*Vertaald door Deepl zonder nalezing*

**Ethiek WG 19/5/2025**

**Ontmoeting met Dr Pierre-Jean Verheyden, DPO-CISO in het Centre Hospitalier Interrégional Edith Cavell (CHIREC)**

*Zie ook Dr. Verheyden's PPT.*

Dr. P.-J. Verheyden (PJV) is arts en coördinator van de implementatie van het elektronisch medisch dossier. Onlangs werd hij DPO en vervolgens CISO (hoofd cyberbeveiliging). Als DPO is hij verantwoordelijk voor het vervolg van de IT ACT en de nieuwe normen.

PJV: AI is een hulpmiddel. Ziekenhuizen en zorgverleners hebben in het verleden al andere hulpmiddelen gebruikt (robots). Zorgverleners worden voortdurend getraind om de best mogelijke kwaliteit te garanderen.

AI is een verzameling gegevens die wordt vertaald in algoritmen om versterkte menselijke intelligentie te simuleren. Het is een verzameling regels die machines vertellen hoe ze hun taken moeten uitvoeren. AI heeft een grote hoeveelheid informatie nodig en maakt vaak gebruik van de cloud. Er verandert voortdurend veel. Het is noodzakelijk om voortdurend up-to-date te blijven.

De principes die bij AI in acht moeten worden genomen, zijn :

* VEILIGHEID ;
* transparantie (= het verstrekken van de best mogelijke informatie, maar hulpmiddelen zijn overal en het is moeilijk om je de toekomst voor te stellen in een context van voortdurende revolutie in hulpmiddelen);
* bescherming tegen discriminerende vooroordelen (controle van de gebruikte AI en controle van de bronnen: smalle AI (afbeeldingen) gebruiken smalle informatie terwijl generatieve AI zoeken naar informatie in databases waarvan de bronnen niet worden gecontroleerd);
* de invoering van controles om de verantwoording van besluiten te waarborgen ;
* inclusie en gelijkheid voor iedereen garanderen.

De Europese context is gestandaardiseerd: gegevensbescherming, NIS2-wetgeving (voor de beveiliging van informatiesystemen). Dit creëert een nalevingslast. De *AI-functionaris* is verantwoordelijk voor het AI-register, risicobeoordeling en -beheer, naleving, opleiding van personeel en vervolg en audit van de geïmplementeerde AI-systemen. Dit is een taak waarvoor ziekenhuizen geen geld krijgen, terwijl de normen steeds strenger worden.

AI in de gezondheidszorg?

AI in de gezondheidszorg gaat niet alleen over zorg. AI dringt door in alle dienstverlenende structuren van ziekenhuizen (inclusief administratie). Het komt tegemoet aan de behoeften van zorgverleners. Bijvoorbeeld:

* Voor grote dossiers (800 pagina's) waarvoor het moeilijk is om alle gegevens op te zoeken en te controleren. AI maakt het mogelijk om oplossingen te vinden die tijd besparen en de patiëntenzorg verbeteren.
* Eerste AI = medische beeldvorming (smalle AI).
* Operatierobots (bewegingsbeheer): prestaties verbeteren.
* Farmacologie.
* Patiëntenbewaking op afstand en detectie van anomalieën (bijv. vallen).

Training voor zorgpersoneel?

Training voor personeel in de gezondheidszorg gaat niet alleen over AI. Het gaat over voortdurende training voor alle technologische ontwikkelingen. Want het principe is dat wanneer een AI-systeem wordt geïmplementeerd, er altijd menselijk toezicht is om de output te controleren. Je moet dus de capaciteit hebben om dit te doen. Dit vereist aanpassing van het personeel en dus een verplichting om training te geven binnen ziekenhuizen.

Transparantie in diagnostiek?

Wanneer AI-systemen worden geïmplementeerd, zullen artsen zich moeten aanpassen door te leren nadenken over wat de AI voorstelt en om de bronnen te controleren (met de moeilijkheid van generatieve AI). Kwaliteitscontroles worden geïmplementeerd. Er worden vergelijkingen gemaakt met bestaande of menselijke oplossingen. Soms is dit niet overtuigend, dus wordt de AI verlaten. De CHIREC controleert AI in projectmodus en kijkt naar de RGPD, cyberbeveiliging en effectiviteit: we controleren de bronnen van de gecontroleerde gegevens en de controle van de algoritmen; we beoordelen de risico's (als er risico's zijn, worden specifieke controles georganiseerd; als er hoge risico's zijn, wordt AI verboden). Artsen moeten toegang hebben tot implementatie-informatie, zien hoe de algoritmen werken en deelnemen aan interacties met ontwikkelaars tijdens de implementatie.

Ethische principes bij het gebruik van AI?

* Welwillendheid: AI verbetert de prestaties.
* Patiënteninformatie.
* Autonomie van de patiënt.
* Geïnformeerde toestemming: de patiënt moet het gebruik van AI kunnen begrijpen en er vrijwillig mee instemmen.

Het bestuur vindt plaats op het niveau van het Uitvoerend Comité.

Invloed op de medische praktijk?

AI verandert de praktijk en maakt tijd vrij voor patiëntenzorg. De relatie tussen patiënt en arts verandert: enerzijds wordt de arts geholpen door de AI om het dossier bij te werken, anderzijds communiceert de arts met de patiënt over het soort hulpmiddel dat wordt gebruikt. De relatie moet er een van vertrouwen zijn. De patiënt blijft de baas over zijn of haar beslissing.

PMH?

Mensen met een PMH mogen niet worden uitgesloten. Toegang moet gegarandeerd zijn voor alle patiënten. Sommige onderzoeken vereisen inclusie van bepaalde profielen, afhankelijk van het onderhouden van het onderzoek. Gelijke behandeling moet echter gegarandeerd zijn.

Discriminatie?

Ja, die zijn er, maar we moeten ze kunnen analyseren en controleren. Dit vereist menselijke controle van de kwaliteit van AI. Zie hierboven het projectmanagement bij CHIREC, met een ja/nee-beslissing.

Toestemming voor onderzoeksprogramma's?

Patiënten hebben het recht om hun toestemming in te trekken. Hierop wordt toegezien door ethische commissies. Uitzondering: hergebruik van gezondheidsgegevens, maar dit is nog niet duidelijk. De RGPD blijft de basis. Hier komt de verplichting vandaan om een DPO in ziekenhuizen te hebben en een *IT-functionaris* om risico's te monitoren. We moeten kijken hoe ziekenhuizen gefinancierd kunnen worden voor deze werklast. Onderzoek staat onder toezicht van ethische commissies. Secundaire gegevens worden geanonimiseerd. Deze kwestie wordt momenteel besproken.

Wie verzamelt de gegevens? De zorgverlener. De gegevens worden verwerkt door de verantwoordelijke voor de verwerking (behandelend arts). De instelling heeft een verplichting om de gegevens te beschermen. Dit is een algemene wettelijke verplichting, niet alleen gekoppeld aan AI. Wanneer gegevens naar generatieve AI worden gestuurd, moeten ze worden geanonimiseerd.

De principes van beroepsgeheim en vertrouwelijkheid blijven ongewijzigd. Dit is een zaak voor het wetboek van strafrecht. Het is de verantwoordelijkheid van de arts om deze vertrouwelijkheid niet te schenden. Daarom moeten we controle uitoefenen op de manier waarop AI gegevens gebruikt. Dit kan leiden tot veroordelingen.

Uitdagingen van het gebruik van AI?

* Controleren.
* Gebruik de kans om de zorg te verbeteren.
* Governance-verantwoordelijkheid: ervoor zorgen dat de principes van verantwoordingsplicht, transparantie, naleving van de wet en respect voor mensen en gegevens worden nageleefd.
* Verplichting voor ziekenhuizen om gegevens actueel te houden en te beschermen (robuustheidsprincipe). Bestrijding van cyberaanvallen (Wet NIS2).
* IT ACT.
* Toezicht door het Centre for Cybersecurity Belgium (CCB).

Gegevens worden 30 tot 50 jaar bewaard. Dit beperkt het recht van de patiënt om zijn gegevens te laten verwijderen. Maar het recht op correctie bestaat wel. Hier blijft het toezicht menselijk. Er is (nog) geen AI om dit te doen.

Beheren en bijwerken van gegevens in het datawarehouse van het ziekenhuis

1. Wie identificeert fouten?

Wanneer de AI is geïmplementeerd, wordt het gereedschap gecontroleerd. Het prestatieniveau wordt gecertificeerd. Bij CHIREC werkt dit in projectmodus (zie hierboven), als onderdeel van een continu verbeteringsproces, omdat AI voortdurend in ontwikkeling is. Dit vereist transparantie en voortdurende audits.

1. Gegevensopslag

Huisartsen spelen een rol in het behandelingsproces. Gegevens worden verzonden via *hubs*. Dossiers worden gedeeld met toestemming van de patiënt. Als de huisarts niet meewerkt, heeft de patiënt gegarandeerd toegang. Verpleegkundigen, fysiotherapeuten, apothekers, enz. hebben ook toegang. Is coördinatie zonder huisarts mogelijk in een sterk geautomatiseerd ziekenhuis? De toekomst zal het uitwijzen. Voorlopig is het bij afwezigheid van een huisarts aan de patiënt om zijn of haar gegevens door te geven aan de juiste partij. Geconfronteerd met de vooroordelen en hallucinaties van AI, moeten we deze vergelijken met onze eigen kennis en onze kritische geest alert houden.

1. Gegevensbescherming

De RGPD blijft de basis. Ter bescherming tegen cyberaanvallen wordt de toegang tot gegevens beperkt, gecontroleerd en onderworpen aan tweefactorauthenticatie. De naleving van de regelgeving is doorlopend.

Vrij verkeer van gegevens?

Het doel is om Belgische en Europese gezondheidsinstanties toegang te geven tot de gegevens. Deze gegevens zijn secundair en geanonimiseerd zodat ze gebruikt kunnen worden voor testen. Hiervoor moet een systeem worden opgezet voor opt-in/opt-out van patiënten. Deelname is cruciaal als ons land wil profiteren van de vooruitgang in de productie van nieuwe geneesmiddelen.

Gegevens commercialiseren?

Nog niet geïmplementeerd. Dit vereist een opt-in/out van de patiënt. Patiënten moeten ervan bewust worden gemaakt dat hun gegevens kunnen helpen om de volksgezondheid te verbeteren. Er zijn bijeenkomsten over dit onderwerp. Dit vereist governance door de instellingen en hangt af van het besluit van de voor de verwerking verantwoordelijken.

Wolk?

Niet alle ziekenhuizen gebruiken de cloud. In dit geval worden de gegevens opgeslagen op de servers. De cloud maakt het mogelijk om te verhuizen en beschermt tegen storingen, maar vereist wel cyberveiligheidsbeheer. Sommige ziekenhuizen die zijn overgestapt op de cloud zijn teruggekomen. Ziekenhuizen hebben in elk geval noodaggregaten om de continuïteit van de dienstverlening te waarborgen. Er zijn strenge normen met jaarlijkse tests.

Problemen ondervonden?

We ontvangen voornamelijk verzoeken van patiënten om hun rechten uit te oefenen. Het recht op verwijdering wordt beperkt door wettelijke verplichtingen. Gegevens worden minimaal 30 jaar bewaard. Veel gegevens worden opgeslagen in gedeelde bestanden als de patiënt daar toestemming voor heeft gegeven. In dat geval heeft de patiënt het recht om een kopie van zijn of haar dossier op te vragen. Dit brengt extra werk met zich mee voor het ziekenhuis.

Onderhouden?

Deze objecten moeten altijd worden onderhouden door een cyberbeveiligingsinventarisatie om gevoelige gegevens te beschermen tegen cyberaanvallen. Er worden beveiligingsprotocollen opgesteld. Het niveau van cybervolwassenheid in ziekenhuizen neemt geleidelijk toe. De implementatie van wettelijke naleving verbetert de beveiliging dankzij de NIS2-wet en CCB-verplichtingen.

Financiering en continuïteit van zorg?

Sommige AI-modules kunnen worden verwijderd. Op dit moment is het zo dat wanneer AI wordt geïntroduceerd, dit ter vervanging van bestaande protocollen is. Als die worden afgeschaft, gaan we terug naar het vorige protocol. Er is dus geen risico dat de continuïteit van de zorg wordt verstoord.

Hoe zien patiënten hun gegevens?

Patiënten hebben de volgende rechten met betrekking tot hun gegevens: toegang, rectificatie, wissing (beperkt in het geval van gezondheidsgegevens) en overdraagbaarheid (overdracht van de ene dienstverlener naar de andere). Toestemmingsmechanismen zijn nodig om ervoor te zorgen dat de toestemming van de patiënt geïnformeerd, vrij en herroepbaar is. Tot slot moeten er procedures worden vastgesteld om ervoor te zorgen dat deze toestemming (of weigering) wordt gerespecteerd.

Vooruitgang in onderzoek verzoenen met respect voor vertrouwelijkheid?

Pseudonimisering en anonimisering worden gebruikt om de vertrouwelijkheid van gegevens te garanderen. Bij pseudonimisering worden identificatoren vervangen door pseudoniemen. Anonimisering is gericht op het verwijderen van persoonlijke informatie zodat de persoon in kwestie niet kan worden geïdentificeerd. Meerlaagse anonimisering maakt het moeilijk om personen opnieuw te identificeren.

Er zijn veel uitdagingen bij het combineren van onderzoek en vertrouwelijkheid, waaronder het voldoen aan strenge normen voor gegevensbescherming, goed gegevensbeheer en de implementatie van ethische praktijken bij het hergebruik van gegevens.

Uitdagingen?

Een van de belangrijkste uitdagingen is het creëren van vertrouwen in gegevensbeheer en -bescherming. In België zullen regelgevende instanties worden opgericht, maar hoe? De rekenkracht van AI zal het mogelijk maken om de zorg te verbeteren, behandelingen te ontwikkelen en te personaliseren. Met de uitdaging van de RGPD en in een context waarin de invloed van AI voortdurend toeneemt. We zullen in staat moeten zijn om de risico's van AI te identificeren en preventieve maatregelen te nemen. Daar komt nog bij dat smalle AI's gebaseerd zijn op geïdentificeerde bronnen, in tegenstelling tot generatieve AI's. Dit vereist constante controle met menselijke supervisie. Dit vereist voortdurend vervolg met menselijk toezicht.

Wat is de rol van de regelgevende instanties?

Nog geen retourzendingen.

Robots?

Ja, tegenwoordig gebruiken we chirurgische robots. Maar we gebruiken ze nog niet voor ondersteuning. Dit werpt ethische vragen op die de toepassingen van AI *kunnen* beperken om misbruik te voorkomen.

Chatbox?

Hybride AI plaatst AI-agenten tegenover mensen. Sommige ziekenhuizen installeren dit al om de behandelingssnelheid te verhogen. Het principe blijft dat de bronnen gecontroleerd moeten worden om de hallucinaties van de AI te beperken.

Klachten?

Ze komen terecht bij de DPO. Er is een procedure voor het corrigeren van onjuiste gezondheidsgegevens, onder de verantwoordelijkheid van de verantwoordelijke voor de verwerking. De afdeling Patiëntenrelaties ontvangt klachten, waaronder klachten over gegevensbescherming en partijdigheid.

Regulering van rechten?

CHIREC heeft nog geen relaties met de toezichthoudende instanties. CHIREC wil graag meer leren omdat het nog geen expertise heeft op dit gebied. Samenwerking met UNIA zal het mogelijk maken om de vaardigheden op dit gebied te vergroten, met name wat betreft controlesystemen. Er moeten controleambtenaren worden aangeworven. *De NHRPH kan een cruciale rol spelen door aanbevelingen te doen over IT ACT-standaarden en de ethische naleving van IT-instrumenten te waarborgen*.

De toekomst?

We staan aan het begin van de AI-revolutie. Die zal exponentieel zijn. Het is essentieel om grip te houden op de dingen, om controle te kunnen garanderen over hoe dingen worden gebruikt. AI is slechts een van de vele hulpmiddelen. We moeten de ontwikkelingen in de hand houden en er gelijke tred mee houden, ethische blunders vermijden en de patiënt centraal stellen: het is een uitdaging. Dit is een uitdaging, omdat belangrijke Europese regelgeving een steeds grotere werkdruk creëert. Ziekenhuizen staan machteloos tegenover deze zware werklast. Ze hebben ondersteuning nodig om aan deze regelgeving te voldoen en om AI te implementeren. En hoe zit het met budgetten?

GM : Hartelijk dank voor uw presentatie en voor het serieus nemen van onze vragen! Er spelen verschillende kwesties. AI is een van de vele instrumenten waar we niet bang voor hoeven te zijn. Maar er zijn grenzen nodig. Het is belangrijk om zwakke punten als uitdagingen te zien. Niet alle ziekenhuizen hebben hetzelfde niveau. Er is ook behoefte aan een toezichthoudend orgaan. Welke betrokkenheid zullen functionarissen voor gegevensbescherming hebben in toekomstige toezichthoudende organen? Er is ook behoefte aan ondersteuning en financiering. Tot slot is er de kwestie van de mogelijke verkoop van gegevens. Dit is normaal gesproken verboden, maar Prof. G. Briganti gelooft dat er een risico is.

PJV: Sommige klinische onderzoeken worden gefinancierd door farmaceutische bedrijven. Om de mensen die eraan werken te betalen, ontvangen farmaceutische bedrijven rendement met gezondheidsgegevens. Het kader is gereguleerd. Met de komst van de gezondheidsagentschappen en de Europese gezondheidsgegevensstromen zal de vraag rijzen of de gegevens gecommercialiseerd kunnen worden. Het doel is hier om de volksgezondheid en de toegang tot op de markt gebrachte geneesmiddelen te verbeteren. Het ziekenhuismanagement heeft geen winstoogmerk. Maar hoe financier je het verstrekken en anonimiseren van gegevens, terwijl je patiënten nog steeds het recht geeft om al dan niet toestemming te geven? Het is moeilijk voor te stellen wat er daarna komt. In ieder geval is samenwerking tussen ziekenhuizen en nationale instanties noodzakelijk.

PJV stuurt zijn PPT naar de WG en vraagt om opeenvolgende uitwisselingen om kennis te delen.