	Bij een architectuurtoets speelt de classificatie van het informatiesysteem een belangrijke rol bij de beoordeling van architectuur- en beveiligingsmaatregelen. In het BIA Advies geeft de ISO aan welke aandachtspunten specifiek aandacht dienen te krijgen.		
	Een voorbeeld vormt de verwerking van medische gegevens die vereist dat 2-factor authenticatie van kracht is bij de toegang tot deze gegevens.		
	Bij SaaS applicaties wordt de nadruk gelegd op het aantonen/laten bevestigen door leveranciers dat maatregelen zijn geimplementeerd.		
1	**Algemene eisen**		
Item	**Omschrijving van gestelde eis door Ziekenhuis Gelderse Vallei**	**Antwoord (ja/Nee/N.V.T)**	**Indien niet met Ja volstaan kan worden: Toelichting bij antwoord en/of referentie naar documentatie**
1.1	Datacenter heeft een tier 3 classificatie		
2	**Toegang**		
Item	**Omschrijving van gestelde eis door Ziekenhuis Gelderse Vallei**	**Antwoord (ja/Nee/N.V.T)**	
2.1	Security tokens ten behoeve van authenticatie worden geleverd via een Cloud Secure Token Service, Azure Active Directory (AAD) (indien AAD niet kan dan Active Directory Federation Services (ADFS)). Geldt alleen voor de zorgprofessional applicatie		
2.2	Federatieve Authenticatie protocollen voldoen aan SAML(v2) of OpenID Connect. Geldt alleen voor de zorgprofessional applicatie		
2.3	Eisen voor wachtwoorden voldoen aan de wachtwoord policy (Lengte minimaal 8, Complexe wachtwoorden, geldigheidsduur max 6 maanden, blokkeringsfactor bij 6 verkeerde pogingen) wanneer er geen gebruik wordt gemaakt van een koppeling met ZGV Azure-AD of ADFS.		
2.4	Leverancier biedt een 2-factor authenticatie mechanisme aan wanneer (bijzondere/medische) persoonsgegevens worden verwerkt en er geen gebruik kan worden gemaakt van ZGV Azure AD.		
3	**Koppelingen**		
Item	**Omschrijving van gestelde eis door Ziekenhuis Gelderse Vallei**	**Antwoord (ja/Nee/N.V.T)**	
3.1	Voor uitwisseling van gegevens wordt gebruik gemaakt van HL7 FHIR of HL7 v2.4 (of JSON/XML)		
3.2	Gegevensstromen zijn bekend en inzichtelijk. Laat dit zien in een plaat.		
3.3	Applicaties zijn voorzien van relevante API's (functionaliteit moet ontsloten/gebruikt kunnen worden middels een API/microservice)		
3.4	Indien er sprake is van dossiervoering zijn de gegevens benaderbaar vanuit het EPD		
4	**Database/gegevens opslag**		
Item	**Omschrijving van gestelde eis door Ziekenhuis Gelderse Vallei**	**Antwoord (ja/Nee/N.V.T)**	
4.1	(Bijzondere) persoonsgegevens worden versleuteld opgeslagen		
4.2	Elk gegeven is te herleiden tot op de individuele gebruiker en patiënt		
4.3	Wat is het maximale verlies aan gegevens gebaseerd op de gehanteerde backup/restore strategie? Geef inzicht in de backup/restore strategie?		
4.4	(Persoons)gegevens worden opgeslagen en verwerkt binnen de EU		
4.5	Geregistreerde data is op te slaan in nog te realiseren regionale data hub (moet dus voldoen aan landelijke standaarden o.a. Medmij)		
4.6	Data en functionaliteit zijn gescheiden van elkaar		
5	**(web)Applicatie**		
Item	**Omschrijving van gestelde eis door Ziekenhuis Gelderse Vallei**	**Antwoord (ja/Nee/N.V.T)**	
5.1	Voor kritische applicaties (Beschikbaarheid=Hoog), wordt een testomgeving beschikbaar gesteld om wijzigingen vooraf te testen.		
5.2	HTTP applicaties hebben minimaal een A-rating op SSLLABS.com		
5.3	DNSSEC wordt toegepast, toetsen met internet.nl		
5.4	Alle communicatie met- en tussen Webservices met vertrouwelijke informatie moet versleuteld plaats vinden via SSL verbinding (https) met minimaal TLS 1.2		
5.5	Gebruikerssessies worden automatisch na een vastgestelde tijd van inactiviteit automatisch verbroken (richtlijn is tussen 30 min a maximaal 60 minuten)		
5.6	De leverancier beschikt over een actief beleid voor het opsporen van tekortkomingen of kwetsbaarheden in de aangeboden dienst. Denk aan het uitvoeren van vulnerability scans of pentesten.		
5.7	Wijzigingen in informatiesystemen worden altijd op structurele wijze door leverancier getest.		
5.8	Belangrijke events worden gelogd (bewaartermijn is minimaal 1 jaar). Denk hierbij aan: ->activiteiten van (systeem)beheerders ->Inlog en uitlogsessies van gebruikers ->Wijzigingen in toegangsrechten binnen de applicatie ->acties van gebruikers binnen de applicatie		
5.9	Leverancier heeft een proces ingericht dat voorziet in een periodieke implementatie van patches om gebreken in gebruikte systeemsoftware te dichten. Belangrijke patches worden maandelijks uitgerold.		
5.10	Leverancier heeft een proces ingericht dat voorziet in een versnelde implementatie van (zeer) kritische patches om kwetsbaarheden met een hoog risico te dichten. Dergelijke (zeer) kritische patches worden binnen 1 week geimplementeerd.		

5.11	De applicatie (geldt alleen voor de zorgprofessional applicatie) kan in ieder geval in een Citrix Virtual Desktop (VDI omgeving) draaien gebaseerd op Windows Server 2016 en de volgende browsers worden ondersteunt: -Chrome versie N-1 en hoger (waarbij N de laatst beschikbare versie is) -Microsoft Edge (alle versies) -> Geef aan of er plug-ins worden gebruikt -> Geef aan of de applicatie op mobiele devices gebruikt kan worden en welke devices worden ondersteund		
5.12	De url van de dienst is indien gewenst bereikbaar onder door afnemer te bepalen url?		
5.13	Zijn de NCSC richtlijnen voor web applicaties gevolgd? (https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties)		
5.14	Applicaties zijn device aware (responsive)		