NEN 7510-1+A1:2020 and ISO/IEC 27001:2013/Cor 2:2015
Name of the organization: Roseman Labs B.V.
Date: 16-11-2023. **Version number**: 1.0

Beheersmaatregel	Omschrijving beheersmaatregel (ISO/IEC 27001) - NL	NEN7510 specific requirements? (ja/ Nee)	Zorgspecifieke beheersmaatregel	Van toepassing	Geimple-menteerd	Reden	Uitbesteed	Naam in eng	Omschrijving beheersmaatregel (ISO/IEC 27001) - ENG
A.5.1.1 Beleidsregels voor informatiebeveiliging	Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	Ja	Zorgspecifieke beheersmaatregel: Organisaties moeten beschikken over een schriftelijk informatiebeveiligingsbeleid dat door het management wordt goedgekeurd, wordt gepubliceerd en vervolgens wordt gecommuniceerd aan alle werknemers en relevante externe partii.	Ja	Ja	Wet- en regelgeving, contract, risicoanalyse	Nee	A. 5. 1. 1 Policies for information security	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.
A.5.1.2 Beoordelen van het informatie-beveiligingsbeleid	Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.	Ja	Zorgspecifieke beheersmaatregel: Het informatiebeveiligingsbeleid moet aan voortdurende, gefaseerde beoordelingen worden onderworpen zodat het volledige beleid ten minste eenmaal per jaar wordt beoordeeld. Het beleid moet worden beoordeeld als er zich een ernstig beveiligingsincident heeft voorgedaan.	Ja	Ja	Wet- en regelgeving, contract, risicoanalyse	Nee	A. 5. 1. 2 Review of the policies for information security	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
A.6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging	Alle verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen.	Ja	Zorgspecifieke beheersmaatregel: Organisaties moeten: a) duidelijk verantwoordelijkheden op het gebied van informatiebeveiliging definiëren en toewijzen; b) over een informatiebeveiligingsmanagementforum (IBMF) beschikken om te garanderen dat er duidelijke aansturing en zichtbare ondersteuning vanuit het management is voor beveiligingsinitiatieven die betrekking hebben op de beveiliging van gezondheidsinformatie, zoals beschreven in 8.3 en 8.4 van bijlage B (NEN 7510-2). Er moet minimaal één individu verantwoordelijk zijn voor beveiliging van gezondheidsinformatie binnen de organisatie. Het	Ja	Ja	Wet- en regelgeving, contract, risicoanalyse	Nee	A. 6. 1. 1 Information security roles and responsibilities	All information security responsibilities shall be defined and allocated.
A.6.1.2 Scheiding van taken	Conflicterende taken en verantwoordelijkheidsgebieden moeten worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.	Nee		Ja	Ja	Risicoanalyse, contract	Nee	A. 6. 1. 2 Segregation of duties	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
A.6.1.3 Contact met overheidsinstanties	Er moeten passende contacten met relevante overheidsinstanties worden onderhouden.	Nee		Ja	Ja	Risicoanalyse	Nee	A. 6. 1. 3 Contact with authorities	Appropriate contacts with relevant authorities shall be maintained.
A.6.1.4 Contact met speciale belangengroepen	Er moeten passende contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en professionele organisaties worden onderhouden.	Nee		Ja	Ja	Risicoanalyse	Nee	A. 6. 1. 4 Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.
A.6.1.5 Informatiebeveiliging in projectbeheer	Informatiebeveiliging moet aan de orde komen in projectbeheer, ongeacht het soort project.	Ja	Zorgspecifieke beheersmaatregel: Bij het management van projecten moet de patiëntveiligheid als projectrisico in aanmerking worden genomen voor elk project dat gepaard gaat met het verwerken van persoonlijke gezondheidsinformatie.	Ja	Ja	Risicoanalyse	Nee	A. 6. 1. 5 Information security in project management	Information security shall be addressed in project management, regardless of the type of the project.
A.6.2.1 Beleid voor mobiele apparatuur	Beleid en ondersteunende beveiligingsmaatregelen moeten worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren	Nee		Ja	Ja	Risicoanalyse	Nee	A. 6. 2. 1 Mobile device policy	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.
A.6.2.2 Telewerken	Beleid en ondersteunende beveiligingsmaatregelen moeten worden geïmplementeerd ter beveiliging van informatie die vanuf telewerklocaties wordt bereikt, verwerkt of opgeslagen.	Nee		Ja	Ja	Risicoanalyse	Nee	A. 6. 2. 2 Teleworking	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking.
A.7.1.1 Screening	Verificatie van de achtergrond van alle kandidaten voor een dienstverband moet worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en moet in verhouding staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's.	Ja	Zorgspecifieke beheersmaatregel: Organisaties moeten minimaal de identiteit, het huidige adres en de vorige werkkring van personeel en contractanten en vrijwilligers op het moment van de sollicitatie verifiëren. Verificatiecontroles van de achtergrond van alle kandidaten voor een dienstverband moeten een verificatie omvatten van de toepasselijke kwalificaties voor zorgverleners, indien er sprake is van accreditatie voor de beroepsgroep op basis van die kwalificaties (bijv. artsen, verpleegd personeel enz.). Als een persoon wordt ingehuurd voor een specifieke beveiligingsrol, moet de	Ja	Ja	Risicoanalyse, contract	Nee	A. 7. 1. 1 Screening	Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.
A.7.1.2 Arbeidsvoorwaarden	De contractuele overeenkomst met medewerkers en contractanten moeten hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie vermelden.	Ja	Zorgspecifieke beheersmaatregel: Alle organisaties waarvan personeelsleden betrokken zijn bij het verwerken van persoonlijke gezondheidsinformatie, behoren die betrokkenheid in relevante functieomschrijvingen vast te leggen. Beveiligingsrollen en verantwoordelijkheden, zoals vastgelegd in het informatiebeveiligingsbeleid van de organisatie, behoren ook in relevante functieomschrijvingen te worden vastgelegd. Er behoort speciale aandacht te worden besteed aan de rollen en verantwoordelijkheden van tijdelijk personeel of personeel met een kort dienstverband zoals vervangers, studenten,	Ja	Ja	Risicoanalyse	Nee	A. 7. 1. 2 Terms and conditions of employment	The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.
A.7.2.1 Directieverantwoordelijkheden	De directie moet van alle medewerkers en contractanten eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie	Nee		Ja	Ja	Risicoanalyse, contract	Nee	A. 7. 2. 1 Management responsibilities	Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.

A.7.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	Alle medewerkers van de organisatie en, voor zover relevant, contractanten moeten een passende bewustzijnsopleiding en -training krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.	Ja	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten garanderen dat onderwijs en training over informatiebeveiliging worden gegeven bij de introductie van nieuwe medewerkers en dat er regelmatig updates van beveiligingsbeleid en -procedures van de organisatie worden verstrekt aan alle werknemers en, indien relevant, derdecontractanten, onderzoekers, studenten en vrijwilligers die persoonlijke gezondheidsinformatie verwerken. Werknemers van de organisatie en, waar relevant, derde-contractanten moeten worden gewezen oo disciplinaire	Ja	Ja	Wet- en regelgeving, contract, risicoanalyse	Nee	A. 7.2.2 Information security awareness, education and training	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organisational policies and procedures, as relevant for their job function.
A.7.2.3 Disciplinaire procedure	Er moet een formele en gecommuniceerde disciplinaire procedure zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging.	Nee		Ja	Ja	Risicoanalyse	Nee	A. 7.2.3 Disciplinary process	There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.
A.7.3.1 Beëindiging of wijziging van verantwoordelijkheden van het dienstverband	Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband moeten worden gedefinieerd, gecommuniceerd aan de medewerker of contractant, en ten uitvoer worden gebracht.	Nee		Ja	Ja	Risicoanalyse	Nee	A. 7.3.1 Termination or change of employment responsibilities	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.
A.8.1.1 Inventariseren van bedrijfsmiddelen	Informatie, andere bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten, behoren te worden geïdentificeerd, en van deze bedrijfsmiddelen behoort een inventaris te worden opgesteld en onderhouden.	Ja	Zorgspecifieke beheersmaatregel: Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten: a) verantwoording afleggen over informatiebedrijfsmiddelen (d.w.z. een inventaris bijhouden van dergelijke bedrijfsmiddelen); b) een eigenaar hebben aangewezen voor deze informatiebedrijfsmiddelen (zie 8.1.2); c) regels hebben voor het aanvaardbare gebruik van deze bedrijfsmiddelen die geïdentificeerd, gedocumenteerd en geïmplementeerd worden.	Ja	Ja	Risicoanalyse	Nee	A. 8.1.1 Inventory of assets	Information, assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.
A.8.1.2. Eigendom van bedrijfsmiddelen	Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden moeten een eigenaar hebben.	Nee		Ja	Ja	Risicoanalyse	Nee	A. 8.1.2 Ownership of assets	Assets maintained in the inventory shall be owned.
A.8.1.3. Aanvaardbaar gebruik van bedrijfsmiddelen	Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten moeten regels worden geïdentificeerd, gedocumenteerd en geïmplementeerd.	Nee		Ja	Ja	Risicoanalyse	Nee	A. 8.1.3 Acceptable use of assets	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.
A.8.1.4 Teruggeven van bedrijfsmiddelen	Alle medewerkers en externe gebruikers moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst teruggeven.	Ja	Zorgspecifieke beheersmaatregel: Alle werknemers en contractanten moeten, na beëindiging van hun dienstverband, alle persoonlijke gezondheidsinformatie in niet-elektronische vorm die zij in hun bezit hebben, teruggeven en erop toezien dat alle persoonlijke gezondheidsinformatie in elektronische vorm die zij in hun bezit hebben, op relevante systemen wordt bijgewerkt en vervolgens op beveiligde wijze wordt gewist van alle apparaten waarop deze aanwezig was.	Ja	Ja	Risicoanalyse	Nee	A. 8.1.4 Return of assets	All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.
A.8.2.1 Classificatie van informatie	Informatie moet worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.	Ja	Zorgspecifieke beheersmaatregel: Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten dergelijke gegevens op uniforme wijze als vertrouwelijk classificeren.	Ja	Ja	Risicoanalyse	Nee	A. 8.2.1 Classification of information	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.
A.8.2.2 Informatie labelen	Om informatie te labelen moet een passende reeks procedures worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	Ja	Zorgspecifieke beheersmaatregel: Alle gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moeten de gebruikers wijzen op de vertrouwelijkheid van persoonlijke gezondheidsinformatie die toegankelijk is vanaf het systeem (bijv. bij het opstarten of inloggen), en moeten papieren output als vertrouwelijk labelen als die output persoonlijke gezondheidsinformatie bevat.	Ja	Ja	Risicoanalyse	Nee	A. 8.2.2 Labelling of information	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.
A.8.2.3 Behandelen van bedrijfsmiddelen	Procedures voor het behandelen van bedijfsmiddelen moeten worden ontwikkeld en geïmplementeerd in overeenstemming met het classificatieschema dat is vastgesteld door de organisatie.	Nee		Ja	Ja	Risicoanalyse	Nee	A. 8.2.3 Handling of assets	Procedures for handling assets shall be developed and implemented in accordance with the classification scheme adopted by the organization.
A.8.3.1 Beheer van verwijderbare media	Voor het beheren van verwijderbare media moeten procedures worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.	Ja	Zorgspecifieke beheersmaatregel: Media die persoonlijke gezondheidsinformatie bevatten, moeten fysiek worden beschermd of de gegevens ervan moeten versleuteld worden. De status en locatie van media die niet-versleutelde persoonlijke gezondheidsinformatie bevatten, moeten gemonitord worden.	Ja	Ja	Risicoanalyse	Nee	A. 8.3.1 Management of removable media	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization
A.8.3.2 Verwijderen van media	Media moeten op een veilige en beveiligde manier worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.	Ja	Zorgspecifieke beheersmaatregel: Alle persoonlijke gezondheidsinformatie moet veilig worden gewist of anders moeten de media worden vernietigd als ze niet meer gebruikt hoeven te worden.	Ja	Ja	Risicoanalyse	Nee	A. 8.3.2 Disposal of media	Media shall be disposed of securely when no longer required, using formal procedures.
A.8.3.3 Media fysiek overdragen	Media die informatie bevatten, moeten worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.	Nee		Ja	Ja	Risicoanalyse	Nee	A. 8.3.3 Physical media transfer	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.

A.9.1.1 Beleid voor toegangsbeveiliging	Een beleid voor toegangsbeveiliging moet worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.	Ja	Zorgspecifieke beheersmaatregel: Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten de toegang tot dergelijke informatie controleren. In het algemeen moeten de gebruikers van gezondheidsinformatiesystemen hun toegang tot persoonlijke gezondheidsinformatie beperken tot situaties: a) waarin er een zorgrelatie bestaat tussen de gebruiker en de persoon wiens de gegevens betrekking hebben (de cliënt tot wiens persoonlijke gezondheidsinformatie er toegang wordt gemaakt); b) waarin de gebruiker een activiteit uitvoert namens de persoon wiens de gegevens betrekking hebben; c) waarin er specifieke gegevens nodig zijn om deze activiteit te ondersteunen. Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten een toegangscontrolebeleid hebben waarmee de toegang tot dieregegevens wordt geregeld. Het beleid van de organisatie met betrekking tot toegangscontrole moet worden vastgesteld op basis van vooraf gedefinieerde rollen met bijbehorende bevoegdheden die passen bij, maar beperkt zijn tot, debehoeften van die rol. Het toegangscontrolebeleid, als bestanddeel van het in 5.1.1 beschreven beleidskader voor informatiebeveiliging, moet professionele, ethische, juridische en cliëntgerelateerde eisen weerspiegelen en moet de taken die worden uitgevoerd door zorgverleners, en de workflow van de taak in aanmerking nemen. De organisatie moet alle partijen identificeren en documenteren waarmee cliëntgegevens worden uitgewisseld, en met deze partijen moeten contractuele afspraken over toegang en rechten worden gemaakt, alvorens cliëntgegevens uit te wisselen.	Ja	Ja	Risicoanalyse, contract	Nee	A. 9. 1. 1 Access control policy	An access control policy shall be established, documented and reviewed based on business and information security requirements.
A.9.1.2 Toegang tot netwerken en netwerkdiensten	Gebruikers moeten alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	Nee		Ja	Ja	Risicoanalyse, contract	Nee	A. 9. 1. 2 Access to networks and network services	Users shall only be provided with access to the network and network services that they have been specifically authorized to use.
A.9.2.1 Registratie en afmelden van gebruikers	Een formele registratie- en uitschrijvingsprocedure moet worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	Ja	Zorgspecifieke beheersmaatregel: De toegang tot gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moet onderhevig zijn aan een formeel gebruikersregistratieproces. Procedures voor het registreren van gebruikers moeten garanderen dat het vereiste niveau van authenticatie van de geclaimde identiteit van gebruikers overeenkomt met het (de) toegangsniveau(s) waarover de gebruiker zal gaan beschikken. De gebruikersregistratiegegevens moeten regelmatig worden beoordeeld om te garanderen dat ze volledig en juist zijn en dat toegang nog altijd vereist is.	Ja	Ja	Wet- en regelgeving, contract, risicoanalyse	Nee	A. 9. 2. 1 User registration and de-registration	A formal user registration and de-registration process shall be implemented to enable assignment of access rights.
A.9.2.2 Gebruikers toegang verlenen	Een formele gebruikerstoegangsverleningsprocedure moet worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	Nee		Ja	Ja	Risicoanalyse, contract	Nee	A. 9. 2. 2 User access provisioning	A formal user access provisioning process shall be implemented to assign or revoke accesss rights for all user types to all systems and services.
A.9.2.3 Beheren van speciale toegangsrechten	Het toewijzen en gebruik van bevoorrechte toegangsrechten moet worden beperkt en gecontroleerd.	Nee		Ja	Ja	Risicoanalyse, contract	Nee	A. 9. 2. 3 Management of privileged access rights	The allocation and use of privileged access rights shall be restricted and controlled.
A.9.2.4 Beheer van geheime authenticatie-informatie van gebruikers	Het toewijzen van geheime authenticatie-informatie moet worden beheerst via een formeel beheerproces.	Nee		Ja	Ja	Risicoanalyse, contract	Nee	A. 9. 2. 4 Management of secret authentication information of users	The allocation of secret authentication information shall be controlled through a formal management process.
A.9.2.5 Beoordeling van toegangsrechten van gebruikers	Eigenaren van bedrijfsmiddelen moeten toegangsrechten van gebruikers regelmatig beoordelen.	Nee		Ja	Ja	Risicoanalyse, contract	Nee	A. 9. 2. 5 Review of user access rights	Asset owners shall review users' access rights at regular intervals.
A.9.2.6 Toegangsrechten intrekken of aanpassen	De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatieverwerkende faciliteiten moeten bij beëindiging van hun dienstverband, contract of overeenkomst worden verwijderd, en bij wijzigingen moeten ze worden aangepast.	Ja	Zorgspecifieke beheersmaatregel: Alle organisaties die persoonlijke gezondheidsinformatie verwerken, moeten voor elke vertrekkende afdelings- of tijdelijke medewerker, derde-contractant of vrijwilliger zo snel mogelijk na beëindiging van het dienstverband of de werkzaamheden als contractant of vrijwilliger de toegangsrechten als gebruikers tot dergelijke informatie beëindigen.	Ja	Ja	Risicoanalyse, contract	Nee	A. 9. 2. 6 Removal or adjustment of access rights	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.
A.9.3.1 Geheime authenticatie-informatie gebruiken	Van gebruikers moet worden verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie.	Nee		Ja	Ja	Risicoanalyse, contract	Nee	A. 9. 3. 1 Use of secret authentication information of users	Users shall be required to follow the organization's practices in the use of secret authentication information.
A.9.4.1 Beperking toegang tot informatie	Toegang tot informatie en systeemfuncties van applicaties moet worden beperkt in overeenstemming met het beleid voor toegangscontrole.	Ja	Zorgspecifieke beheersmaatregel: Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moeten de identiteit van gebruikers vaststellen en dit moet worden gedaan door middel van authenticatie waarbij ten minste twee factoren betrokken worden. De toegang tot functies van informatie- en toepassingssystemen in verband met het verwerken van persoonlijke gezondheidsinformatie moet geïsoleerd (en gescheiden) worden van de toegang tot informatieverwerkingsinfrastructuur die geen verband houdt met het verwerken van persoonlijke	Ja	Ja	Risicoanalyse, contract	Nee	A. 9. 4. 1 Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy.
A.9.4.2 Beveiligde inlogprocedures	Indien het beleid voor toegangsbeveiliging dit vereist, moet toegang tot systemen en toepassingen worden beheerst door een beveiligde inlogprocedure.	Nee		Ja	Ja	Wet- en regelgeving, contract, risicoanalyse	Nee	A. 9. 4. 2 Secure log-on procedures	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.
A.9.4.3 Systeem voor wachtwoordbeheer	Systemen voor wachtwoordbeheer moeten interactief zijn en sterke wachtwoorden waarborgen.	Nee		Ja	Ja	Risicoanalyse	Nee	A. 9. 4. 3 Password management system	Password management systems shall be interactive and shall ensure quality passwords.

A.9.4.4 Speciale systeemhulpmiddelen gebruiken	Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen moet worden beperkt en nauwkeurig worden gecontroleerd.	Nee		Ja	Ja	Risicoanalyse	Nee	A. 9.4.4 Use of privileged utility programs	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.
A.9.4.5 Toegangsbeveiliging op programmabroncode	Toegang tot de programmabroncode moet worden beperkt.	Nee		Ja	Ja	Risicoanalyse, contract	Nee	A. 9.4.5 Access control to program source code	Access to program source code shall be restricted.
A.10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen	Ter bescherming van informatie moet een beleid voor het gebruik van cryptografische beheersmaatregelen worden ontwikkeld en geïmplementeerd.	Nee		Ja	Ja	Wet- en regelgeving, contract, risicoanalyse	Nee	A. 10.1.1 Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.
A.10.1.2 Sleutelbeheer	Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels moet tijdens hun gehele levenscyclus een beleid worden ontwikkeld en geïmplementeerd.	Nee		Ja	Ja	Risicoanalyse, contract	Nee	A. 10.1.2 Key management	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle
A.11.1.1 Fysieke beveiligingszone	Beveiligingszones moeten worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten.	Ja	Zorgspecifieke beheersmaatregel: Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten gebruikmaken van beveiligde zones om gebieden te beschermen die informatieverwerkingsfaciliteiten bevatten die dergelijke gezondheidstoepassingen ondersteunen. Deze beveiligde gebieden moeten worden beschermd door passende beheersmaatregelen voor de fysieke toegang om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	Ja	Ja	Risicoanalyse	Nee	A. 11.1.1 Physical security perimeter	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.
A.11.1.2 Fysieke toegangsbeveiliging	Beveiligde gebieden moeten worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	Nee		Ja	Ja	Risicoanalyse	Nee	A. 11.1.2 Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
A.11.1.3 Kantoren, ruimten en faciliteiten beschermen	Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en toegepast.	Nee		Ja	Ja	Risicoanalyse	Gedeeltelijk	A. 11.1.3 Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and applied.
A.11.1.4 Beschermen tegen bedreigingen van buitenaf	Tegen natuurrampen, kwaadwillige aanvallen of ongelukken moet fysieke bescherming worden ontworpen en toegepast.	Nee		Ja	Ja	Risicoanalyse	Nee	A. 11.1.4 Protecting against external and environmental threats	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.
A.11.1.5 Werken in beveiligde gebieden	Voor het werken in beveiligde gebieden moeten procedures worden ontwikkeld en toegepast.	Nee		Ja	Ja	Risicoanalyse	Nee	A. 11.1.5 Working in secure areas	Procedures for working in secure areas shall be designed and applied.
A.11.1.6 Laad- en loslocatie	Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, moeten worden beheerst, en zo mogelijk worden afgeschermd van informatieverwerkende faciliteiten om onbevoegde toegang te vermijden.	Nee		Ja	Ja	Risicoanalyse, Uitbesteed proces	Gedeeltelijk	A. 11.1.6 Delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access
A.11.2.1 Plaatsing en bescherming van apparatuur	Apparatuur moet zo worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.	Nee		Ja	Ja	Risicoanalyse	Gedeeltelijk	A. 11.2.1 Equipment siting and protection	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
A.11.2.2 Nutsvoorzieningen	Apparatuur moet worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.	Nee		Ja	Ja	Risicoanalyse	Gedeeltelijk	A. 11.2.2 Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.
A.11.2.3 Beveiliging van bekabeling	Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen interceptie, verstoring of schade	Nee		Ja	Ja	Risicoanalyse	Nee	A. 11.2.3 Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.

A.11.2.4 Onderhoud van apparatuur	Apparatuur moet correct worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.	Nee		Ja	Ja	Risicoanalyse	Nee	A. 11.2.4 Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity.
A.11.2.5 Verwijdering van bedrijfsmiddelen	Apparatuur, informatie en software mogen niet van de locatie worden meegenomen zonder voorafgaande goedkeuring.	Ja	Zorgspecifieke beheersmaatregel: Organisaties die uitrusting, gegevens of software voor het ondersteunen van een zorgtoepassing met persoonlijke gezondheidsinformatie leveren of gebruiken, mogen niet toestaan dat die uitrusting, gegevens of software van de locatie wordt of worden verwijderd of erbinnen wordt of worden verplaatst zonder dat de organisatie hiervoor haar goedkeuring heeft gegeven	Ja	Ja	Risicoanalyse	Nee	A. 11.2.5 Removal of assets	Equipment, information or software shall not be taken off-site without prior authorization.
A.11.2.6 Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	Bedrijfsmiddelen die zich buiten het terrein bevinden, moeten worden beveiligd, waarbij rekening moet worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.	Nee		Ja	Ja	Risicoanalyse	Nee	A. 11.2.6 Security of equipment and assets off-premises	Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.
A.11.2.6 Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein - zorgspecifieke beheersmaatregel	N/A	Ja	Zorgspecifieke beheersmaatregel: Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten garanderen dat het eventuele gebruik buiten hun gebouw van medische apparaten die worden gebruikt om gegevens te registreren of te rapporteren, geautoriseerd is. Dit moet apparatuur omvatten die door werknemers op afstand wordt gebruikt, zelfs indien dit gebruik permanent is (d.w.z. waar het een kernaspect is van de rol van de werknemer, zoals het geval is bij ambulancepersoneel, therapeuten enz.	Nee	Nee	Roseman Labs is geen zorginstantie en heeft geen medische apparatuur	N.v.t.	N/A	N/A
A.11.2.7 Veilig verwijderen of hergebruiken van apparatuur	Alle onderdelen van de apparatuur die opslagmedia bevatten, moeten worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of veilig zijn overschreven.	Ja	Zorgspecifieke beheersmaatregel: Organisaties die gezondheidsinformatie verwerken, moeten alle media met toepassingssoftware voor gezondheidsinformatie of persoonlijke gezondheidsinformatie erop veilig wissen of vernietigen als ze niet meer gebruikt hoeven te worden.	Ja	Ja	Risicoanalyse	Nee	A.11.2.7 Secure disposal or re-use of equipment	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior or re-use.
A.11.2.8 Onbeheerde gebruikersapparatuur	Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is.	Nee		Ja	Ja	Risicoanalyse	Nee	A.11.2.8 Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.
A.11.2.9 'Clear desk'- en 'clear screen'-beleid	Er moet een 'clean desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatieverwerkende faciliteiten worden ingesteld.	Nee		Ja	Ja	Risicoanalyse	Nee	A.11.2.9 Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.
A.12.1.1 Gedocumenteerde bedieningsprocedures	Bedieningsprocedures moeten worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze nodig hebben.	Nee		Ja	Ja	Risicoanalyse, contract	Nee	A.12.1.1 Documented operating procedures	Operating procedures shall be documented and made available to all users who need them.
A.12.1.2 Wijzigingsbeheer	Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging moeten worden beheerst.	Ja	Zorgspecifieke beheersmaatregel: Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten de veranderingen aan informatieverwerkingsfaciliteiten en systemen die persoonlijke gezondheidsinformatie verwerken, door middel van een formeel en gestructureerd wijzigingsbeheersproces beheersen om de gepaste beheersing van hosttoepassingen en -systemen en de continuïteit van de cliëntenzorg te waarderen.	Ja	Ja	Risicoanalyse	Nee	A.12.1.2 Change management	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.
A.12.1.3 Capaciteitsbeheer	Het gebruik van middelen moet worden gemonitord en afgestemd, en er moeten verwachtingen worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.	Nee		Ja	Ja	Risicoanalyse	Nee	A.12.1.3 Capacity management	The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.
A.12.1.4 Scheiding van ontwikkel-, test- en productieomgevingen	Ontwikkel-, test- en productieomgevingen moeten worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	Ja	Zorgspecifieke beheersmaatregel: Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten ontwikkel- en testomgevingen voor gezondheidsinformatiesystemen die dergelijke informatie verwerken (fysiek of virtueel), scheiden van operationele omgevingen waar die gezondheidsinformatiesystemen gehost worden. Er moeten regels voor het migreren van software van de ontwikkel naar een operationele status worden gedefinieerd en gedocumenteerd door de organisatie die de betreffende toewassingen host.	Ja	Ja	Risicoanalyse	Nee	A.12.1.4 Separation of development, testing and operational environments	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environmental.
A.12.2.1 Beheersmaatregelen tegen malware	Ter bescherming tegen malware moeten beheersmaatregelen voor detectie, preventie en herstel worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.	Ja	Zorgspecifieke beheersmaatregel: Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten gepaste preventie-, detectie- en responsbeheersmaatregelen implementeren om bescherming te bieden tegen kwaadaardige software en en moeten passende bewustzijnstraining voor gebruikers implementeren.	Ja	Ja	Risicoanalyse	Nee	A.12.2.1 Controls against malware	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.
A.12.3.1 Back-up van informatie	Regelmatig moeten back-up kopieën van informatie, software en systeemafbeeldingen worden gemaakt en getest in overeenstemming met een overeengekomen back-up beleid.	Ja	Zorgspecifieke beheersmaatregel: Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten back-ups maken van alle persoonlijke gezondheidsinformatie en deze in een fysiek beveiligde omgeving opslaan om te garanderen dat de informatie in de toekomst beschikbaar is. Om de vertrouwelijkheid ervan te beschermen moeten er versleutelde back-ups worden gemaakt van persoonlijke gezondheidsinformatie.	Ja	Ja	Risicoanalyse, contract	Nee	A.12.3.1 Information backup	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.

A.12.4.1 Gebeurtenissen registreren	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, moeten worden gemaakt, bewaard en regelmatig worden beoordeeld.	Nee		Ja	Ja	Wet- en regelgeving, contract, risicoanalyse	Nee	A.12.4.1 Event logging	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.
A.12.4.2 Beschermen van informatie in logbestanden	Logfaciliteiten en informatie in logbestanden moeten worden beschermd tegen vervalsing en onbevoegde toegang.	Ja	Zorgspecifieke beheersmaatregel: Auditverslagen moeten beveiligd zijn en mogen niet gemanipuleerd kunnen worden. De toegang tot hulpmiddelen voor audits van systemen en audittrajecten moet worden beveiligd om misbruik of compromitterinte voorkomen.	Ja	Ja	Wet- en regelgeving, contract, risicoanalyse	Nee	A.12.4.2 Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.
A.12.4.3 Logbestanden van beheerders en operators	Activiteiten van systeembeheerders en -operators moeten worden vastgelegd en de logbestanden moeten worden beschermd en regelmatig worden beoordeeld.	Nee		Ja	Ja	Risicoanalyse, contract	Nee	A.12.4.3 Administrator and operator logs	⠀ System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.
A.12.4.4 Kloksynchronisatie	De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein moeten worden gesynchroniseerd met één referentietijdbron.	Ja	Zorgspecifieke beheersmaatregel: Gezondheidsinformatiesystemen die tijdkritische activiteiten voor gedeelde zorg ondersteunen, moeten in tijdsynchronisatiediensten voorzien om het traceren en reconstrueren van de tijdlijnen voor activiteiten waar vereist te ondersteunen.	Ja	Ja	Risicoanalyse	Nee	A.12.4.4 Clock synchronization	The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to a single reference time source.
A.12.5.1 Software installeren op operationele systemen	Om het op operationele systemen installeren van software te beheersen moeten procedures worden geïmplementeerd.	Nee		Ja	Ja	Risicoanalyse	Nee	A.12.5.1 Installation of software on operational systems	Procedures shall be implemented to control the installation of software on operational systems.
A.12.6.1 Beheer van technische kwetsbaarheden	Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt moet tijdig worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden moet worden geëvalueerd en passende maatregelen moeten worden genomen om het risico dat ermee samenhangt aan te pakken.	Nee		Ja	Ja	Risicoanalyse, contract	Nee	A.12.6.1 Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.
A.12.6.2 Beperkingen voor het installeren van software	Voor het door gebruikers installeren van software moeten regels worden vastgesteld en geïmplementeerd.	Nee		Ja	Ja	Risicoanalyse	Nee	A.12.6.2 Restrictions on software installation	Rules governing the installation of software by users shall be established and implemented.
A.12.7.1 Beheermaatregelen betreffende audits van informatiesystemen	Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, moeten zorgvuldig worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren.	Nee		Ja	Ja	Risicoanalyse, contract	Nee	A.12.7.1 Information system audit controls	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes.
A.13.1.1 Beheersmaatregelen voor netwerken	Netwerken moeten worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	Nee		Ja	Ja	Risicoanalyse	Nee	A.13.1.1 Network controls	Networks shall be managed and controlled to protect information in systems and applications.
A.13.1.2 Beveiliging van netwerkendiensten	Beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle netwerkdiensten moeten worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	Nee		Ja	Ja	Risicoanalyse, contract	Nee	A.13.1.2 Security of network services	Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.
A.13.1.3 Scheiding in netwerken	Groepen van informatiediensten, -gebruikers en -systemen moeten in netwerken worden gescheiden.	Nee		Ja	Ja	Risicoanalyse, contract	Nee	A.13.1.3 Segregation in networks	Groups of information services, users and information systems shall be segregated on networks.
A.13.2.1 Beleid en procedures voor informatietransport	Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, moeten formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht zijn.	Nee		Ja	Ja	Wet- en regelgeving, risicoanalyse	Nee	A.13.2.1 Information transfer policies and procedures	Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.
A.13.2.2 Overeenkomsten over informatietransport	Overeenkomsten moeten betrekking hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.	Nee		Ja	Ja	Risicoanalyse	Nee	A.13.2.2 Agreements on information transfer	Agreements shall address the secure transfer of business information between the organization and external parties.

A.13.2.3 Elektronische berichten	Informatie die is opgenomen in elektronische berichten moeten passend beschermd zijn.	Nee		Ja	Ja	Risicoanalyse	Nee	A.13.2.3 Electronic messaging	Information involved in electronic messaging shall be appropriately protected.
A.13.2.4 Vertrouwelijkheids- of geheimhoudingsovereenkomst	Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen moeten worden vastgesteld, regelmatig worden beoordeeld en gedocumenteerd.	Ja	Zorgspecifieke beheersmaatregel: Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten beschikken over een vertrouwelijkheidsovereenkomst waarin de vertrouwelijke aard van de ze informatie staat omschreven. De overeenkomst moet van toepassing zijn op al het personeel dat toegang heeft tot gezondheidsinformatie.	Ja	Ja	Risicoanalyse	Nee	A.13.2.4 Confidentiality or non-disclosure agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.
A.14.1.1 Beveiligingseisen van informatiesystemen	De eisen met betrekking tot informatiebeveiliging worden opgenomen in de eisen voor nieuwe informatiesystemen of verbeteringen aan bestaande informatiesystemen.	Nee		Ja	Ja	Risicoanalyse	Nee	A.14.1.1 Security requirements of information systems	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.
A.14.1.1.1 Zorgontvangers op unieke wijze identificeren	De eisen die verband houden met informatiebeveiliging moeten worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.	Ja	Zorgspecifieke beheersmaatregel: Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moeten: a) zeker stellen dat elke cliënt op unieke wijze kan worden geïdentificeerd binnen het systeem; b) in staat zijn dubbele of meerdere registraties samen te voegen indien wordt vastgesteld dat er onbedoeld meer registraties voor dezelfde cliënt zijn aangemaakt, of tijdens een medisch noodgeval.	Nee	Nee	Roseman Labs faciliteert geen gezondheids-informatie systemen in het primaire zorgproces	N.v.t.	N/A	N/A
A.14.1.1.2 Validatie van outputgegevens	N/A	Ja	Zorgspecifieke beheersmaatregel: Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moeten voorzien in persoonsidentificatie-informatie die zorgverleners helpt bevestigen dat de opgevraagde elektronische gezondheidsregistratie overeenkomt met de cliënt die wordt behandeld.	Ja	Ja	Risicoanalyse	Nee	N/A	N/A
A.14.1.2 Toepassingen op openbare netwerken beveiligen	Informatie die deel uitmaakt van uitwisselingsdiensten en die via openbare netwerken worden uitgewisseld, moet worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.	Nee		Ja	Ja	Risicoanalyse	Nee	A.14.1.2 Securing application services on public networks	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.
A.14.1.3 Transacties van toepassingen beschermen	Informatie die deel uitmaakt van transacties van toepassingsdiensten moet worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.	Nee		Ja	Ja	Risicoanalyse	Nee	A.14.1.3 Protecting application services transactions	Information involved in applications service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
A.14.1.3.1 Openbaar beschikbare gezondheidsinformatie	N/A	Ja	Openbaar beschikbare gezondheidsinformatie (niet zijnde persoonlijke gezondheidsinformatie) moet worden gearchiveerd. De integriteit van openbaar beschikbare gezondheidsinformatie moet worden beschermd om onbevoegde wijzigingen te voorkomen. De bron (auteurschap) van	Nee	Nee	Roseman Labs publiceert zelf geen gezondheidsinformatie.	N.v.t.	N/A	N/A
A.14.2.1 Beleid voor beveiligd ontwikkelen	Voor het ontwikkelen van software en systemen moeten regels worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie worden toegepast	Nee		Ja	Ja	Risicoanalyse	Nee	A.14.2.1 Secure development policy	Rules for the development of software and systems shall be established and applied to developments within the organization.
A.14.2.2 Procedures voor wijzigingsbeheer met betrekking tot systemen	Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling moeten worden beheerst door het gebruik van formele controleprocedures voor wijzigingsbeheer.	Nee		Ja	Ja	Risicoanalyse	Nee	A.14.2.2 System change control procedures	Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.
A.14.2.3 Technische beoordeling van toepassingen na wijzigen besturingsplatform	Als bedieningsplatforms zijn veranderd, moeten bedrijfskritische toepassingen worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of de beveiliging van de organisatie.	Nee		Ja	Ja	Risicoanalyse	Nee	A.14.2.3 Technical review of applications after operating platform changes	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.
A.14.2.4 Beperkingen op wijzigingen aan softwarepakketten	Wijzigingen aan softwarepakketten moeten worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen moeten strikt worden gecontroleerd.	Nee		Ja	Ja	Risicoanalyse	Nee	A.14.2.4 Restrictions on changes to software packages	Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.
A.14.2.5 Principes voor engineering van beveiligde systemen	Principes voor de engineering van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen.	Nee		Ja	Ja	Wet- en regelgeving, contract, risicoanalyse	Nee	A.14.2.5 Secure system engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.

A.14.2.6 Beveiligde ontwikkelomgeving	Organisaties moeten beveiligde ontwikkelomgevingen vaststellen en passend beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.	Nee		Ja	Ja	Risicoanalyse	Nee	A.14.2.6 Secure development environment	Organisations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.
A.14.2.7 Uitbestede softwareontwikkeling	Uitbestede systeemontwikkeling moet onder supervisie staan van en worden gemonitord door de organisatie.	Nee		Ja	Ja	Risicoanalyse	Nee	A.14.2.7 Outsourced development	The organization shall supervise and monitor the activity of outsourced system development.
A.14.2.8 Testen van systeembeveiliging	Tijdens ontwikkelactiviteiten moet de beveiligingsfunctionaliteit worden getest.	Nee		Ja	Ja	Risicoanalyse, contract	Nee	A.14.2.8 System security testing	Testing of security functionality shall be carried out during development.
A.14.2.9 Systeemacceptatietests	Voor nieuwe informatiesystemen, upgrades en nieuwe versies moeten programma's voor het uitvoeren van acceptatietests en gerelateerde criteria worden vastgesteld. Zorgspecifieke beheersmaatregel: Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten acceptatiecriteria vaststellen voor geplande nieuwe informatiesystemen, upgrades en nieuwe versies. Voorafgaand aan acceptatie moeten ze geschikte tests van het systeem uitvoeren. Klinische gebruikers moeten worden	Nee		Ja	Ja	Risicoanalyse	Nee	A.14.2.9 System acceptance testing	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.
A.14.3.1 Bescherming van testgegevens	Testgegevens moeten zorgvuldig worden gekozen, beschermd en gecontroleerd.	Nee		Ja	Ja	Risicoanalyse	Nee	A.14.3.1 Protection of test data	Test data shall be selected carefully, protected and controlled.
A.15.1.1 Informatiebeveiligingsbeleid voor leveranciersrelaties	Met de leverancier moeten de informatiebeveiligingseisen om risico's te verlagen, die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, worden overeengekomen en gedocumenteerd.	Ja	Zorgspecifieke beheersmaatregel: Organisaties die gezondheidsinformatie verwerken, moeten de risico's in verband met toegang door externe partijen tot deze systemen of gegevens die zij bevatten, beoordelen en vervolgens beveiligingsbeheersmaatregelen implementeren die bij het geïdentificeerde risiconiveau en de toegepaste technologieën passen.	Ja	Ja	Wet- en regelgeving, contract, risicoanalyse	Nee	A.15.1.1 Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.
A.15.1.2 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	Alle relevante informatiebeveiligingseisen moeten worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.	Nee		Ja	Ja	Contract, risicoanalyse	Nee	A.15.1.2 Addressing security within supplier agreements	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.
A.15.1.3 Toeleveringsketen van informatie- en communicatietechnologie	Overeenkomsten met leveranciers moeten eisen bevatten die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie-en communicatie technologie.	Nee		Ja	Ja	Contract, risicoanalyse	Nee	A.15.1.3 Information and communication technology supply chain	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.
15.2.1 Monitoring en beoordeling van dienstverlening van leveranciers	Organisaties moeten regelmatig de dienstverlening van leveranciers monitoren, beoordelen en auditen.	Nee		Ja	Ja	Risicoanalyse	Nee	A.15.2.1 Monitoring and review of supplier services	Organizations shall regularly monitor, review and audit supplier service delivery.
15.2.2 Beheer van veranderingen in dienstverlening van leveranciers	Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, moeten worden beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.	Nee		Ja	Ja	Risicoanalyse	Nee	A.15.2.2 Managing changes to supplier services	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.
A.16.1.1 Verantwoordelijkheid en procedures	Directieverantwoordelijkheden en -procedures moeten worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.	Nee		Ja	Ja	Risicoanalyse	Nee	A.16.1.1 Responsibilities and procedures	Management responsibilities and procedure shall be established to ensure a quick, effective and orderly response to information security incidents.
A.16.1.2 Rapportage van informatiebeveiligingsgebeurtenissen	Informatiebeveiligingsgebeurtenissen moeten zo snel mogelijk via de juiste leidinggevende niveaus worden gerapporteerd.	Ja	Zorgspecifieke beheersmaatregel: Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten verantwoordelijkheden en procedures met betrekking tot het managen van beveiligingsincidenten vaststellen: a) om een doeltreffende en tijdige respons op informatiebeveiligingsincidenten te bewerkstelligen; b) om te garanderen dat er een doeltreffend en geprioriteerd escalatiepad is voor incidenten zodat in de juiste omstandigheden en tijdig een beroep kan worden gedaan op plannen voor crisismanagement en bedrijfscontinuïteitsmanagement; c) om incidentgerelateerde auditverslagen en ander relevant bewijs te verzamelen en in stand te houden. Informatiebeveiligingsincidenten omvatten corruptie of onbedoelde openbaarmaking van persoonlijke gezondheidsinformatie of het niet langer beschikbaar zijn van gezondheidsinformatiesystemen waarbij dit niet beschikbaar zijn nadelige gevolgen heeft voor de zorg voor cliënten of bijdraagt aan nadelige klinische gebeurtenissen.	Ja	Ja	Risicoanalyse, contract	Nee	A.16.1.2 Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.

A.16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging	Van medewerkers en contractanten die gebruik maken de informatiesystemen en -diensten van de organisatie moet worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.	Nee		Ja	Ja	Risicoanalyse, contract	Nee	A.16.1.3 Reporting information security weaknesses	Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.
A.16.1.4 Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen	Informatiebeveiligingsgebeurtenissen moeten worden beoordeeld en er moet worden geoordeeld of zij moeten worden geclassificeerd als informatie-beveiligingsincidenten.	Nee		Ja	Ja	Risicoanalyse	Nee	A.16.1.4 Assessment of and decision on information security events	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.
A.16.1.5 Respons op informatiebeveiligingsincidenten	Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.	Nee		Ja	Ja	Risicoanalyse	Nee	A.16.1.5 Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.
A.16.1.6 Lering uit informatiebeveiligingsincidenten	Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen moet worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.	Nee		Ja	Ja	Risicoanalyse	Nee	A.16.1.6 Learning from information security incidents	Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.
A.16.1.7 Verzamelen van bewijsmateriaal	De organisatie moet procedures definiëren en toepassen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.	Nee		Ja	Ja	Wet- en regelgeving, contract, risicoanalyse	Nee	A.16.1.7 Collection of evidence	The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.
A.17.1.1 Informatiebeveiligingscontinuiteit plannen	De organisatie moet haar eisen voor informatiebeveiliging en voor de continuiteit van het informatiebeveiligingsbeheer in ongunstige situaties bijv. een crisis of een ramp vaststellen.	Nee		Ja	Ja	Risicoanalyse	Nee	A.17.1.1 Planning information security continuity	The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.
A.17.1.2 Informatiebeveiligingscontinuiteit implementeren	De organisatie moet processen, procedures en beheersmaatregelen vaststellen, documenteren, implementeren en handhaven om het vereiste niveau van continuiteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.	Nee		Ja	Ja	Risicoanalyse	Nee	A.17.1.2 Implementing information security continuity	The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.
A.17.1.3 Informatiebeveiligingscontinuiteit verifiëren, beoordelen en evalueren	De organisatie moet de ten behoeve van informatiebeveiligingscontinuiteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.	Nee		Ja	Ja	Risicoanalyse	Nee	A.17.1.3 Verify, review and evaluate information security continuity	The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.
A.17.2.1 Beschikbaarheid van informatieverwerkende faciliteiten	Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	Nee		Ja	Ja	Risicoanalyse	Gedeeltelijk	A.17.2.1 Availability of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.
A.18.1.1 Vaststellen van toepasselijke wetgeving en contractuele eisen	Alle relevante wettelijke, statutaire, regelgevende, contractuele eisen en de aanpak van de organisatie om aan deze eisen te voldoen moeten voor elk informatiesysteem en de organisatie expliciet worden vastgesteld, gedocumenteerd en actueel gehouden.	Nee		Ja	Ja	Wet- en regelgeving	Nee	A.18.1.1 Identification of applicable legislation and contractual requirements	All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.
A.18.1.2 Intellectuele-eigendomsrechten	Om de naleving van wettelijke, regelgevende en contractuele eisen in verband met intellectuele eigendomsrechten en het gebruik van eigendomssoftwareproducten te waarborgen moeten passende procedures worden geïmplementeerd.	Nee		Ja	Ja	Risicoanalyse	Nee	A.18.1.2 Intellectual property rights	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.
A.18.1.3 Beschermen van registraties	Registraties moeten in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.	Nee		Ja	Ja	Risicoanalyse	Nee	A.18.1.3 Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.
A.18.1.4 Privacy en bescherming persoonsgegevens	Privacy en bescherming van persoonsgegevens moeten voor zover van toepassing, worden gewaarborgd in overeenstemming met relevante wet-en regelgeving.	Nee		Ja	Ja	Risicoanalyse	Nee	A.18.1.4 Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.

A.18.1.4 Privacy en bescherming persoonsgegevens -zorgspecifieke beheersmaatregel	N/A	Ja	Zorgspecifieke beheersmaatregel: Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten de geïnformeerde toestemming van cliënten beheren. Waar mogelijk moet geïnformeerde toestemming van cliënten worden verkregen voordat persoonlijke gezondheidsinformatie per -mail, fax of telefonisch wordt gecommuniceerd of anderszins bekend wordt gemaakt aan partijen buiten de zorginstelling.	Nee	Nee	Het beheer van toestemming van cliënten is de verantwoordelijkheid van onze klanten.	N.v.t.	N/A	N/A
A.18.1.5 Voorschriften voor het gebruik van cryptografische beheersmaatregelen	Cryptografische beheersmaatregelen moeten worden toegepast in overeenstemming met alle relevante overeenkomsten, wet-en regelgeving.	Nee		Ja	Ja	Risicoanalyse	Nee	A.18.1.5 Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.
A.18.2.1 Onafhankelijke beoordeling van informatiebeveiliging	De aanpak van de organisatie ten aanzien van beheer van informatiebeveiliging en de implementatie ervan (bijv. beheersdoelstellingen, beheersmaatregelen, beleidsregels, processen en procedures voor informatiebeveiliging), moeten onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen worden beoordeeld.	Nee		Ja	Ja	Risicoanalyse, contract	Nee	A.18.2.1 Independent review of information security	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.
A.18.2.2 Naleving van beveiligingsbeleid en -normen	Leidinggevenden moeten regelmatig de naleving van de informatieverwerking en -procedures binnen hun verantwoordelijkheidsgebied beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	Nee		Ja	Ja	Risicoanalyse, contract	Nee	A.18.2.2 Compliance with security policies and standards	Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.
A.18.2.3 Beoordeling van technische naleving	Informatiesystemen moeten regelmatig worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.	Nee		Ja	Ja	Risicoanalyse, contract	Nee	A.18.2.3 Technical compliance review	Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.