전자의무기록시스템 인증제

외부보관 및 클라우드 컴퓨팅 서비스 인증

인증기준 및 심사방안 FAQ

한국보건의료정보원

보건복지부 (재)한국보건의료정보원 Korea Health Information Service

FAQ

Q.

기 인증받은 업체의 온 프레미스 기반 EMR제품을 의료기관에 납품 시, 의료기관의 요청에 의해 클라우드 업체의 IaaS 에 구축하는 경우 인증은 어떻게 진행하면 되나요 ?

A.

업체의 온프레미스 기반 EMR제품을 의료기관에 SI 형태로 구축하는 경우 별도의 제품인증(의료기관이 신청) 심사를 통해 기능 변경 유무를 확인 및 의료기관에 제품인증을 부여하고 있으며, 이때 S014 인증기준까지 인증심사를 진행합니다.

FAQ

Q.

기존에 인증 신청이 접수된 클라우드 방식의 EMR제품도 변경된 인증기준으로 심사를 진행하나요?

A.

기 인증서 발급이 된 경우 外(인증신청 접수 또는 심사 미진행된 상태의 건)에는 변경된 인증기준으로 심사를 진행하게 됩니다.

따라서 심사원이 사전문서검토 단계 또는 현장심사 시 S014에 대한 추가 증빙자료 요청을 할 예정입니다.

FAQ

Q.

ISMS 인증된 인프라를 사용하는 경우, S014 제1호(EMR시설장비기준 고시 준수)에 대해서는 3가지 사항만 추가 증빙자료를 제출하는 것으로 확인됩니다. 이때에도 현장 심사를 진행하나요?

A.

EMR제품을 운영하는 인프라사업자가 ISMS 인증 취득을 하였다면, S014 제1호 항목은 ISMS의 통제항목이 아닌 3가지 항목에 대해서 심사원이 확인을 합니다.

이때 EMR업체는 인프라사업자로 부터 3가지 항목에 대한 증빙자료를 취합하여 제출하여야 하며, 심사원이 증빙자료의 추가적인 확인이 필요하다고 판단한 경우 현장 심사를 진행할 수 있습니다.

FAQ

Q.

취약점 점검 및 모의침투테스트에 대한 증빙자료는 어떤 것을 제출하면 됩니까?

A.

변경된 S014 인증기준에서는 EMR 운영 인프라 및 EMR SW에 대하여 취약점 점검 및 모의침투테스트를 실시하고 취약점 조치 수행을 요구하고 있습니다.

이때 EMR인증 신청기관은 발견된 취약점에 대해 조치 완료하였음을 '취약점 점검 및 모의침투테스트 수행 확인서'에 서명하여 제출하여야 합니다.

단, 확인서 제출 시 취약점 점검 세부 내역은 제출하지는 않아도 됩니다.

FAQ

Q.

(적용대상) 의료기관 내부에 의료기관이 직접 프라이빗 클라우드 환경을 구축하고, 해당 의료기관의 내부적으로 활용하는 경우는 S014 인증기준의 대상에서 제외된다고 하셨는데, 의료기관에서 보안 인증을 원하는 경우도 신청할 수 없나요?

A.

EMR 인증제는 자율적 참여이므로, 해당기관에서 원하는 경우 인증신청을 할 수 있습니다.

FAQ

Q.

(심사면제) 보안인증 3종 중에 일부만 있는 경우, 예를 들어 ISMS, ISO 27017은 제출가능하나 ISO 27018은 없는 경우는 어떻게 하나요?

A.

해당 기관에서 인증 신청을 하면, 보유하지 않은 보안인증에 대해 부가적으로 심사를 받아야 하는 증빙 목록과 준비사항을 정하여 인증기관이 신청기관에 별도 요청할 예정입니다.

FAQ

Q.

(의료정보시스템 보안) ISO 27799, HITRUST 등 국외 의료정보분야 보안인증을 제시하면 추가적인 면제 사항은 있나요?

A.

보건의료 분야 정보보호관리 요구사항의 준수를 검증하는 의료정보에 특화된 보안인증은 추후 반영 검토할 예정이며, 클라우드 EMR 등 '의료 클라우드 보안 가이드라인' 마련을 함께 검토할 예정에 있습니다.

FAQ

Q.

(인증기준) 인증기준 S014 제3호 (시범) 항목 “별도의 분리된 의료 전용 독립 네트워크 구성”은 필수로 받아야 하는 기준입니까?

A.

본 시범항목은 집적정보통신사업자가 EMR시스템을 구축 시, 인프라 내에서 의료 外 서비스와 물리적으로 분리된 네트워크를 구성토록 요청하는 기준입니다.

인증제 인증기준 내 ‘시범항목’은 인증기준을 적용하기 위한 기술적, 정책적 제반 환경 여건 미흡 등으로 시범적으로 운영하는 사항으로, 향후 현장 여건의 성숙 및 정책 방안 마련 후 본 항목으로 전환할 수 있습니다.

따라서 현재 S014 심사 패스를 위한 필수 항목은 아닙니다.

FAQ

Q.

ISO 27799(개인의료정보보호 국제표준) 공식 인증기준에서 제외되었나요?

A.

ISO 27799(보건의료정보보호) 표준은 현재 S014 인증기준 심사 시, 심사 일부 면제를 위한 보안인증서에서 제외되었습니다. 향후 연구를 통해 추가 반영 여부를 검토할 예정입니다.

FAQ

Q.

EMR 외부보관 사업자(예: 클라우드 EMR 개발업체)가 제품인증 신청을 하는 경우 Iaas + SaaS에 대한 "취약점 점검 및 모의테스트"를 "외부 전문서비스 기업" 통해 수행하길 권장받지만, 자체적인 수립/점검도 인증요건에 충족된다면 심사가 가능한지 궁금합니다.

A.

S014 인증심사 시 취약점 점검 및 모의해킹테스트 수행 확인서 제출이 필요하며, 자체적인 점검도 가능합니다. 단, 심사원이 수행 확인서에 대한 추가 검토가 필요한 경우 현장심사 등을 통해 추가 증빙자료를 요청할 수 있습니다.

감 사 합 니 다.