StrokeViewer Security Whitepaper

INLEIDING

Deze whitepaper gaat in op de regelgeving en beveiliging rondom StrokeViewer. StrokeViewer is door Nico.lab ontworpen voor het verzenden en analyseren van radiologische beelden met (verdenking op) een acute beroerte. De gegevens die StrokeViewer verwerkt zijn een vorm van bijzondere persoonsgegevens, namelijk patiëntgegevens. Deze gegevens zijn gevoelig en vallen onder de Algemene Verordening Gegevensbescherming (AVG) en de Wet op Geneeskundige Behandelingsovereenkomst (WGBO). Het belang van informatiebeveiliging rondom het beheren en uitwisselen van patiëntengegevens is evident. De combinatie van een geavanceerd dataverkeersysteem met een werkwijze conform Nederlandse standaarden en frequente controles stelt Nico.lab in staat te voldoen aan de veeleisende verplichtingen rondom beveiliging van patiëntgegevens.

RELEVANTE WETGEVING

WGBO en AVG

De gegevens die StrokeViewer verwerkt in de Nico.lab cloud-omgeving vallen onder het medisch beroepsgeheim. De Wet op Geneeskundige Behandelingsovereenkomst (WGBO) geldt zodra er een behandelingsovereenkomst is tussen een zorgverlener en een cliënt, en stelt onder andere het medisch beroepsgeheim vast. Sinds 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG), oftewel de General Data Protection Regulation [GDPR] in de Europese Unie van kracht.[1] Volgens de AVG is het gebruik van de cloud voor het opslaan en verwerken van patiëntengegevens toegestaan.[2] De privacyregels zoals beschreven in de WGBO blijven ook na de introductie van de AVG van kracht. Het ziekenhuis als verantwoordelijke, Nico.lab als verwerker, en de cloudprovider als sub-verwerker zijn allen verplicht deze regels na te leven. Zij zijn samen rechtstreeks betrokken bij de uitvoering van de behandeling van de patiënt en vallen zodoende ook onder het medisch beroepsgeheim. Alle relevante rollen volgens de AVG worden weergegeven in **Tabel 1.**

Toestemming van de patiënt

Volgens de AVG is het niet nodig om toestemming te vragen aan de patiënt om beelden te laten analyseren en te verzenden met StrokeViewer. Artikel 7:457 Burgerlijk Wetboek bepaalt namelijk dat patiëntgegevens zonder toestemming mogen worden verstrekt aan ‘degenen die rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst’. De autoriteit persoonsgegevens beschouwt StrokeViewer als een entiteit die patiëntgegevens verwerkt voor de zorgaanbieder als ‘rechtstreeks betrokken bij de uitvoering van de behandelingsovereenkomst’. Ook het medisch beroepsgeheim in de WGBO schrijft in deze situatie niet voor dat hiervoor expliciet toestemming moet worden gevraagd aan de patiënt.

> Note: Meer informatie over de AVG kunt u vinden op:
> https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving/algemene-informatie-avg

Tabel 1. Relevante rollen en begrippen volgens de AVG

De patiënt	Alle gegevens die zijn terug te voeren tot de patiënt, zijn privacygevoelig, en blijven eigendom van de patiënt. Dit is niet van toepassing op geanonimiseerde data.
Verwerkingsverantwoordelijke	De verwerkingsverantwoordelijke is degene die 'het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt'. De verantwoordelijke bepaalt welke persoonsgegevens, voor welk doel, op welke manier en met welke middelen worden verwerkt.[2] Het ziekenhuis is in de meeste gevallen de verwerkingsverantwoordelijke gezien deze verantwoordelijk is voor het beheren en beschermen van patiëntgegevens.
Verwerker	Nico.lab – de verwerker – verwerkt in opdracht van een verwerkingsverantwoordelijke (zoals een ziekenhuis) de patiëntgegevens. Er is sprake van verwerking van persoonsgegevens, al dan niet automatisch uitgevoerd, bij het 'verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen' van de patiëntgegevens.
Verwerkersovereenkomst	De rechtsverhouding tussen verantwoordelijke en bewerker wordt vastgelegd in een verwerkersovereenkomst. Nico.lab stelt dit op met uw ziekenhuis. Hierin maken beide partijen afspraken over de verwerking van de data.
Derde of sub-verwerker	Een cloudprovider die servers aan Nico.lab beschikbaar stelt (bijv. Google Cloud) is in dit scenario een derde partij, of sub-verwerker, gezien deze niet de verantwoordelijke noch directe verwerker van de persoonsgegevens zijn. De sub-verwerker heeft met de verwerker (Nico.lab) een schriftelijke overeenkomst afgesloten die aansluit op de verwerkersovereenkomst tussen het ziekenhuis en Nico.lab. Wanneer de sub-verwerker tekortschiet in de nakoming van de overeenkomst dan blijft Nico.lab ten aanzien van de verwerkingsverantwoordelijke volledig aansprakelijk.

Verantwoordelijkheden Nico.lab

Het ziekenhuis dat van StrokeViewer gebruikt maakt is volgens de wet verwerkingsverantwoordelijke, met bijbehorende verantwoordelijkheden. Verwerkers mogen uitsluitend handelen in opdracht van de verwerkersverantwoordelijke. Binnen de AVG wordt aan de verwerker een grote verantwoordelijkheid toegekend. In de verwerkersovereenkomst tussen het participerende ziekenhuis en Nico.lab wordt vastgelegd hoe concreet aan de AVG zal worden voldaan Nico.lab zorgt onder meer voor:

1. **Privacy-by-design:** Het verwerken van patiëntengegevens neemt risico's met zich mee. Daarom zorgt Nico.lab zowel technisch als organisatorisch in een vroeg stadium voor zorgvuldige omgang met persoonsgegevens en de nodige aandacht voor privacy. Intern heeft Nico.lab een procedure voor het faciliteren van de rechten van de betrokkenen. StrokeViewer zal daarnaast buiten de noodzakelijke radiologische beelden en de bijbehorende DICOM-informatie geen andere patiëntengegevens opslaan. Deze data wordt automatisch verwijderd op het aangegeven termijn in de verwerkersovereenkomst. Ook hebben alle betrokken werknemers bij Nico.lab en bij haar sub-verwerkers een geheimhoudingsverklaring getekend om vertrouwelijkheid in acht te nemen. Door middel van hoogwaardige informatiebeveiliging voldoet Nico.lab aan de wettelijk verplichte bescherming van patiëntengegevens.
2. **Inlichtingen:** Nico.lab dient het participerende ziekenhuis in te lichten over het inschakelen van nieuwe sub-verwerkers. Nico.lab zal nooit een samenwerking aangaan met een nieuwe sub-verwerker zonder schriftelijke toestemming. In het onwaarschijnlijke geval dat er een datalek plaatsvindt wordt dit onverwijld aan het ziekenhuis gemeld. Het ziekenhuis als verwerkingsverantwoordelijke blijft vallen onder de meldplicht datalekken, en zal dit binnen 72 uur na bewustwording moeten melden aan de Autoriteit Persoonsgegevens.
3. **Documentatie en zorgplicht:** Nico.lab houdt een register bij van alle verwerkingscategorieën die ten behoeve van u zijn verricht. Nico.lab heeft tevens een zorgplicht en dient het participerende ziekenhuis bijstand te verlenen bij het nakomen van de verplichtingen. Voorbeelden hiervan zijn zaken omtrent de beveiliging en het uitvoeren van een Privacy Impact Assessment (PIA). Nico.lab staat ook open voor medewerking aan (onafhankelijke) audits en relevante verzoeken van de Autoriteit Persoonsgegevens.

DATABEVEILIGING

Door de implementatie van een Information Security Management System (ISMS) tracht Nico.lab te voldoen aan de hoogste standaarden omtrent databeveiliging, en onze kernwaarde bij de ontwikkeling van StrokeViewer is 'security-by-design'. In **Tabel 2** staan de belangrijkste beveiligingsfuncties weergegeven die van toepassing zijn op StrokeViewer.

Tabel 2. Beveiligingsfuncties van StrokeViewer

Beveiligingsfunctie	*StrokeViewer*	*Voordeel*
Stapverificatie (two-factor authentication)	Stapverificatie voor gevoelige acties, zoals bijvoorbeeld het veranderen van de pipeline en het configureren van data	Vertrouwelijkheid van het hoogste niveau
Inlogbeleid (Login policy)	Wachtwoord, verlengingsperiode en inactiviteit-time-out van de webviewer	Vertrouwelijkheid van het hoogste niveau
Audit trailing	Alle acties binnen het platform worden geregistreerd	Garandeert dat aan de wettelijke vereisten wordt voldaan
Data encryptie	Alle gegevens worden versleuteld '*in transit*' (TLS) alsmede in opslag '*at rest*' (AES 256/128). Verder wordt in geval van een datalek de functionaris gegevensbescherming gewaarschuwd en worden de betreffende gegevens in quarantaine geplaatst. Zodra de oorzaak is bepaald, wordt passende actie ondernomen.	Beveiligde overdracht via internet en bij verwerking en opslag in de cloud

Cloud-omgeving van StrokeViewer

Nico.lab heeft gekozen voor een stabiele, snelle en veilige manier van gegevensverwerking en heeft daarom StrokeViewer ontworpen op basis van een cloud-model (**figuur 1**). Het unieke cloud-model van StrokeViewer verzekert:

- Schaalbaarheid**.** Door het inzetten van een parallelle analyse pipeline op verschillende Virtual Machines (VM). Wanneer er meer rekenkracht nodig is kan er snel een extra VM worden opgestart. Dit ondersteunt de analyse van grote gegevenssets zonder de verwerkingsduur, latentie of efficiëntie in gevaar te brengen.
- Snelheid. StrokeViewer maakt gebruik van Tensor Processing Units (TPU); TPU is een AI-accelerator application-specific integrated circuit (ASIC), speciaal ontwikkeld door Google voor het uitvoeren van machine learning met neurale netwerken. De combinatie van StrokeViewer's hoogstaande AI-algoritmen met TPU's zorgt voor een zeer snel analyseresultaat, wat cruciaal is tijdens een acute beroerte.
- Beschikbaarheid. Nico.lab is uiterst zorgvuldig bij het selecteren van betrouwbare cloud-providers en kijkt hierbij naar beschikbaarheid, continuïteit en beveiliging. In tegenstelling tot een lokale server in het ziekenhuis, kan de cloud-server niet zomaar uitvallen en daardoor onbereikbaar zijn. StrokeViewer stuurt met de beelden altijd een zogenaamde 'life-line' mee, en kan zo in de gaten houden of er een VM uitvalt. In het onwaarschijnlijke geval dat dit gebeurt, wordt er snel volledig automatisch een nieuwe VM opgestart.
- Continue geoptimaliseerde AI-algoritmen. Nico.lab kan snel en makkelijk verandering doorvoeren in StrokeViewer en is door het cloudmodel sterk configureerbaar, flexibel en uitbreidbaar. Zo kan Nico.lab verzekeren dat StrokeViewer is ten alle tijden is uitgerust met de meest recente en best geteste algoritmen.
- Sterke beveiliging. Vertrouwelijkheid van gevoelige informatie wordt vaak geïdentificeerd als een belangrijke risicofactor in de context van een cloud-omgeving. De gegevens die door StrokeViewer worden verwerkt zullen worden versleuteld en verspreid over verschillende dataopslagplaatsen. Hierdoor zal er nooit een complete set gegevens op één plaats aanwezig zijn, maar altijd gefragmenteerd. De gegevens zullen na afloop van de termijn die is opgenomen in de

verwerkersovereenkomst weer automatisch verwijderd worden uit de cloud. Naast gegevensversleuteling 'in transit' en 'at rest' heeft Nico.lab een inlogbeleid geïmplementeerd om de toegang tot zijn platform te beperken.

De cloud-omgeving waar StrokeViewer gebruik van maakt zal altijd binnen de grenzen van de EU gevestigd zijn, en in de landen waar de AVG van toepassing is. Dit is van essentieel belang om te voldoen aan de Nederlandse wettelijke vereisten, die stelt dat gegevens de EU niet mogen verlaten en moeten worden geëxploiteerd in overeenstemming met Nederlandse voorschriften inzake dataprivacy.

Bij de verwerking van patiëntengegevens moet de cloudinfrastructuur altijd beschikbaar, snel en sterk beveiligd zijn. Daarom selecteert Nico.lab zorgvuldig een betrouwbare datacenterpartners dat garanties biedt op het gebied van beschikbaarheid en voldoet aan beveiligingsvereisten. De specifieke vereisten hebben betrekking op beschikbaarheid, integriteit, vertrouwelijkheid, transparantie, gegevensisolatie, portabiliteit en aansprakelijkheid.

Vertrouwelijkheid van gevoelige informatie wordt vaak geïdentificeerd als een belangrijke risicofactor in de context van een cloud omgeving. Om de vertrouwelijkheid van alle gegevens die in StrokeViewer worden verwerkt te waarborgen, worden de gegevens zowel '*in transit*' (onderweg van de Nico.lab server naar gebruiker en vice versa) als '*at rest*' (in opslag) gecodeerd. Naast gegevensversleuteling heeft Nico.lab de nodige toegangscontroles geïmplementeerd om de toegang tot het platform te beperken. Gezien het doel van Nico.lab's cloud-gebaseerde analyseplatform, is het garanderen van een hoge mate van vertrouwelijkheid een uiterst belangrijk onderdeel bij het definiëren van de keuze van een serviceprovider. Daarom wordt de vertrouwelijkheid verder verzekerd door middel van identiteits- en toegangsbeheer, met behulp van hoogwaardige autorisatie- en authenticatiemechanismen. Tevens zijn alle werknemers en contractanten van Nico.lab gebonden door vertrouwelijkheidsverplichtingen.

RELEVANTE NORMEN

Er zijn meerdere normen opgesteld die de implementatie van de AVG in de zorgsector ondersteunen. Deze zogenaamde Nederlandse Normen (NEN) zijn een concrete invulling van de wereldwijde ISO-normen en Europese CEN-normen op het gebied van informatiebeveiliging in de zorg. Ze bieden een kader voor beveiliging van persoonsgegevens, toegespitst op de Nederlandse situatie.[3] Voor StrokeViewer zijn de volgende normen relevant:

- NEN 7510:2017: Informatiebeveiliging in de Zorg, afgeleid van ISO 27001 (Information Technology)
- NEN 7512:2017: Medische informatica - Informatiebeveiliging in de zorg - Vertrouwensbasis voor gegevensuitwisseling

NEN 7510

De NEN 7510 is een uitwerking van de ISO 27001, 27002 en 27017, en is primair toegespitst op de Nederlandse zorgsector. Het is daarom ook de belangrijkste Nederlandse privacy-standaard voor organisaties die met patiëntgegevens omgaan. Deze norm is toegesneden op informatiebeveiliging binnen de gezondheidszorg en behelst het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van alle informatie ten behoeve van verantwoorde patiëntenzorg. Naast het borgen van kwaliteit moeten de informatiebeveiligingsmaatregelen volgens de norm zo zijn ingericht dat deze te controleren zijn. In de NEN 7510 wordt tevens aandacht besteed aan de inrichting van de Information Security Management System (ISMS) zoals ook gehanteerd door Nico.lab, en voor verder risicomanagement. Per fase (*Plan, Do, Check* en *Act*) is beschreven welke stappen genomen moet worden. Met de norm wordt een goede basis gelegd voor de inrichting van de ISMS, en kan de beveiliging van gegevens worden gestructureerd, gehandhaafd en waar nodig verscherpt. De belangrijkste implicatie van de NEN 7510 voor Nico.lab is beveiliging van de cloud-omgeving. Nico.lab en StrokeViewer functioneren conform de NEN 7510 en dit wordt door een onafhankelijke instantie gecertificeerd. Aangezien Nico.lab de ontwikkelaar van StrokeViewer is, zal zij verantwoordelijk zijn voor het implementeren van de NEN 7510. Nico.lab schrijft deze eisen ook voor aan haar leveranciers, en gaat alleen contracten aan met de leveranciers die hieraan

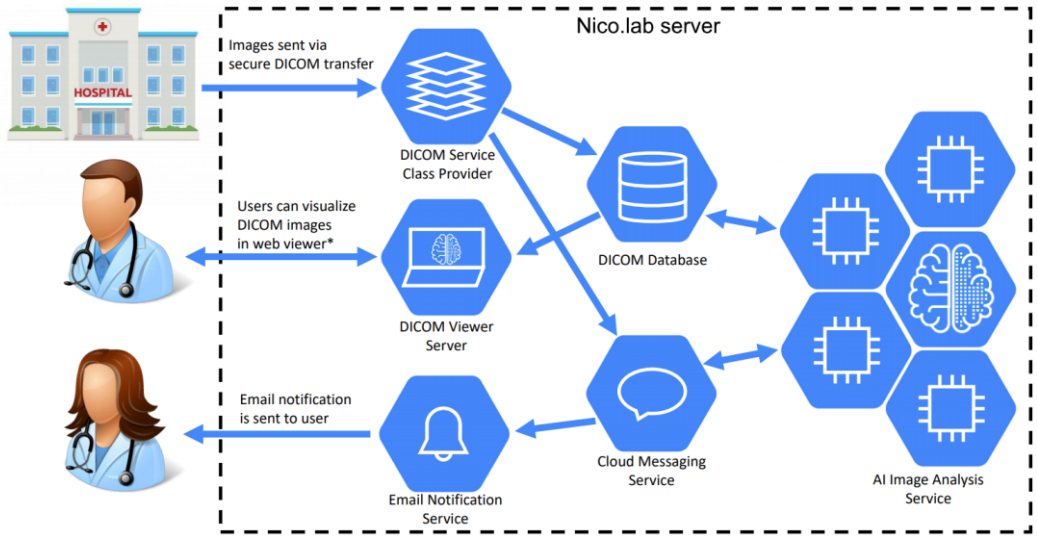
voldoen. De NEN 7510 bevat ook concrete richtlijnen voor het gebruik van een cloud. In de overeenkomst die Nico.lab heeft met de cloudprovider, wordt vastgesteld dat deze aan de richtlijnen voldoet (en blijft voldoen). Ten slotte zal Nico.lab hier regelmatig op controleren.

NEN 7512

De NEN 7512 sluit aan op de NEN 7510. Deze schrijft een beveiligde gegevensoverdracht tussen ziekenhuis en de externe server voor. In de praktijk schrijft deze norm voor hoe de uitwisseling van beelden tussen het werkstation en de cloud zo veilig mogelijk plaats kan vinden. Nico.lab draagt er zorg voor dat de gegevens alleen kunnen worden ingezien door de personen die daarvoor bevoegd zijn, en dat de viewer automatisch uitlogt als deze een paar minuten niet wordt gebruikt.

PRODUCTVEILIGHEID

StrokeViewer is CE klasse 1 gecertificeerd en daarmee een verondersteld veilig product. Met deze certificering toont Nico.lab aan dat onze algoritmes klinisch zijn gevalideerd en voldoen aan de 'Medical Devices Directive' (MDD 93/42/EEC)[4]. Door middel van constante risicoanalyse en kwaliteitsmanagement systemen wordt de veiligheid van het product gewaarborgd.



Figuur 1. Schematisch overzicht van de cloudinfrastructuur van StrokeViewer.

Note: Meer informatie omtrent de NEN 7510 en haar aanvullingen is te vinden op:
https://www.nen.nl/Alles-over-NEN-7510.htm
https://www.werkenmetnen7510.nl

REFERENTIES

1. *Autoriteit Persoonsgegevens - Algemene Informatie AVG*. https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving/algemene-informatie-avg.
2. *Autoriteit Persoonsgegevens - Praktijkgids Patiëntgegevens in de Cloud*. https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/praktijkgids_patientgegevens_in_de_cloud_def.pdf.
3. *Hoe Ondersteunen Normen de Implementatie van de AVG in de Zorg?* https://www.nen.nl/web/file?uuid=7708176b-077e-4eae-9ac7-60018b085b23&owner=8c53c600-a0c7-4552-b616-1965c7cca6cd.
4. *Medical Devices - Council Directive 93/42/EEC of 14 June 1993 Concerning Medical Devices OJ L 169 of 12 July 1993*. https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/medical-devices_en.

VOORWAARDEN

Handelsmerk

StrokeViewer is een handelsmerk van Nico-lab B.V., een besloten vennootschap met beperkte aansprakelijkheid, geregistreerd te Paasheuvelweg 25, 1105 BP, Amsterdam, Nederland.

Vertrouwelijkheid

Dit document bevat eigendomsrechten en vertrouwelijke informatie van Nico.lab. De ontvanger mag dit document niet aan derden verspreiden zonder toestemming van Nico.lab.

Belangrijke notitie

Er kunnen geen rechten worden ontleend aan dit document. Dit document wordt uitsluitend ter informatie verstrekt, is niet bindend en mag niet worden opgevat als een verplichting, verklaring of garantie. Hoewel Nico.lab uiterste zorg heeft besteed aan het verstrekken van juiste, volledige en actuele informatie, kan Nico.lab niet garanderen dat deze whitepaper vrij is van fouten. De informatie in dit document is de laatst beschikbare informatie op de datum van productie en kan van tijd tot tijd veranderen. Let op: Nico.lab's services en producten evolueren in de loop van de tijd. Als u wilt controleren of de informatie in dit document nog steeds geldig is, neem dan contact op met Nico.lab

Over ons:

Nico.lab richt zich op het verbeteren van de zorg bij beroertes door middel van AI-ondersteunde beeldanalyses. Onze baanbrekende technologie maakt een snelle en nauwkeurige analyse mogelijk die artsen helpt bij het nemen van weloverwogen beslissingen. Nico.lab heeft StrokeViewer® ontwikkeld om het complexe proces van klinische besluitvorming te ondersteunen in een wereld waar elke minuut telt

Nico·lab

Lees meer op:

www.nico-lab.com

Contact:

Amsterdam Health and Technology Center (AHTC)
Paasheuvelweg 25-Wing 5C
1105BP Amsterdam
info@nico-lab.com | +31 20 244 0852