

Onderwerp	Eis
NEN7510 Certificering	Inschrijver voldoet aantoonbaar aan de informatiebeveiligingsnorm NEN7510 voor informatiebeveiliging in de zorg.
Classificatie van gegevens	GGD IJsselland hanteert een BIV classificatie Beschikbaarheid, Integriteit en Vertrouwelijkheid van 3,3,3. Op deze basis zijn maatregelen genomen op Beschikbaarheid, Integriteit en Vertrouwelijkheid.
Backup	Maatregelen zijn getroffen om minimaal een dagelijkse backup te realiseren.
Rapportage	Opdrachtgever wil periodiek de beschikking krijgen over een SLA rapportage over de uptime, eventueel onderhoud, verstoringen in de applicatie, en incidenten op het gebied van informatiebeveiliging, en de bijbehorende Root Cause Analyse (oorzaaksanalyse).
Rapportage	Er wordt periodiek (idealiter elk jaar) bewijslast aangeleverd aan opdrachtgever voor een uitgevoerde externe security test/penetratietest op de verwerking van laboratorium (of haar netwerkomgeving).
Logging en monitoring	De bewaartermijn van de samples wordt vastgesteld in samenspraak met Inschrijver.
Veilige connectiviteit	De HTTPS-configuratie voldoen aan de TLS-richtlijnen en Webapplicatie-richtlijnen van het Nationaal Cyber Security Centrum (NCSC). Inschrijver zorgt voor dit resultaat.
Veilige connectiviteit	Er dient ervoor te zorgen worden dat de gegevens van onze gebruikers veilig worden getransporteerd tussen waar deze wordt ingevoegd of wordt bekeken, en waar deze informatie wordt verwerkt of opgeslagen. Dit geldt ook voor interacties met derde partijen.
Veilige dataopslag	Alle opgeslagen gebruiker en clientgegevens worden versleuteld met behulp van de "Data in ruste encryptie" - zodat we er zeker van kunnen zijn dat deze informatie nutteloos is voor derde partijen bij diefstal.
Hosting	Opdrachtnemer garandeert dat persoonsgegevens altijd binnen de Europese Economische Ruimte (EER) wordt opgeslagen en altijd binnen de EER blijven. Er wordt voor de hosting gebruik gemaakt van partijen die hosten en verwerken binnen de geografische regio van de EER (Europa = voorkeur Nederland/Ierland/Duitsland). De configuratie moet zijn ingesteld op gegevensopslag en verwerking binnen die regio of combinatie van regio's.
Integriteit	Data binnen de (applicatie) omgeving is integer en wordt hierop gecontroleerd.
Integriteit	De koppelingen met derde partijen garanderen volledige en correcte gegevensoverdracht.
Archivering	De opdrachtnemer moet voldoen aan relevante wet- en regelgeving met betrekking tot archivering, waaronder wetten en voorschriften met betrekking tot gegevensbescherming, bewaartermijnen en toegang tot informatie.
Business Continuïteit	De continuïteit van de business is geborgd door een aantal (redundante) maatregelen op de applicatie.
OTAP	Op de OTA omgeving wordt niet gewerkt met productiegegevens. In alle gevallen wordt gewerkt met eigen aangemaakte of gepseudonimeerde en aangepaste gegevens waarbij een representatieve dataset wordt gecreëerd.
Logging	De applicatie beschikt over een functionele log waarbij de belangrijkste events voor inschrijver inzichtelijk zijn. Alle activiteiten zijn herleidbaar tot een natuurlijk persoon (gebruiker) of een geautomatiseerd proces.
Beschikbaarheid	Het beschikbaarheidspercentage van de uitwisseling van data is 99,8%, uitgezonderd hiervan is aangekondigd onderhoud of de verwerking door derde partijen in deze keten.