

De veiligheid van de ZiZo-portal

In de ZiZo-portal van Zichtbare Zorg registreren zorginstellingen hun gegevens over de zorgkwaliteit. Lees hier welke maatregelen Zichtbare Zorg heeft getroffen om de veiligheid en privacy van deze gegevens te waarborgen.

1 Hoe worden 'ongewenste bezoekers' geweerd?

De ZiZo-portal wordt beschermd door een firewall, die ongewenst netwerkverkeer weert. De portal en de firewall worden regelmatig geüpdate, om ook de nieuwste virussen en aanvallen tegen te houden. De ZiZo-portal is alleen toegankelijk met een geldige gebruikersnaam en een wachtwoord. Het wachtwoord bestaat uit minimaal 6 tekens, een hoofdletter en cijfer. Instellingen beheren zelf de wachtwoorden van hun gebruikers. Deze worden niet centraal opgeslagen.

2 Wie kan gegevens zien/invoeren/wijzigen en (hoe) zijn die acties traceerbaar?

Alleen ingelogde gebruikers kunnen gegevens inzien, invoeren of wijzigen. Een ingelogde gebruiker heeft alleen toegang tot functionaliteiten en gegevens waarvoor hij rollen en rechten heeft gekregen van zijn of haar concernbeheerder. Acties waarmee een gebruiker gegevens in de ZiZo-portal wijzigt, worden vastgelegd. Op die manier kan desgewenst worden achterhaald wie wanneer welke actie heeft uitgevoerd. Dit is alleen mogelijk binnen de instellingen zelf door de concernbeheerder van die instelling. Alleen de actie zelf (of er bijvoorbeeld iets is toegevoegd of gewijzigd) wordt vastgelegd, wát er precies gewijzigd is niet.

3 Waar worden de gegevens opgeslagen?

Gegevens die in de ZiZo-portal worden ingevoerd, zowel gegevens voor de indicatoren als gegevens over de organisatie, worden opgeslagen op 'database-servers'. Een database server is een andere omgeving dan de omgeving waar de portal op draait (deze draait op een 'web-server'). Deze database server is niet toegankelijk vanaf het internet en wordt ook beschermd met een firewall.

4 Zijn de data ook beveiligd tijdens het transport van de web- naar de database-servers?

De data worden tijdens het transport van de web- naar de database-server versleuteld, zodat ze onleesbaar zijn. Hiervoor wordt gebruik gemaakt van een zogenaamde 'https'-verbinding. Pas bij aankomst op de server wordt de data ontcijferd.

Ook verwijzingen vanuit de ZiZo-portal naar de vragenlijstomgevingen zijn gecodeerd (64 bits DES encryptie algoritme). Alleen met een sleutelcode kan deze onleesbare verwijzing worden ontcijferd.

5 Kan achterhaald worden welke gegevens bij welke cliënt horen?

Bij een aantal sectoren moeten vragenlijsten van cliënten worden ingevoerd in de ZiZo-portal. Ook moeten de gegevens van de cliënten geregistreerd worden. Die gegevens en de vragenlijsten worden in aparte omgevingen (database-servers) opgeslagen. Dat maakt het onmogelijk te achterhalen welke gegevens bij welke cliënt horen. Alleen gebruikers die hier specifieke rechten voor hebben, bijvoorbeeld coördinatoren of invullers, kunnen zien welke gegevens bij welke cliënt horen omdat dit noodzakelijk is voor hun functie.