mcss

AKTIVITET

Misstänkta fall av läsning av patientuppgifter där patientrelation ej är självklar

Säker rapportering med MCSS Loggverktyg

Lagstiftningen ställer krav på regelbundna kontroller för att upptäcka om någon obehörig försöker komma åt sekretessbelagda personuppgifter. Dessa kontroller ska dokumenteras och vara utformade så att de kan utgöra ett underlag för utvärdering.

Med hjälp av Loggverktyget i MCSS kan lagkravet uppfyllas samtidigt som både informations- och patientsäkerheten förbättras. Rapporter som fås via Loggverktyget bildar ett värdefullt underlag för ett effektivt och systematiskt arbete med loggupp-följning.

SÅ HÄR FUNGERAR LOGGVERKTYGET

Varje månad skapas automatiskt en loggrapport där stickprov genomförs på persona-lens aktiviteter som rör åtkomst av patientuppgifter. Detta inkluderar:

- Åtkomst till patientens uppgifter som skett ett stort antal gånger.
- Intrångsförsök vid autentisering och låsningar av användarkonton.
- Åtkomst vid avvikande tidpunkter.
- Åtkomst vid boenden/enheter.
- Åtkomst till resurser som användaren inte är behörig till.
- Åtkomst till patients uppgifter via tredje land.
- Antal uttag av kontrolläkemedel i förhållande till signeringar.
- Sökningar på person av medialt intresse.
- Åtkomst till skyddade och/eller känsliga person-uppgifter som skett ett stort antal gånger.

2.1: 2022-03

forsaljning@appva.com
www.appva.com

appva
Part of Vitec Software Group

SP CERTIFIED ISO 27001 Information security management systems RI.SE

TEKNISK SPECIFIKATION

DRIFTSMILJÖ

MCSS IT-infrastruktur och drift är specifikt anpassad för att möta de legala krav, regelverk och rekommendationer som ställs på medicintekniska produkter inom vård och omsorg gällande informationssäkerhet.

TILLGÄNGLIGHET

MCSS levereras via en klustrad High-Availability (HA), lastbalanserad och redundant servermiljö. Normal tillgänglighet för MCSS är 99,5% beräknat på årsbasis.

AUTENTISERING

MCSS stödjer säker tvåfaktorsinloggning via tjänstelegitimation (SITHS) och möjliggör för federerad inloggning med Single Sign-On (SSO) integration.

LOGGNING

Loggning av åtkomstkontroll sker enligt Integritetsskyddsmyndighetens och Socialstyrelsens riktlinjer för kontroll av åtkomst.

AUKTORISERING

Administration av MCSS via enheter åtkomst- och behörighetskontrolleras via ett klientcertifikat knutet till verksamheten och utfärdat av Vitec Appva AB. Tillsammans möjliggör kombinationen av klientcertifikatet och slutanvändarens autentiseringsuppgifter att både verksamhet och Vitec Appva AB kan upprätthålla en fullständig kontroll över dels vilka slutanvändare och dels vilka enheter som är behöriga att få åtkomst till tjänsten.

SYSTEMKRAV

MCSS stödjer senaste version av Microsoft Edge, Google Chrome, Firefox, samt Safari på löpande basis samt senaste version av iOS och Android operativsystem.

2.1: 2022-03

forsaljning@appva.com
www.appva.com