 항목
2. 유출된 시점과 그 경위
3. 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
4. 윌스기념병원의 대응조치 및 피해 구제절차

5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

② 윌스기념병원은 개인정보가 유출된 경우 그 피해를 최소화하기 위하여 침해사고 대응팀을 구성하고 필요한 조치를 한다.

제19조 (개인정보 유출 등의 신고)

① 윌스기념병원은 1만명 이상의 개인정보가 유출된 경우에는 본 계획 제18조에 따른 통지 및 조치 결과를 지체 없이 행정자치부장관 또는 대통령령으로 정하는 전문기관(한국정보화진흥원, 한국인터넷진흥원)에 신고하여야 한다. 이 경우 행정자치부장관 또는 전문기관은 피해 확산방지, 피해 복구 등을 위한 기술을 지원할 수 있다.

② 개인정보 유출에 따른 통지의 시기, 방법 및 절차 등에 관하여 필요한 사항은 아래와 같다.

1. 윌스기념병원은 개인정보가 유출되었음을 알게 되었을 때에는 서면 등의 방법으로 지체 없이 제18조 각 호의 사항을 정보주체에게 알려야 한다. 다만, 유출된 개인정보의 확산 및 추가 유출을 방지하기 위하여 접속경로의 차단, 취약점 점검·보완, 유출된 개인정보의 삭제 등 긴급한 조치가 필요한 경우에는 그 조치를 한 후 지체 없이 정보주체에게 알릴 수 있다.

2. 윌스기념병원은 구체적인 유출 내용(시점 및 경위)을 확인하지 못한 경우에는 먼저 개인정보가 유출된 사실과 유출이 확인된 사항만을 서면 등의 방법으로 먼저 알리고 나중에 확인되는 사항을 추가로 알릴 수 있다.

3. 1만명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 서면 등의 방법과 함께 인터넷 홈페이지에 정보주체가 알아보기 쉽도록 정보를(①유출된 개인정보의 항목, ②유출된 시점과 그 경위, ③유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보, ④윌스기념병원의 대응조치 및 피해 구제절차, ⑤정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처) 7일 이상 게재하여야 한다.

[별첨 3] 개인정보처리위탁계약서

안양 윌스기념병원 OCS/EMR 소프트웨어 운영보조 및 지원 용역계약에 따른 개인정보 열람에 관한 위탁 협정서

안양 윌스기념병원(이하 "갑"이라 한다)과 (주)엔지테크(이하 "을"이라 한다)는 "갑"의 개인정보 처리업무를 "을"에게 위탁함에 있어 다음과 같은 내용으로 본 개인정보열람 보안협약을 체결한다.

제1조 (목적) 이 계약은 "갑"이 개인정보 열람업무를 "을"에게 위탁하고, "을"은 이를 승낙하여 "을"의 책임아래 성실하게 업무를 완성하도록 하는데 필요한 사항을 정함을 목적으로 한다.

제2조 (용어의 정의) 본 계약에서 별도로 정의되지 아니한 용어는「개인정보 보호법」시행령 및 시행규칙,「개인정보의 안전성 확보조치 기준」(행정자치부 고시 제2014-7호) 및「표준 개인정보 보호지침」(행정안전부 고시 제2011-45호)에서 정의된 바에 따른다.

제3조 (열람 목적 및 범위)

3조1항. "을"은 계약이 정하는 바에 따라 "OCS/EMR 소프트웨어 운영보조 및 지원을 위한 용역 수행"을 목적으로 한다.

3조2항. 범위는 "OCS/EMR 소프트웨어 운영보조 및 지원을 위한 용역 계약서"에 준하여, 용역내용의 관련된 개인정보 처리 업무를 수행한다.

제4조 (재위탁 제한)

4조1항. "을"은 "갑"의 사전 승낙을 얻은 경우를 제외하고 "갑"과의 계약상의 권리와 의무의 전부 또는 일부를 제3자에게 양도하거나 재위탁할 수 없다.

4조2항. "을"이 재위탁받은 수탁회사를 선임한 경우 "을"은 당해 재위탁계약서와 함께 그 사실을 즉시 "갑"에 통보하여야 한다.

제5조 (개인정보의 안전성 확보조치) "을"은 개인정보보호법 제29조, 동법 시행령 제30조 및 개인정보의 안전성 확보조치 기준 고시(행정안전부 고시 제2011-43호)에 따라 개인정보의 안전성 확보에 필요한 관리적·기술적 조치에 "갑"과 함께 협력 한다.

제6조 (개인정보의 처리제한)

6조1항. "을"은 계약기간은 물론 계약 종료 후에도 위탁업무 수행 목적 범위를 넘어 개인정보를 이용하거나 이를 제3자에게 제공 또는 누설하여서는 안 된다.

6조2항. "을"은 계약이 해지되거나 또는 계약기간이 만료된 경우 위탁업무와 관련하여 보유하고 있는 개인정보를 「개인정보보호법」시행령 제16조에 따라 즉시 파기하거나 "갑"에게 반납하여야 한다.

6조3항 제6조2항에 따라 "을"이 개인정보를 파기한 경우 지체 없이 "갑"에게 그 결과를 통보하여야 한다.

제7조 (수탁자에 대한 관리.감독 등) "갑"은 "을"에 대하여 다음 각 호의 사항을 관리하도록 요구할 수 있으며, "을"은 특별한 사유가 없는 한 이에 응하여야 한다.

(단, "갑"이 "을"에게 요구시 반드시 서면으로 요구 해야 하며, 서면으로 요구된 항목에 한하여 "을"은 응할 수 있다.)

1. 개인정보의 처리 현황
2. 개인정보의 접근 또는 접속현황
3. 개인정보 접근 또는 접속 대상자

[별첨 4] 통제구역출입관리대장

전산서버실 출입 대장

날짜	출입시간	성명	부서명 / 회사명	연락처	출입 목적

행정원장	담당

[별첨 5] 전산권한신청서

EMR 권한 (발급,변경,취소) 신청서

부서		이름	
ID	전산팀 통보	Password	전산팀 통보(변경 가능)
신청사유			

상기와 같은 사유로 업무상 필요한 EMR 권한을 신청합니다.

날 짜 : 년 월 일

부 서 장 : (인)

부서별 시작 번호					
외래간호사	23	심사	50	총무,인사	52, 57
병동간호사	26, 27	영상의학	54	관리,홍보	53
수술실간호사	21	임상병리	58	약국	30
마취과간호사	24	운동,재활	55	영양	56
상담간호사	20	원무	51	의료진	10

상기 인원의 EMR □발급 □변경 □취소를(을) 허가함

날 짜 : 20 년 월 일

윌스기념병원장

[별첨 6] 개인정보침해사실 신고서

개인정보침해사실 신고서

① 신고인	성 명		
	생년월일		
	연락처	전화번호(핸드폰)	
		전자우편	
		주 소	
② 피신고기관	기 관 명		
	연락처	전화번호	
		주 소	
③ 신고내용			

「개인정보보호법」 제34조 제1항에 따라 위와 같이 개인정보침해사실을 신고합니다.

첨부 :

년 월 일

신고인 : (서명 또는 인)

[별첨 7] 처리결과 통지서

처리결과통지서

① 접수번호		② 처리기한		
③ 처리기관명		④ 담당자	직위/성명	
			연락처	
⑤ 침해신고 주요내용				
⑥ 처리결과				

「개인정보보호법」 제32조의 제1항에 따라 귀하께서 신고하신 개인정보의 침해사실에 대하여 위와 같이 처리하였음을 알려드립니다.

년 월 일

윌스기념병원