일본 의료기관의 프라이버시마크 제도

The Privacy Mark System for Medical Institutions in Japan

송 태 민 한국보건사회연구원 부연구위원
이 중 순 일본 NTT커뮤니케이션즈 부장

1. 서 론

일본의 프라이버시마크 제도는 JIS Q 15001에 의거하여 개인정보보호[1]의 적절한 보호를 위한 체제를 정비하고 있는 사업자에 대하여, 신청서를 받아 심사를 하고 프라이버시마크를 부여하는 제도를 말한다. 현재 일본의 의료기관에 있어서는 전자차트나 원무전산시스템의 보급이 확대됨에 따라 환자나 의료관계자의 편의성이 확대되는 반면, 의료기관의 컴퓨터에 축적되어 있는 환자정보의 누설에 따른 프라이버시 침해의 위험이 커져가고 있다. 따라서 이에 대한 대책으로서 의료기관에 있어서의 프라이버시마크 제도가 도입되어 현재 인증을 희망하는 의료기관이 급속히 늘어 가고 있는 상황이다. 본 고는 이러한 일본의 의료분야에 있어서 개인정보보호의 실현을 목적으로, JIS Q 15001에 근거하여 시행되고 있는 프라이버시마크 제도를 살펴보고 국내 도입가능성에 대한 시사점을 논하고자 한다.

1) 일본의 민간부문에 있어서의 개인정보 보호에 대해서는 개인정보보호 가이드라인을 기준으로 하고 있다. 이러한 가이드라인을 기반으로 하여 「개인정보에 관한 컴플라이언스(compliance)·프로그램의 요구사항(JIS Q 15001)」이 제정됐으며, JIS의 규정은 개인정보를 취급하는 기관의 업무가 JIS규정에 적합한지를 스스로 평가할 수 있도록 하고 제3자에 의한 평가기준으로서도 활용 가능하도록 기술되어 있다.

2. 일본 의료기관의 프라이버시마크(P-Mark) 제도

1) 의료기관의 프라이버시마크 취득의 개요

의료기관이 프라이버시마크를 취득하려면 JIS Q 15001에 의거하여 의료기관이 보유하는 개인정보를 보호하기 위한 방침, 조직, 계획, 실시, 감사, 재검토를 포함한 관리시스템을 구축・운용하여 신청한다. 인증된 사업자에게는 그 취지를 나타내는 프라이버시마크가 부여된다. 구체적인 사업으로는 의료기관에서 취급하는 진료기록, 처방전표, 검사의료전표, 검사결과보고서, 간호기록, 원무기록 등의 개인정보를 포함한 보호대상을 추출하고 리스크를 분석하여 환자로부터 그 이용목적의 동의를 받아 목적에 따른 진료정보를 수집하고 적절한 보안 관리 하에 개인이 동의하는 범위 내에서 이용할 수 있다는 내용 등이다. 과거의 의료기관에서의 프라이버시보호는 1인실의 권유나 환자의 진료내용이 외부에서 청취되지 않도록 하는 등의 주의가 고작이었으나, 새로운 개인정보보호의 개념에서는 개인정보를 환자의 동의에 의해서만 이용목적에 따라 활용할 수 있다는 것과 역으로 동의가 없는 이용 목적에는 사용하지 못하도록 하는 것 등의 운용규범이 요구되고 있다. 즉, 개인정보보호는 환자정보가 외부에 누설방지를 위해 사용을 억제하는 소극적인 관리가 아니라, 활용을 바라는 환자의 데이터는 동의한 이용목적이나 이용자의 범위가 지켜지도록 안전하게 관리하여 적절한 활용을 가능케 하는 것이다. 이러한 개인정보보호를 위한 활동은 의료의 투명화를 지원하고 환자들로부터의 신뢰를 높여 환자가 주체적으로 진료에 참가하는 열린 의료를 실현하기 위해 매우 중요한 활동이다.

2) 프라이버시마크 제도의 실시 체계

일본의 프라이버시마크 제도는 프라이버시마크 부여기관과 프라이버시마크 부여 인증 지정기관의 2종류의 기관으로 운영되고 있다. 부여기관은 (재)일본정보처리개발협회에서 담당하며, 지정기관은 4개의 기관(정보서비스산업협회, 일본마케팅리서치협회, 전국학습학원협회, 의료정보시스템개발센터)에서 담당하고 있다. 부여기관과 지정기관의 역할은 다음과 같다.

프라이버시마크 부여기관의 역할은 다음과 같다.

① 사업자로부터의 프라이버시마크 부여의 신청을 심사하여 인증하는 것
② 프라이버시 지도를 적정하게 운영하는 것
③ 소비자로부터의 불평을 받아들이는 것
④ 프라이버시 마크를 부여하는 것

프라이버시마크 부여 인증 지정기관의 역할은 다음과 같다.

① 지정기관을 지정하는 것
② 프라이버시마크 제도 위원회의 설치
③ 제도의 기준, 규정 등의 책정 및 개정
④ 지정기관의 지정 및 취소
⑤ P마크 부여 인증의 취소
⑥ 제도의 운용 상황의 감사

3) 보건의료 분야의 프라이버시마크 부여대상

보건의료분야의 프라이버시마크 부여의 대상은 JIS Q 15001에 준해 책정한 「의료기관의 인증지침」을 적용범위로 하는 보건・의료에 관한 사업을 주로 실시하는 사업자를 대상으로 하며 해당되는 사업대상자는 다음과 같다.

- 병원
- 진료소(일반・치과 진료소)
- 의학・약학계 교육기관 및 연구소 등
- 조제 약국, 검사 센터 등
- 그 외, 보건의료(복지 분야를 포함)에 관련하는 사업자

프라이버시마크 부여 단위는 사업자(법인) 단위로 부여를 한다. 프라이버시마크 부여와 관련된 비용은 신규일 경우 소규모사업자는 220,000¥, 중규모사업자는 450,000¥, 그리고 대규모사업자는 900,000¥을 2년간의 사용료로 집행한다. 프러이버시마크의 유효기간은 2년간이며 이후 2년마다 갱신할 수 있다. 그리고 프라이버시마크 제도 운용에 문제가 있는 사업자는 비록 유효기관 내라 할지라도 프라이버시마크 부여 인증을 취소할 수 있다.

4) 의료기관의 프라이버시마크 도입 현황

일본은 2005년 4월 1일부터 개인정보보호법이 시행된 이후, 개인정보 취급에 대한 사회적인 인식이 높아졌다. 특히, 개인정보를 취급하는 기관이나 종사자의 데이터를 포함하여 5,000건 이상의 개인정보를 보유하고 있는 기관은 개인정보의 누설방지책을 강구하는 법적책임이 주어지고 있다. 이러한 시점에서 일본의 의료기관에서 프라이버시마크의 도입은 2004년부터 소개되어 2005년에 인증심사를 받아 현재 약 50개 기관이 마크를 부여받고, 100개 기관은 심사대기중에 있다. 현재까지 P-Mark를 부여받은 기관은 병원 보다는 검진센터, 병리검사센터, 개호지원사업자 등 개인정보를 취급하는 의료지원 사업자가 많으나 병원에서의 도입은 이러한 사업자의 다음 단계로서 시작될 것으로 예상하고 있다. P-Mark 제도의 유용성은 마크를 눈에 잘 띄는 곳에 부착하여 의료기관이 개인정보 취급에 대한 적절한 체제를 정비하여 운용하고 있다는 것을 알려서 환자들이 안신감과 신뢰감을 갖게 한다. 따라서 P-Mark 제도는 의료기관 스스로도 개인정보 관리에 철저를 기함은 물론, 환자들로 하여금 개인정보보호에 대한 의식을 향상시키는 것이 목적이다.

그림 1. P-Mark Logo

3. 의료기관의 프라이버시마크(P-Mark) 제도의 시사점

국내에서 유무선 통신망, 인터넷, 인트라넷 등에 의한 정보통신망의 급격한 보급으로 각종 개인정보의 유출 위험을 가중시키고 있다. 개인정보보호 및 프라이버시 보장을 위해서는 국제적으로는 1980년 OECD 가이드라인, 1981 유럽회의 협약, 1990년 UN의 가이드라인, 1995년 EU 개인정보보호 지침 등이 개인정보보호를 위한 원칙으로 확립되고 있다. 국내의 개인정보보호기구로는 개인정보심의위원회, 공정거래위원회, 금융감독위원회, 한국정보보호진흥원의 개인정보침해신고센터 등이 있다. 그리고 국내의 공공기관의 개인정보보호에 관한 법률은 1999년 1월에 개정되어 개인정보의 범위를 '생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명·주민등록번호 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)라고 규정되어 있다. 한편 이러한 개인정보를 인증하기 위한 제도로는 '인터넷 사이트 안전마크', '개인정보보호마크', 'eTrust마크' 등이 있으나 의료분야에 있어서는 아직 논의가 되고 있지 않다. 현재 국내 의료분야의 개인정보보호에 대해서는 '공공기관의개인정보보호에관한법률'에 준용하여 관리하고 있다. 특히 동법에 의한 개인정보의 수집, 처리, 열람에 대해서는 매우 엄격한 규정을 두고 있으나, 해당 공공기관에서 조차 개인정보 관리의 세부내용에 대한 의식이 부족한 실정에 있다. 따라서 국내의 공공과 민간 의료기관의 P-Mark 도입은 환자가 의료기관을 신뢰하고 개인정보 관리에 철저를 기함은 물론 의료기관과 환자 쌍방이 개인정보보호에 대한 의식을 향상시키는데 기여할 것으로 본다.