LIFECYCLE MANAGEMENT VAN AI-MODELLEN

Sparrenheuvel 32, 3708 JE Zeist | (030) 2 270 500 | kennis@mxi.nl | www.mxi.nl

Richard Sitters

Het enthousiasme over de mogelijkheden van Artifical Intelligence (AI) in de zorg geeft veel zorgorganisaties de ruimte te experimenteren en AI-toepassingen in te zetten voor medische toepassingen. Maar juist na de initiële investeringen om AI-modellen en AI-toepassingen te ontwikkelen blijkt structureel tijd, geld en inspanning nodig te zijn. Om een ontwikkeld AI-model te implementeren en veilig te blijven gebruiken moet er nog veel gebeuren. Het gat van een veilige experimenteer- of ontwikkelomgeving naar productie moet overbrugd worden. En daarnaast moeten de prestaties van het model continu gemonitord, bijgestuurd, geborgd en aantoonbaar gemaakt worden. Lifecycle Management doet een intrede.

Voor het ontwikkelen of verwerven van softwareapplicaties is het van belang om tijdens de ontwikkelfase/verwervingsfase rekening te houden met vervolgstappen in de levenscyclus, te weten implementatie (voorbereiden vrijgave en inproductiename), gebruik (monitoren en beheren), doorontwikkeling en uiteindelijk afstoting. We spreken dan over Lifecycle Management. Lifecycle Management is het continu leveren, integreren en continu reviewen, aanpassen en verbeteren van een toepassing of oplossing. Het heeft als doel de toepassing van de oplossing te borgen aan de veranderende omstandigheden van de organisatie en doelstellingen. Het omvat belangrijke activiteiten zoals governance, in productie nemen van de oplossing, monitoren en “drift detection” (afwijkingen van de businessdoelstellingen), troubleshooten, onderhouden en actualiseren, versiebeheer, bijhouden van de catalogus, model vrijgave, privacy impactanalyse, ethische impactanalyse en logging. Kortom, het introduceren, in stand houden en continu blijvend onderhouden van een AI-oplossing.

AI Lifecycle Management is nog een onvolwassen vakgebied en heeft nog veel aan bewustwording te winnen. Voor Lifecycle Management van software is ondertussen 35 jaar ervaring opgebouwd en een standaard DevOps proces beschikbaar. AI kent parallellen en tegelijkertijd zijn er essentiële verschillen en komen er meer aspecten kijken bij AI Lifecycle Management dan bij andere software.
Er moeten meer gegevens over de AI-oplossing worden bijgehouden en de governance moet strak zijn ingeregeld. AI-toepassingen in de zorg vragen, in tegenstelling tot de meer reguliere ondersteunende software, om een intensievere medisch inhoudelijke beoordeling, monitoring en governance.

LEESWIJZER

Dit artikel geeft een overzicht van Lifecycle Management van AI-modellen, de stakeholders die erbij betrokken zijn, de activiteiten en de uitdagingen die daarbij komen kijken voor AI. Vervolgens gaan we in op de specifieke eisen die de zorg aan AI Lifecycle Management stelt.

Responsible AI en wet- en regelgeving spelen een belangrijke rol. Hieruit volgen de eisen die de invoering en het gebruik leggen op het configuratiebeheer van AI-modellen. Ook de gegevens die bijgehouden moeten worden volgen hieruit. Als het aantal modellen groeit kan het managen ervan niet meer handmatig. Een Data Science Machine Learning (DSML) platform helpt daarbij. Wij gaan in het artikel in op de eisen die aan een goed platform (moeten) worden gesteld.

Ook monitoring is essentieel in de AI Lifecycle. We gaan in op performance degradatie van AI aan de hand van “modeldrift” en geven een aantal best practices bij het inrichten van monitoring. Tot slot komen kwaliteitsmanagement en governance in het AI Lifecycle Management aan bod.

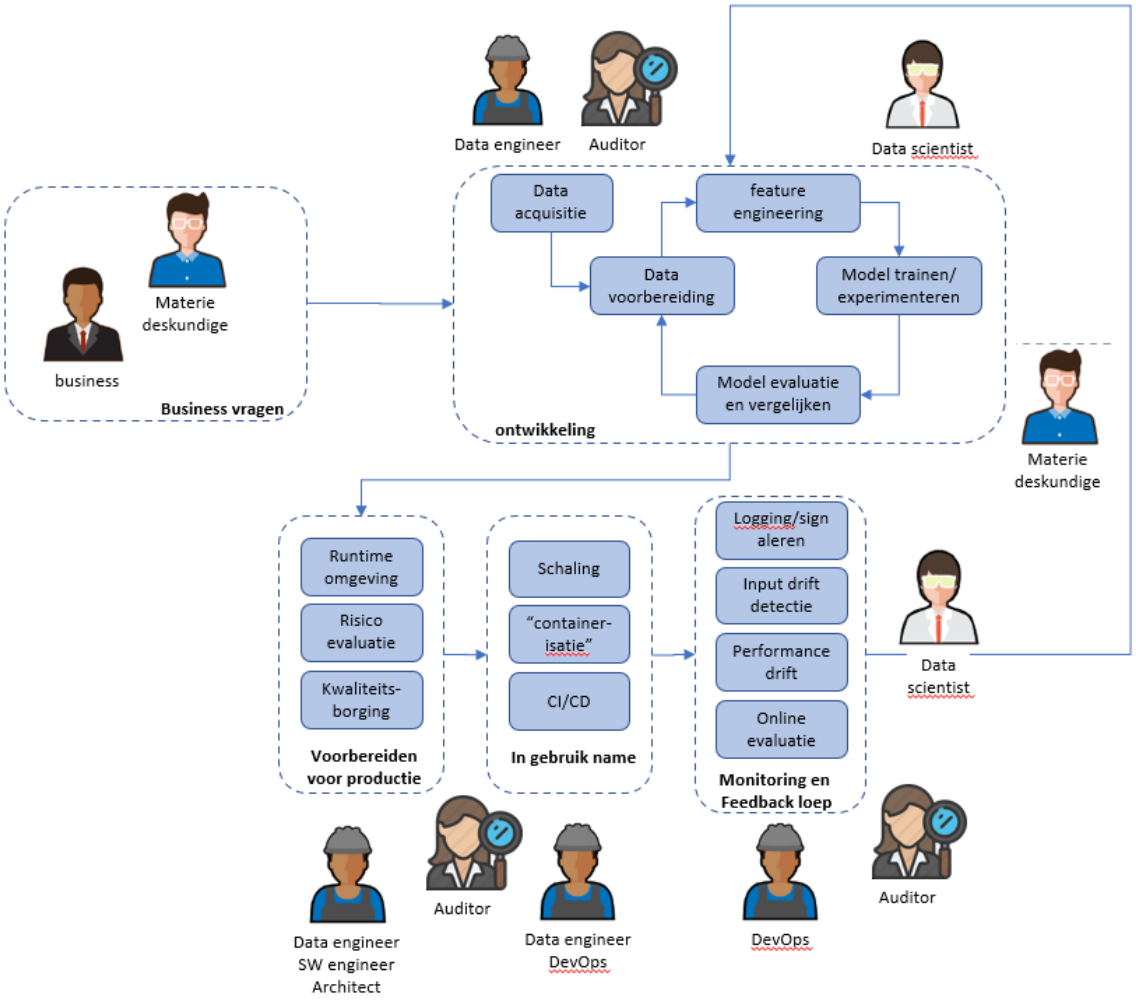
INHOUDSOPGAVE

LIFECYCLE MANAGEMENT & AI

Organisaties experimenteren volop met het ontwikkelen, aanschaffen en in praktijk brengen van AI-toepassingen. Voor het ontwikkelen of verwerven van softwareapplicaties is het van belang om tijdens de ontwikkelfase/verwervingsfase rekening te houden met de vervolgstappen in de levenscyclus, te weten implementatie (voorbereiden vrijgave en inproductiename), gebruik (monitoren en beheren), doorontwikkeling en uiteindelijk afstoting. We spreken dan over Lifecycle Management. Een organisatie die dit niet meteen adresseert kan later geconfronteerd worden met herstelmaatregelen of complicaties tijdens de implementatie en gebruik. Dit is voor AI niet anders.

STAKEHOLDERS AI

Er zijn diverse rollen in de AI Lifecycle. Tijdens de ontwikkelfase van het AI-model moet voorgesorteerd worden op de eisen die het gebruik van AI in de praktijk met zich meebrengt. Het is dus van belang de diverse gebruikersgroepen/rollen tijdens de ontwikkelfase te betrekken. Hieronder een schematische weergave van de rollen en activiteiten zoals die in de praktijk een rol spelen [1].



Hieronder staan de verschillende activiteiten van de diverse rollen in de lifecycle en de eisen die deze rollen stellen aan het AL Lifecycle Management proces.

Rol	Rol in de lifecycle	Eisen die de rol aan AI Lifecyle Management proces stelt
Onderwerp materiedeskundigen	- Vaststellen van business-vraagstellingen en businessdoelstellingen. - Vaststellen van de te meten KPI's (meten van de effectiviteit van het AI-model). - Continu evalueren en vaststellen dat de modelperformance in overeenstemming is en blijft bij de business behoeften.	- Begrijpelijk kunnen vaststellen wat de performance van het model dat in gebruik is (in businesstermen). - Een mechanisme / feedbackloop om vast te kunnen stellen wanneer een model niet meer aan de business eisen/verwachtingen voldoet.
Data scientists	- Bouwt modellen op basis van de vraagstelling van de business of onderwerp materiedeskundigen". - Leveren modellen op die in gebruik kunnen worden genomen in de productieomgeving (met de productiedata). - Toetsen modelkwaliteit in samenwerking met de materiedeskundigen tegen de business vraag/vereisten.	- Geautomatiseerde model *packaging* en ingebruikname op de productieomgeving - Mogelijkheid om tests te ontwikkelen om de kwaliteit van de modellen te meten en verbeteren - Inzicht in de performance van alle modellen die in gebruik zijn vanaf één centrale locatie/platform - Inzicht in de pipeline van elk model zodat men snel nieuwe versies van het betreffende model kan maken / de betreffende modelversie kan reproduceren.
Data engineers	- Data ophalen, optimaliseren en voorbewerken van data. - Continu integreren en leveren.	- Zichtbaarheid van de performance van de modellen die in gebruik zijn. - Inzicht in alle details van de hele datapipeline.
Software engineers, ICT-architect	- Integreren van AI-modellen in de applicatieomgeving / systemen van de organisatie. - Zeker stellen dat de AI-modellen goed integreren met bestaande applicaties. - Bouwen van operationele systemen en testen (security, performance, beschikbaarheid). - Continu integreren en leveren.	- Versiebeheer en automatische testen. - De mogelijkheid om parallel met meerdere versies en applicaties te werken. - Seamless deployment - Integratie van AI Lifecycle Management in het DevOps proces van de organisatie.
Model risk managers / auditoren	- Minimaliseren van risico van het gebruik van AI-modellen - Compliance met interne en externe wet- en regelgeving aantonen. - Checken monitoring en log registraties>	- Robuuste, bij voorkeur geautomatiseerde, report tooling - Ontwerp(beslissingen), gebruik van AI-modellen - Governanceprocessen en opvolgen daarvan

AI-architecten	- Verzekeren van een schaalbare, flexibele omgeving voor AI-modellen, van design tot ontwikkeling, deployment en monitoring. - Introduceren van nieuwe technologieën. - Integratie van het AI-model in de productie infrastructuur.	- High level overview van modellen en de resources die het nodig heeft. - Inzicht in het gebruik van resources om de infrastructuur en applicatie vereisten/benodigdheden te bepalen.

Tabel 1: rollen in- en eisen aan het AI Lifecycle Management proces

De invulling van de rollen zoals hierboven beschreven is afhankelijk van de sourcing (waar draait het model en wie beheert de productieomgeving?) van het AI-model. Zie daarvoor de paragraaf over governance. Het is van belang om al tijdens de ontwikkelfase van het AI-model de AI Lifecycle Management vereisten in betrekking te nemen en de daarbij gebruikersgroepen te betrekken.

DE AI LIFECYCLE

De lifecycle van AI kent dezelfde fasen als die bij software engineering. Door de extra datadimensie zijn er extra activiteiten per fase die andere methoden, tooling en expertises vereisen. Hieronder beperken we ons tot de Lifecycle Management activiteiten.

1 **Experimenteerfase**

Veel organisaties zitten nog in de experimenteerfase. Deze fase is vooral bedoeld om de potentie van de inzet van AI te verkennen. Ook in deze fase moeten data expertises betrokken worden. In deze fase wordt nog niet gelet op implementatieaspecten die de organisatie wel moet adresseren in de opvolgende fasen. De uitkomst van de experimenteerfase is een advies om wel of niet verder te gaan met de technologie. De experimenteerfase wordt soms gezien als onderdeel van de ontwikkelfase[1].

2 **Ontwikkel- of verwervingsfase**

Als eerste stap moet een organisatie onderzoeken of er op de markt al oplossingen verkrijgbaar zijn en kiezen voor zelfbouw/co-creatie of inkopen van een beschikbare oplossing (voor zorginstellingen is dit zelfs verplicht). Wanneer sprake is van zelfbouw of co-creatie gaat het om het ontwerpen en het schrijven van de AI-code welke definieert hoe het AI-model “leert” van de trainingsdata. In de praktijk kunnen er meerdere AI-algoritmes zijn om uit te testen. Ten opzichte van softwareontwikkeling zijn er een aantal extra activiteiten.

- Dataselectie: welke data gaat het model gebruiken, welke data is voor handen, hoe komt men aan de data, en wat is de kwaliteit van de data zijn vragen die hierbij moeten worden geadresseerd?
- Data voorbewerking (Extraction, Transformation and Load - ETL) omvat:
  - schrijven van code om de data voor te bewerken zodat deze geschikt wordt als trainingsdata;
  - het importeren van data;
  - brondata bevat in het algemeen veel vuile data, data die niet geschikt is voor de AI-oplossing (bijvoorbeeld incorrecte waarden, incomplete waarden, onleesbare waarden, ontbrekende waarden). De dataengineer modelleert de gegevens naar de definitieve opslagformaat en slaat die op.

[1] De experimenteerfase kan ook gezien worden als onderdeel van het ontwikkelen van een AI-model (ontwikkelfase). Echter, de doelstelling is anders (het kan resulteren in “niet doen”) en de betrokkenen zijn anders. Daarnaast geldt dat je voor een bepaald model (met bepaald doel) hooguit één keer een experiment uitvoert: de vervolgfasen worden cyclisch mogelijk meervoudig doorlopen. Daarom hebben we het hier als aparte fase benoemd.

- Featureselectie en dataverrijking: het resultaat van deze activiteit is een dataset waarmee het model kan worden getraind. Tijdens deze activiteit is aandacht voor het voorkomen van overfitting en bias van het model.
- De brondata moeten worden opgesplitst in “training data”, “test data” en “validatie data” (de “validatie data” wordt in een volgende fase gebruikt – voor validatie worden ook vaak nieuwe data opgehaald).
- Trainen van het AI-model met de training data.
- Testen van het AI-model met de testdata. Daarbij is het van belang om aandacht te besteden aan de runtime/accuratie ratio. Door het “tweaken” van parameters en datasets kan deze ratio worden beïnvloed.
- Gewenste data architectuur: hoe ziet de datapipeline eruit?
- Het deployment model (welke data wordt waar bewaard en geprocessed), data processing stappen en gerelateerde data layers, batch processing v.s. datastreaming, eisen aan de data architectuur (performance, storage, toegangspermissies, retientietijden, schaalbaarheid, datakwaliteit, beschikbaarheid) worden hier bepaald.
- Toolselectie ten behoeve van databewerkingsstappen zoals hierboven genoemd.

In plaats van zelf ontwikkelen kan een organisatie ook kiezen om een AI-model te kopen. Veel van de activiteiten die een rol spelen bij zelf ontwikkelen spelen ook wanneer je een model verwerft van een leverancier. In beide gevallen moet je nadenken over de eisen die je aan het model stelt en krijg je veelal te maken met het (her)trainen[2] en valideren van het model (samen de leverancier) en dus met data-activiteiten.

De AI-oplossing wordt in een bestaand werkproces binnen een bestaande organisatie ingezet en moet samenwerken met andere systemen (interoperabiliteit, koppelingen). Keuzes tijdens deze fase hebben gevolgen voor de volgende fasen. Kies je voor een on-premise omgeving, of plaats je delen van je oplossing en data in een datalake in de cloud? Privacy aspecten moeten in deze fase worden vastgelegd en besproken met de eventuele co-creating partner of de partij waar de data tijdens de hele cyclus wordt opgeslagen. En hoe zorg je bij plaatsing elders ervoor dat bij de afvoeringsfase alle data worden verwijderd? Hoe zit het met de performance als je een datastreaming oplossing hebt in plaats van een batch processing?

Als je samenwerkt en je hebt de dataprocessing uitbesteed aan een partner hoe zit het dan met de toegang tot data (privacy en beveiliging) en ook het data eigenaarschap? Met betrekking tot dit laatste moet je afspraken maken over eigenaarschap toegang tijdens de deployment fase en overdracht bij het afscheid nemen van het model en elkaar. En hoe zit het met de monitoring gegevens op basis waarvan (tijdens de gebruiksfase) wordt besloten tot aanpassing van het model?

Tot slot worden KPI’s/metrics op basis waarvan de performance van het model tijdens de gebruiksfase wordt gemonitord tijdens de ontwikkelfase/verwervingsfase bepaald. Het model wordt getraind en beoordeeld tegen de KPIs.

[2] Als je een andere patiëntpopulatie krijgt moet opnieuw worden getraind.

3 Voorbereiding vrijgave (validatie)

De nadruk in deze fase ligt op de validatie van het model en kwaliteitsborging (risico inschatting, het inregelen van maatregelen). Activiteiten in de voorbereidingsfase omvatten.

- Ontwerpen van de runtime/productie omgeving
  Hierbij gaat het om het verzekeren dat het technisch mogelijk is om een model in productie te nemen (in ICT-infrastructuur) en te valideren of het model in de productieomgeving goed performt (latency, ICT-resource gebruik, data toegang en data retrieval in de productieomgeving). De productieomgeving kan verschillen van de ontwikkelomgeving. Voor meer informatie, zie paragraaf "**Fout! Verwijzingsbron niet gevonden.**" in de bijlage.
- Uitvoering van een DPIA en optioneel AI impact assessment (AIIA)
  Voorafgaand aan het gebruik van data voer je een DPIA uit. Het is aan te bevelen om ook voorafgaand aan het gebruik van de AI-toepassing een AIIA uit te voeren. Het is noodzakelijk de DPIA en de AIIA regelmatig te reviseren in lijn met de levenscyclus van de AI-toepassing.
- Uitvoeren van een (prospectieve) risicoanalyse
  Het is noodzakelijk om ook een goede risicoanalyse uit te voeren op "verkeerde uitkomsten". Wat is de kans en impact op verkeerde beslissingen op basis van uitkomsten van het algoritme en hoe zijn die risico's te minimaliseren?
- Validatie van het model
  Tijdens de voorbereidingsfase wordt het model gevalideerd op correcte werking. Dit gebeurt met de validatie dataset die eerder in de ontwikkelfase is vastgesteld. Dat verschilt met het testen van het model omdat het model hier in de productieomgeving wordt gevalideerd. Doordat de productieomgeving niet altijd hetzelfde is als de testomgeving kan dit de werking van het model beïnvloeden.
- Inregelen van de kwaliteitsmaatregelen
  Hier speelt vooral datakwaliteit een belangrijke rol (hoe borg je de kwaliteit van de gegevens die je aan het model tijdens gebruik voedt) en het opzetten en borgen van de monitoring activiteiten (hoe zorg je ervoor dat monitoringsactiviteiten plaatsvinden en feedback wordt geëvalueerd).
- Informatie beveiligingsmaatregelen implementeren.
- Borgen van herleidbaarheid en auditability.
  Hier speelt configuratiemanagement een belangrijke rol (documenteren welke datasets en modelversie zijn gebruikt voor het testen/valideren en op welke omgeving het model is getest/gevalideerd).
- Eventuele proefplaatsing en evaluatie van de proefplaatsing.
- Verifiëren en aanvullen van de vastgelegde gegevens.
  Voor audits moeten voor elke versie van het model en gebruikte data tijdens het testen verschillende gegevens worden vastgelegd. Tijdens deze fase dient die informatie te worden gecompleteerd en gearchiveerd. Zie paragraaf "Configuratie managementgegevens".

4 Implementatie fase (in productie name)

Na ontwikkelen en valideren kan het model worden geïmplementeerd in de productieomgeving. De deployment architectuur van het model wordt definitief vastgesteld. Activiteiten zijn in beginsel niet veel verschillend van het implementeren van een softwareoplossing met uitzondering van de extra activiteiten die de data verantwoording en datapipeline betreffen.

- Bouwen van het model en installeren in de productieomgeving (containerisatie, packaging).
- De data scientist (in samenwerking met de software-enigineer) moet de code genereren en publiceren in de productieomgeving, metadata en documentatie opnemen in een centraal archief/documentatiesysteem en de koppelvlakken implementeren.
- Datapipeline implementeren (ophalen data) en testen.
- Logging systeem wordt geïmplementeerd en getest.

- Monitoring inrichten.
- Onderhoudsplan opstellen.
- De data-engineer of data scientist stelt de eerste fairness en explainability rapportages op.
- Inrichten beheerprocessen en overdracht (inclusief beheertooling, onderhoudsplan).
- Trainen van gebruikers en de beheerorganisatie.
- Vrijgave (technisch, functioneel, klinisch) en acceptatie.

Zie ook paragraaf "**Fout! Verwijzingsbron niet gevonden.**" van de bijlage

5 Gebruiksfase (motoring en feedback)

Tijdens het gebruik moet het model onderhouden worden. Kernvraag is: wanneer moet het model opnieuw worden getraind? Dat hangt van de monitoringuitkomsten af. Monitoring is essentieel omdat de performance in de loop van de tijd verslechtert door datadrift en conceptdrift.

- Datadrift: de data die het AI-model ontvangt en op basis waarvan het model beslissingen neemt kan langzaam veranderen in de loop van de tijd. Als dat gebeurt moet het model worden aangepast om goed te blijven presteren.
- Conceptdrift: als verwachtingen veranderen. Wat voorheen als wenselijk of goed werd beschouwd kan onder veranderende omstandigheden, niet meer als wenselijk worden beschouwd.

Bij gevonden issues is het niet mogelijk om alleen de code te updaten en het model opnieuw in gebruik te nemen. Het nieuwe model moet mogelijk opnieuw worden getraind, daarbij in betrekking nemende welke oorspronkelijke dataset was gebruikt en welke parameters er waren gebruikt.

- Resource monitoring: meten van gebruik van ICT-resources zoals CPU, memory, disk.
- Healthcheck: check of het model "up and running" is, latency checks.
  Performance monitoring: checken van de performance van het model, checken of het de juiste resultaten oplevert. Door datadrift is er bij de inzet van AI altijd sprake van performance degradatie. De organisatie zal de performance van het model monitoren op gewenst gedrag en afwijkingen.
- Beheer en onderhoud: storingen oplossen, ondersteuning leveren aan gebruikers, wijzigingen implementeren.
- Training: nieuwe gebruikers.
- Post Market Surveillance: alleen bij eigen ontwikkelde software die aan derden beschikbaar is gesteld.
- Rapportages en analyse: fairness en uitlegbaarheid, veilig gebruik, monitoring feedback.

Voor meer detail, zie paragraaf "**Fout! Verwijzingsbron niet gevonden.**" in de bijlage.

6 Afvoeringsfase

In deze fase, waarin het model uit dienst wordt genomen, is het van belang dat de organisatie de gebruikte data veilig stelt. Een actueel overzicht van gebruikte data en wie eigenaar is van de data (onderdeel van de configuratie management database) is hierbij van essentieel belang. Speciale aandacht is nodig voor het verwijderen van backup-data en data die in de cloud zijn geplaatst.
In deze fase moet de organisatie ook kijken naar wat gedaan moet worden om aan zijn archiveringsplicht te voldoen (welke datasets en modelversies moeten worden bewaard? Moeten rapportages en beslissingen over nieuwe trainingsmomenten worden bewaard? Moeten logging gegevens worden bewaard?).

Over al deze fasen heen is governance (regievoering) noodzakelijk om de activiteiten op een beheersbare manier uit te voeren, de risico's te adresseren en beheersen, de kwaliteit te managen en te voldoen aan wet- en regelgeving. Een goed configuratie management systeem en kwaliteitssysteem zijn daarbij onontbeerlijk (zie paragraaf "

Configuratiebeheer van AI-modellen”). In de bijlage staan de verschillende stappen verder uitgewerkt.

UITDAGINGEN BIJ AI LIFECYCLE MANAGEMENT

Op basis van de bekende standaarden voor software Lifecycle Management zijn er acht aanvullende aandachtspunten voor AI Lifecycle Management.

1 **Meer vrijheidsgraden dan bij softwareontwikkeling en -onderhoud.**
Het gedrag van het AI-model is afhankelijk van de programmering van het model én van de data die wordt gebruikt. Bij software resulteert het gebruik van dezelfde input in hetzelfde resultaat. Bij AI is dat niet het geval. Door het zelflerend vermogen kunnen dezelfde inputgegevens resulteren in verschillende uitkomsten. Twee gevallen van hetzelfde model met dezelfde configuratieparameters genereren verschillende uitkomsten als ze getraind zijn met verschillende data. Met de toevoeging van data als extra vrijheidsgraad spelen er bij AI Lifecycle Management meer aspecten een rol (dataset, AI-code, data schoningsalgoritme, configuratie parameters van het AI-algoritme) dan bij software Lifecycle Management.

2 **Meer disciplines betrokken bij AI Lifecycle dan bij de Software Lifecycle.**
Dat betreft data gerelateerde disciplines, met vraagstukken over datakwaliteit en databeschikbaarheid (als input). Ook de juridische en ethische vraagstukken die bij het gebruik van AI komen kijken vragen extra aandacht, zeker in de zorg. Een discipline spreekt een eigen taal, gebruikt eigen tools en methodieken, heeft andere skills, eigen verantwoordelijkheden en een andere focus. Zie paragraaf “Stakeholders AI”.

3 **Huidige vorm van datagedreven AI is een relatief jong vakgebied.**
De huidige vorm van datagedreven AI (waarin data gerelateerde disciplines een belangrijke rol spelen) is relatief nieuw[3]. De focus ligt nog op het ontwikkelen van nieuwe AI-algoritmen en minder op de lifecycle en beheercyclus. Hierdoor is er voor het Lifecycle Management minder bewustzijn en aandacht.

4 **Verantwoordelijkheden voor AI Lifecycle Management moeten nog belegd worden.**
Er is kennis nodig is kennis van AI en data gerelateerde disciplines nodig. Anderzijds is kennis nodig van Lifecycle Management processen zelf. Deze kennis is schaars en – indien al aanwezig – op verschillende plekken in een organisatie aanwezig. Dat vraagt om samenwerking en duidelijke verdeling van verantwoordelijkheden.

5 **Wet- en regelgeving.**
Naast een goed werkende AI-oplossing stelt wet- en regelgeving én de publieke opinie ook steeds meer eisen. Meer dan bij software worden AI-oplossingen onderworpen aan audits waarbij de uitlegbaarheid, nauwkeurigheid en correctheid (ook wel performance) van het model aantoonbaar moeten zijn. ‘Responsible AI’ is een benadering die naast het voldoen aan wet- en regelgeving invulling geeft aan het ethisch gebruik van AI en transparantie van de werking van het model. In sommige gevallen moeten individuele voorspellingen van het model te verklaren zijn in termen van welke elementen van de data welke invloed hebben gehad op de uitkomst van het model. In de eisen die de

[3] Hoewel de grondlegging van AI in de jaren ’40 – ’50 van de vorige eeuw was, waren de AI-toepassingen tot voor kort oplossingen waarin de kunstmatige intelligentie in standaard software regels was geprogrammeerd. Daarmee verschilden de oplossingen niet fundamenteel van andere “standaard” softwareprogramma’s. Met de toevoeging van de dataprocessing zijn systemen nu zelflerend geworden.

EU stelt in haar 'whitepaper on AI – A European approach to excellence and trust' en 'Ethics guidelines for trustworthy AI' staat ethisch gebruik, het respecteren van menselijke autonomie, privacy, reproduceerbaarheid, traceerbaarheid en verifieerbaarheid van AI centraal.

6 **Snellere ontwikkel- en onderhoudscycli.**
Tijdens het gebruik van het AI-model treden veranderingen op in de programmering van het model (dooronderhoud, wijzigingsvoorstellen, *bugfixing*). Ook is onderhoud op het AI-model nodig door performance degradatie. Verder is onderhoud nodig als de productieomgeving (waarin het model actief is) verandert (interface wijzigingen, andere apparatuur). Door de incrementele manier van agile ontwikkeling (net zoals bij software) komen er veel nieuwe versies in een kort tijdsbestek beschikbaar. Het gecombineerde effect is dat er sprake is van steeds snellere ontwikkel- en onderhoudscycli. Dit vereist (nog meer dan bij software) nauwkeurige monitoring tijdens de gebruiksfase en directe feedback van de monitoring resultaten naar de ontwikkeling van een nieuwe modelversie.

7 **Meerdere versies die gelijktijdig in gebruik zijn.**
Het meten van de performance van een AI-model kan soms alleen in de productieomgeving. Dat betekent dat het nieuwe model en het in gebruik zijnde model in dezelfde omgeving draait. De reden daarvoor is dat tijdens ontwikkeling de performance alleen voorspeld kan worden op basis van de trainings-, test- en validatiedata en niet op basis van actuele productiedata. Ten tweede kan het lastig kan zijn om modellen die met een datastreaming pipeline werken (pin plaats van batchprocessing) te testen in een testomgeving waar de real-time datastream niet voorhanden is. Ten derde kunnen meerdere groepen met verschillende versies werken van een model omdat ze verschillende studies of werkzaamheden uitvoeren[4]. Tot slot kan de reden van het inzetten van een voorlopig model in de productieomgeving zijn om de CPU performance (latency) in modellen te testen. Resultaat hiervan is dat er (soms) meerdere versies van modellen tegelijk actief zijn. Wanneer meerdere modellen tegelijkertijd operationeel zijn wordt het lastig om een overzicht te houden over de status van alle modellen en de risico's goed te blijven managen. Wanneer er slechts een handvol AI-modellen actief zijn in de productieomgeving kan het managen van AI-modellen grotendeels nog handmatig. Maar met de steeds snellere cycli groeit dat aantal steeds sneller. Als het aantal in gebruik zijnde, en in ontwikkeling zijnde modellen groeit gaat dat niet meer handmatig.

8 **Meer en nauwkeuriger versiebeheer.**
Centraal in het goed en verantwoord gebruik van AI-modellen staat de herleidbaarheid, aantoonbaarheid en reproduceerbaarheid: wat is de herkomst van alle data? Hoe is het getest, met welke datasets? Wie heeft eraan gewerkt? Hoe is bias voorkomen of overfitting? En hoe presteert het model in de loop van de tijd? Op welk stack van open source software is het AI-model gebouwd? Daarvoor moet een organisatie een flink aantal gegevens bijhouden waaronder de herkomst van data en voor welke versie welke data is gebruikt en dat legt extra eisen op aan configuratiebeheer van het model: het bijhouden van de precieze code, datasets, configuratie parameters op basis waarvan het huidige productie model is gecreëerd is een uitdaging. Het is tenminste nodig om model version en data set version te archiveren.

De implementatie van AI Lifecycle Management is essentieel voor veilige zorg. Alle Lifecycle Management activiteiten hebben hier een bijdrage aan. Dit vraagt binnen de zorginstelling om organisatie. Hoe eerder in het proces deze bewustwording aanwezig is, aandacht krijgt en ondersteund wordt, hoe eenvoudiger het proces van ontwikkeling en inkoop naar veilige implementatie en gebruik wordt.

[4] Wanneer je bijvoorbeeld AI inzet voor medische alarmroutering zijn de keuzes hoe en wanneer je een alarm routeert bij neonatologie anders dan die voor de IC. Beide afdelingen zouden dan met verschillende versies van eenzelfde AI-model kunnen werken.

AI LIFECYCLE MANAGEMENT IN DE ZORG

De zorg legt extra eisen op aan de AI Lifecycle Management activiteiten. Met de toepassing van AI in de zorg wordt de AI-oplossing in het algemeen gezien als medisch hulpmiddel. Daardoor moet de AI-oplossing voldoen aan de Medical Device Regulation (MDR) en het convenant medische technologie. Beide stellen specifieke eisen in de gehele lifecycle van de oplossing waarbij de vraag of AI moet worden gezien als medisch hulpmiddel of niet centraal staat.

De Nederlandse Federatie van Universitair medische centra (NFU) heeft een reeks artikelen en webinars over de MDR. Zie daarvoor www.nfu.nl (zoek op MDR) en [13] – NFU – SW als medisch hulpmiddel. Hieronder een opsomming van de relevante aspecten.

- **Medisch hulpmiddel**
  Met de toepassing van AI in de zorg wordt de AI-oplossing in het algemeen gezien als medisch hulpmiddel. Daardoor moet de AI-oplossing voldoen aan de MDR [9] en het convenant medische technologie[5]. AI valt onder de medische hulpmiddelen wanneer het gebruikt wordt voor diagnostische en/of therapeutische doeleinden (eventueel in combinatie met andere apparaten) bij patiënten. Daar waar AI wordt ingezet in de zorglogistiek of ten behoeve van financiële controle is het dus geen medisch hulpmiddel. Medische hulpmiddelen kennen vele verschijningsvormen en dit maakt het soms lastig om te beoordelen of het AI-model wel of niet onder die noemer valt. Vanuit de EU Commissie is er een leidraad [10] beschikbaar die organisaties en ontwikkelaars helpt om te bepalen of hun software een medisch hulpmiddel is.

- **Classificatie van de oplossing volgens de MDR**
  De MDR legt extra eisen op. Wordt de oplossing gebruikt voor diagnostische en/of therapeutische doeleinden (eventueel in combinatie met andere apparaten) dan is de classificatie IIa, IIb of zelfs III (in de Medical Device Directive (MDD) nog klasse I). Ten opzichte van de eerder geldende MDD wordt de classificatie, en daaraan verbonden eisen strenger.

- **Zelf ontwikkelen van een AI-oplossing is aan regels gebonden**
  Eigen ontwikkeling van een AI-oplossing is niet zomaar toegestaan, ook in geval dat de oplossing alleen voor eigen gebruik is. Men moet eerst aantonen en documenteren dat er geen oplossing op de markt beschikbaar is die voldoet [12].

- **Regels bij eigen ontwikkeling**
  Bij eigen ontwikkeling (of co-creatie) moet een zorginstelling voldoen aan alle wet- en regelgeving waar een fabrikant ook aan moet voldoen.

- **Certificering**
  - CE certificering en PMS
    Wanneer een zorginstelling zelf een AI-oplossing bouwt en deze beschikbaar stelt aan derden (ook zonder vergoeding) dan wordt het gezien als fabrikant en is CE markering vereist. Ook een Post

[5] De MDR stelt in artikel 1 dat hulpmiddelen moeten voldoen aan de algemene veiligheids- en prestatie-eisen. Dat betekent dat de hulpmiddelen zodanig zijn ontworpen en gemaakt dat zij onder normale gebruiksomstandigheden geschikt zijn voor hun beoogde doeleind en daarbij veilig en doeltreffend zijn en geen onnodige risico's of gevaar in het leven roepen. Daarmee legt de MDR specifieke eisen op aan het risicobeheer en monitoring van de performance van de AI-oplossing.

Market Surveillance is dan verplicht[6]. Dit kan een rol spelen bij ketensamenwerking waarin een instelling een eigen ontwikkelde oplossing beschikbaar stelt aan derden. CE en PMS zijn niet verplicht als de zorginstelling de oplossing alleen voor eigengebruik ontwikkelt.

- Controle verplichtingen
  Er is ook verantwoordelijkheid voor de zorgorganisatie die een model van de markt aanschaft en gebruikt. De zorgorganisaties moeten valideren dat het beoogd gebruik van AI als medisch hulpmiddel past bij het gebruik ervan. Inzet van een middel dat tegen een hoge klasse is gecertificeerd maar voor een ander gebruik dan het beoogd gebruik is dus niet zondermeer toegestaan (voorbeeld: wanneer een AI-oplossing wordt gebruikt voor de routering van medische alarmen is het de vraag of dezelfde oplossing zondermeer ook kan worden ingezet voor het filteren van alarmen (wel of niet alarmeren)).
  Wanneer de zorginstelling de AI-oplossing inzet in een keten van apparatuur is de zorgorganisatie zelf verantwoordelijk voor het functioneren van de gehele keten. Dat kan nog wel eens lastig zijn. Vooral wanneer de implementatie en het beheer van een totaaloplossing over meerdere afdelingen heen is verdeeld (bijvoorbeeld medische techniek en ICT) en er sprake is van meerdere afdelingsverantwoordelijken.

- **Wet- & regelgeving**
  - De Wet kwaliteit, klachten en geschillen zorg (Wkkgz) bepaalt dat een zorgaanbieder zich van zodanige middelen moet bedienen dat deze redelijkerwijs moeten leiden tot het verlenen van goede zorg. Dat betekent dat hulpmiddelen moeten voldoen aan algemene veiligheids- en prestatie-eisen. Het Convenant Medische Technologie stelt risicomanagement verplicht gedurende de gehele lifecycle. Performance degradatie veroorzaakt door datadrift introduceert extra risico's en vereist een dus risicobeheersing waarin de datadimensie nieuw.
  - Ethisch gebruik
    Waar AI wordt toegepast in de zorg is het ethisch gebruik van AI van belang. De toepassing moet bijdragen aan het welzijn van de patiënt. Een AI Impact Assessment kan daarbij helpen. Het is bedoeld wanneer de zorgorganisatie die AI wil inzetten een analyse wil doen van de juridische en ethische gevolgen. Transparantie (uitlegbaarheid) hoe het AI-model tot bepaalde beslissingen is gekomen is daar een onderdeel van.
  - Privacy
    Bij het inzetten van AI in de zorg worden bijzondere persoonsgegevens (medische gegevens) verwerkt. In de AVG geeft de Autoriteit Persoonsgegevens (AP) aan wanneer er een Data Privacy Impact Assessment (DPIA) moet worden uitgevoerd. Dat is niet nieuw. Tijdens de levenscyclus kan het noodzakelijk zijn dat bij het hertrainen van het model opnieuw een DPIA nodig is. Wanner de dataset verandert, of er sprake is van andere feature selectie is het van belang te onderzoeken of er opnieuw een DPIA nodig is. Dat betekent dus dat het kan zijn dat er verschillende DPIA's uitgevoerd moeten worden tijdens één cyclus omdat er in de verschillende lifecycle fases verschillende data kan worden gebruikt.
  - Archivering
    Wanneer afscheid genomen wordt van een AI-oplossing moet een zorginstelling vanuit de archiveringsplicht nagaan welke gegevens (inclusief trainingsdata) en wat er van het model bewaard moet worden. Hier is op dit moment nog geen specifieke wetgeving voor of ervaring mee.

[6] Een PMS is de verzameling van activiteiten die een fabrikant structureel moet uitvoeren om te controleren of de prestaties van het product voldoen aan de gestelde eisen voor kwaliteit en veiligheid, oftewel, of het product doet waar het voor gemaakt is en veilig gebruikt kan worden. PMS is essentieel om de kwaliteit en de veiligheid van medische hulpmiddelen te waarborgen.

Bij AI Lifecycle Management zijn in de zorg veel expertises betrokken. Het is een ingewikkeld proces. De competenties zijn verdeeld over verschillende rollen binnen de zorginstelling. Het mandaat voor beslissingen ligt ook verspreid terwijl beslissingen die genomen moeten worden in veel gevallen meerdere afdelingen raken. Hier lopen procesverantwoordelijkheid en hiërarchische verantwoordelijkheid door elkaar. Om dit goed te implementeren is een hoge mate van procesvolwassenheid en een heldere afspraak over langs welke lijn geëscaleerd moet worden nodig

Eisen bij zelf ontwikkelen van een AI-oplossing

Vanaf mei 2021 worden zorginstellingen die zelf hulpmiddelen vervaardigen (juridisch gezien) als fabrikant gekwalificeerd, inclusief alle bijkomende verantwoordelijkheden en verplichtingen uit de MDR. Een zorginstelling die zelf medische software ontwikkelt wordt volgens de richtlijn Productaansprakelijkheid (Richtlijn 85/374/EEG) als producent beschouwt. Producten moeten voldoen aan de general safety and performance requirements en de ontwikkelaar is aansprakelijk voor eventuele veiligheidsgebreken.

Bij die verplichting zijn ook eisen aan een kwaliteitsmanagementsysteem, risicomanagement, ontwikkelprocessen en productveiligheid. In geval dat een zorginstelling zelf AI ontwikkelt dient de zorginstelling er tenminste voor in te staan dat aan elk van de volgende voorwaarden wordt voldaan. Dit moet vervolgens ook in het Lifecycle Management proces geborgd zijn.

1. De hulpmiddelen worden niet overgedragen aan of gedeeld met een ander rechtspersoon.
2. De hulpmiddelen worden vervaardigd en gebruikt met inachtneming van een passend kwaliteitsmanagementsysteem (onderdeel van de hele lifecycle - regievoering).
3. Eigen ontwikkeling is alleen nog toegestaan als het medisch hulpmiddel met de vereiste prestatie niet op de markt verkrijgbaar is. De zorginstelling rechtvaardigt in haar documentatie dat aan de specifieke behoeften van de patiëntendoelgroep niet kan worden voldaan, of daaraan niet op een passend prestatieniveau kan worden voldaan, door een op de markt beschikbaar gelijkwaardig hulpmiddel (onderdeel van de ontwikkelfase of verwervingsfase).
4. De zorginstelling verstrekt haar bevoegde autoriteit op verzoek informatie over het gebruik van bedoelde hulpmiddelen, waaronder een rechtvaardiging voor de vervaardiging, de wijziging en het gebruik ervan (onderdeel van een audit tijdens de gebruiksfase).
5. De zorginstelling stelt een openbare verklaring op die de naam en het adres van de vervaardigende zorginstelling bevat, gegevens ter identificatie van de hulpmiddelen, waaruit blijkt dat de hulpmiddelen voldoen aan de algemene veiligheids- en prestatie-eisen (conformiteit aan general safety and performance requirements) (onderdeel van de ontwikkelfase).
6. De zorginstelling stelt documentatie op met uitleg over de productiefaciliteit en het productieproces, het ontwerp en de prestatiegegevens van de hulpmiddelen, met inbegrip van het beoogde doeleind, die voldoende gedetailleerd is om de bevoegde autoriteit in staat te stellen te beoordelen of er wordt voldaan aan de algemene veiligheids- en prestatie-eisen (onderdeel van de hele ontwikkel en de validatiefase).
7. De zorginstelling neemt alle maatregelen die nodig zijn om te garanderen dat alle hulpmiddelen in overeenstemming met de bedoelde documentatie uit voorwaarde 6 worden vervaardigd (onderdeel van de hele lifecycle).
8. De zorginstelling evalueert de ervaring die is opgedaan met het klinisch gebruik van de hulpmiddelen en onderneemt alle vereiste corrigerende acties (onderdeel van de gebruiksfase).

AI impact assessment

Een hulpmiddel om inzichtelijk te maken wat de relevante juridische en ethische normen en afwegingen over de inzet van AI-toepassingen zijn het uitvoeren van een AI Impact Assessment. Het vooraf in beeld brengen en adresseren van de impact van AI draagt bij aan een soepele en verantwoorde introductie van

AI in de zorg. AI Impact Assessment - ECP [11] geeft een kader en stappenplan die helpen bij het inzichtelijk maken van juridische en ethische normen en afwegingen bij de besluitvorming over de inzet van AI. Het weegt het doel en de baten van de toepassing af tegen betrouwbaar, veilig en transparant gebruik van AI enerzijds en het ethisch verantwoord gebruik en afweging van belangen en risico's anderzijds door het aangaan van een dialoog met verschillende belangengroepen. Binnen de zorg zijn dat verpleegkundigen (die met het systeem moeten werken), medisch specialisten en patiëntgroepen. Alles met als doel verantwoording te kunnen afleggen over gemaakte keuzes. De stappen die daarbij worden doorlopen zijn:

1 Bepalen van de noodzaak voor AIIA;
2 beschrijving van het doel van de AI-toepassing;
3 beschrijving van de baten van de AI;
4 beoordelen of doel en de wijze waarop dit doel wordt bereikt ethisch en juridisch verantwoord is;
5 of de toepassing betrouwbaar, veilig en transparant (FACT) is;
6 afweging en beoordeling;
7 vastlegging en verantwoording;
8 periodiek evalueren.

CONFIGURATIEBEHEER VAN AI-MODELLEN

Als het aantal en de ontwikkeling van modellen dat in gebruik is groeit kan het managen ervan niet meer handmatig. Een DSML-platform (Data Science Machine Language platform) helpt daarin. DotScience definieert een aantal criteria waar een AI-model dat productieklaar is aan moet voldoen [2]. Een productieklaar AI-model moet reproduceerbaar, transparant en herleidbaar zijn zodat er verantwoording kan worden afgelegd. Ook moet het samenwerking tussen meerdere gebruikersgroepen uit diverse disciplines ondersteunen en continu onderhoudbaar zijn.

CONFIGURATIE MANAGEMENTGEGEVENS

Centraal in de deployment en het verantwoord gebruik van AI-modellen staat herleidbaarheid en aantoonbaarheid: wat is de herkomst van alle data van het model en hoe performt het model in de loop van de tijd? Daarvoor moet een organisatie een aantal gegevens bijhouden. Sommige gegevens (zoals documentatie, motivatie van gemaakte keuzes) kunnen in aparte documentatiesystemen worden bijgehouden. De volgende gegevens moet een organisatie bijhouden in het AI Lifecycle Management proces[7].

- **Model source informatie.**
  - Versie van de model code (versienummer en de code zelf)
  - Gebruikte features die de werking van het model (mede) bepalen (wanneer de code en versie van de code bewaard blijft kan dit mogelijk ook in de code worden teruggevonden)
  - Versies van gebruikte code/development environment, libraries
    Het bijhouden van de modelversie is meer dan alleen het opslaan van de code in een versiebeheersysteem. Het is ook nodig om een exacte beschrijving toe te voegen van de omgeving (bijvoorbeeld alle Pyhthon libraries die gebruikt zijn inclusief de library versies en de systeem afhankelijkheden die van belang zijn.
  - Documentatie (ontwerp, beslissingen).

- **Datacollection code informatie.**
  - Documentatie over de data preprocessing stappen.
    - Aannames die zijn gedaan bij datacollectie.
    - Documentatie hoe data is verzameld (van welke bronnen, hoe aan wet- & regelgeving is voldaan, proces van verzamelen, betrokkenen).
    - Documentatie over de data cleaning, preprocessing en feature engineering stappen.
    - Hoe data bias is voorkomen.
    - Hoe overfitting wordt voorkomen.
  - Versie van de gebruikte input databestanden, de databestanden zelf en de bron waar de data vandaan komen. Hierbij is er onderscheid in trainingdata, testdata en validatiedata.
  - Versie van code voor de voorbewerking van de data (versienummer en code).

- **Managementinformatie over specifieke model runs.**
  - Wie de run (zie note onder) heeft gedaan.
  - In welke omgeving de run is gedaan.
  - Aantekeningen van ontwikkelaars bij de betreffende runs.

---

[7] Bronnen: [1] - introducing MLOps – how to scale machine learning in the enterprise, [3] – deploying machine learning models: a checklist, [4] - DevOps for ML with Dotscience, en [9] - MDR)

- Betrokken ontwikkelaars bij de runs.
- Tijdstip van de runs.

- **Deployment informatie**
  - Model deployment details zoals type deployment, op welke host de modelrun heeft gedraaid, de runtime, configuratie parameters van bijvoorbeeld het gebruikte tensorflow model.
  - Gebruikte deployment strategie (batch scoring versus real-time scoring[8]).
  - Model versies in gebruik en met welke reden (production deployment, test deployment, canary deployment[9]. NB: in de praktijk zullen meerdere versies tegelijkertijd in gebruik zijn)?
  - Bij tests in de productieomgeving, de selectie van gebruikers die gebruik hebben gemaakt van deze specifieke release/deployment (indien van toepassing).
  - Deployment configuration files.
  - Initialisatiewaarden gebruikt voor het initialiseren van het model.
    In veel gevallen worden de parameters van een AI-algoritme geïnitialiseerd met random waarden. Het gedrag van het model is (mede) afhankelijk van de random initialisatie. Het is daarom van belang de daadwerkelijke random initialisatie te bewaren (voor verantwoordingsredenen en debug mogelijkheden)[10].
  - Status van alle versies van alle modellen.
  - Tracking informatie van de performance van het model ten opzichte van de originele business KPI's.

- **Monitoring informatie**
  - Nauwkeurigheidscore van de modelversie en resultaten van statistische monitoring.
  - Welke metrics worden gebruikt om de performance van het model te monitoren.
  - Monitoring waarschuwings dremelwaarden.
    Wat zijn de drempelwaarden waarop waarschuwingen door het monitoring proces worden verstuurd.
  - Gebruikte driftdetectie technieken voor organisaties die bewezen en uitlegbare algoritmes moeten gebruiken.
  - Welke input driftdetectie technieken gebruikt, moment van evaluatie en uitkomst.
  - In de logging info: Model explanation.
    In some highly regulated domains such as finance or healthcare, predictions must come with an explanation (i.e., which features have the most influence on the prediction). This kind of information is usually computed with techniques such as Shapley value computation and should be logged to identify potential Issues with the model (e.g., bias, overfitting).

In AI onderkennen we twee soorten runs.

1 Data run; dit is de run waarin de data wordt voorbewerkt om de training, test en validatiedata set te creëren. In de DSML moet je de relatie bijhouden tussen bepaalde input data en een intermediate dataset.

---

[8] Bij batch scoring worden hele datasets in één slag door het model verwerkt, zoals in een dagelijks geplande job. Bij real-time scoring wordt alleen een klein aantal datarecords per keer verwerkt. Een voorbeeld daarvan is het verwerken van user input als reactie op een advertentie op een website.

[9] Een manier om risico's tijdens het in productie nemen van modellen te verkleinen is door het gebruik van z.g. "canary releaes". Het idee daarbij is om een stabiele versie van het model in productie te houden, maar daarnaast een (nog) vrij te geven release en een deel van de productie workload naar de canary release te sturen en de performance van deze release te monitoren. Deze werkwijze werkt het best bij real-time scoring.

[10] ML coursera standford university – cost function and backpropagation

2 Model run gaat over de run om het AI-model te trainen. Je traint het AI-model op een bepaalde dataset (misschien de intermediate dataset uit de datarun) waarmee een AI-model wordt gecreëerd. Het is dit model dat in productie wordt genomen en wordt gemonitord.

CONFIGURATIE MANAGEMENTTOOLING: DSML-PLATFORMEN

Een DSML-platform (Data Science Machine Learning platform[11]) is een ontwikkel- en beheerplatform om AI-oplossingen (predictive en prescriptive modellen) te bouwen, in gebruik te kunnen nemen en te gebruiken (embedden in businessprocessen en beslisomgevingen), te monitoren en te onderhouden (aanpassen en opnieuw deployen). Een DSML ondersteunt het integreren van de te maken oplossing in de omliggende infrastructuur, producten en applicaties. Daarnaast ondersteunt het taken in de dat- analyse proces pijplijn.

Features die DSML-platformen ondersteunen omvatten

- Data verzamelen, prepareren/transformeren en exploreren/analyseren.
- Feature engineering: bepalen welke features je van de data wilt gebruiken om je model te bouwen.
- Modelcreatie, training en testen: AI-algoritme ontwikkelen, trainen en het kiezen van de juiste technieken.
- In gebruik nemen van de modellen.
- Onderhoud: managen en monitoren van je oplossingen om de relevantie te meten, aanpassen van je model door samenwerking tussen verschillende disciplines en experts, archiveren en later hergebruiken van projecten.

Gartner biedt een magic quadrant voor DSML-platformen ([7] – magic quadrant for DSML). De markt is erg in beweging. Er komen diverse vragen op bij het kiezen en in gebruik nemen van een DSML.

- **Hoe komt een organisatie tot de juiste keuze van een DSML.**
  De keuze rechtsboven uit het magic quadrant is niet altijd de beste. Er zijn een aantal stappen die een organisatie moet doorlopen om een goede keuze te kunnen maken:
  - bepalen van de eigen data science en AI-volwassenheid;
  - leveranciers en platforms evalueren en afzetten tegen markt trends;
  - eventueel inhuren van skills om een data science team te bouwen.

- **Er zijn verschillende groepen gebruikers van een DSML. Wat zijn hun specifieke behoeften, wat zijn de benodigde expertises, zijn die aanwezig in het ziekenhuis en hoe betrek je ze in het keuzeproces?**
  - Expert data scientists
    Kennis van alle onderdelen van de data science lifecycle. Besteden meeste tijd aan modelontwikkeling voor de ondersteuning van dataengineers die voor data pipelining en delen van de het AI Lifecycle Management verantwoordelijk zijn.
  - Citizen data scientists
    Bouwen ook steeds meer AI-modellen. Hebben niet alle skills van de echte experts. Komen vaak uit rollen zoals dataengineer, applicatieontwikkelaar en applicatiebeheerders.
  - Support rollen
    Omvatten data-engineers, AI-ontwikkelaars, ICT-ontwikkelaars. Zijn niet verantwoordelijk voor

[11] Een DSML is meer een ontwikkelplatform om AI-oplossingen (predictive en prescriptive modellen) te bouwen, te kunnen deployen (embedden in business processen en beslis omgevingen, te monitoren) en te onderhouden (aanpassen en opnieuw deployen). Een DSML ondersteunt ook het integreren van de te maken oplossing in de omliggende infra, producten en applicaties. Daarnaast ondersteunt het taken in de data analyse proces pijplijn.

model bouwen, training en testen, maar vervullen rollen in het opschalen naar operations en ervoor zorgen dat de datakwaliteit behouden blijven.
- "De business", business analyst
  Adresseren business initiatieven en behoeften zoals marketing, sales, finance, R&D.
- Corporate teams
  Kunnen ondersteunen in model building, zijn vaak verantwoordelijk voor definiëren en ondersteunen van end-to-end processen voor bouwen en deployment van DSML-modellen.

- **Voor welke fases in de lifecycle wil je de tooling in gaan zetten?**
  - Niet alle platformen zijn totaaloplossingen. De selectie van welk DSML-platform is afhankelijk van de gewenste functionaliteit. Sommige platformen zijn gericht op ontwikkeling maar niet voor monitoring. Sommige zijn simpel maar niet flexibel. Andere zijn flexibel maar vereisen daardoor ook veel expertise.

Er is een afweging tussen hoeveel vrijheid die een organisatie nodig heeft, de welke en de hoeveelheid expertise in huis is, de gewenste functionaliteit, in welke fase van de AI Lifecycle men het platform wil inzetten, wat een organisatie zelf wil doen of uitbesteedt.

MONITORING AND FEEDBACK

Monitoring is essentieel in de AI Lifecycle. Tijdens de gebruiksfase moet de performance van het model worden gemonitord. Op hoog niveau zijn er drie maatregelen.

1 **Resource performance monitoring**
Verzamelen van IT-metrics zoals CPU load, geheugen gebruik, disk gebruik, netwerk gebruik.

2 **Health check**
Om te kijken of het model daadwerkelijk "up" is en de latency te checken kunnen er simpele queries gestuurd worden op gezette tijden en de resultaten worden gelogd.
Frequentie: één keer per minuut.

3 **Model metrics monitoring**
Dit gaat over het meten van de performance (accuracy) van het model en het vergelijken van het model tegen een andere versie.
Doel: bepalen van de performance degradatie van het model.
Frequentie: één keer per week.

Een van de kernvragen: hoe vaak moet een model opnieuw worden getraind? Dit is mede afhankelijk van het probleemdomein (hoe snel verandert de wereld waarover het model voorspellingen moet doen), de kosten van trainen en de beperking / beschikbaarheid van training data. En van de gewenste kwaliteit, de voordelen van het opnieuw trainen versus die kosten. De benadering zou onderdeel moeten zijn van een continue risicoafweging / kosten-baten afweging.

Er zijn twee monitoring benaderingswijzen:

1 **Ground truth evaluatie**
D.i. het wachten op het optreden van daadwerkelijk "gelabelde" gebeurtenis. D.w.z., dat een gebeurtenis optreedt dat bewezen een bepaald label (labels zoals dat in de training is aangegeven aan trainingdata) heeft. Bijvoorbeeld in geval van fraude detectie, dat een daadwerkelijk frauduleus event optreedt. Of in geval van ziekte voorspelling, dat de ziekte daadwerkelijk wordt aangetroffen.
Monitoring ground truth kent twee varianten:
- op basis van statistische metrics (zoals nauwkeurigheid, F-score, logg loss etc);
- op basis van business metrics zoals kosten/baten assesment. Bijvoorbeeld kredietwaardigheid van een klant.

Ground truth evaluatie is onafhankelijk van het domein waarin de AI-oplossing wordt toegepast. Het nadeel is dat ground truth niet onmiddellijk beschikbaar is en dat ground truth en voorspelling niet gekoppeld zijn. Om de performance van het model te meten is het nodig om ground truth bevinding met de observaties te matchen. Daarnaast is het duur om voor alle observaties ground truth te bepalen. Bijvoorbeeld voor fraude detectie: i.g.v. ground truth zou voor elke transactie moeten worden bepaald of deze frauduleus was. Dat is duur. Echter, een steekproef waarbij alleen hoog waarschijnlijk frauduleuze transacties worden bekeken kan fouten in de voorspelling versterken.

1) Modeldrift detectie
   - Matchen van input data tegen de test data en distributie vergelijken. Hier gaan we hieronder nader op in.

MODELDRIFT

Het gedrag van een model (AI-model, datamodel) kan veranderen tijdens productie als de productie data verandert ten opzichte van de trainingsdata. De degradatie van de performance van het model heet ook wel “modeldrift” of “drift”. Er zijn diverse oorzaken.

- **Datadrift**
  Door het veranderen van de business omgeving, veranderingen in menselijk gedrag, wijzigingen in source data van third parties, datakwaliteitsissues en issues in de data processing pipeline (als er veranderingen optreden in de wijze waarop data wordt verzameld, geanalyseerd) kan er in de loop van de tijd een verschuiving in de dataverzameling ontstaan ten opzichte van de trainingsdata.
- **Conceptdrift**
  Conceptdrift treedt op wanneer de verwachtingen van een correcte voorspelling van het model veranderen. Wat at voorheen als wenselijk of goed werd beschouwd kan nu, onder veranderende omstandigheden, als niet wenselijk worden beschouwd.

IDENTIFICEREN VAN MODELDRIFT

- **Verifiëren van model voorspellingen**
  Identificeren van anomalieën in de voorspellingen kan op meerdere manieren.
  - Output distributie
    Modellen produceren een bepaalde set van scores met een bepaalde waarschijnlijkheidsverdeling. Als die verdeling verandert is dat een potentiële indicatie voor model drift.
  - Logische checks van resultaat waarden
    Als resultaatwaarden in de realiteit altijd binnen een bepaalde grenzen moeten liggen, kijkt een logische check of de voorspelde waarden daadwerkelijk daar binnen liggen. Bv de ontslagtermijn van de IC moet altijd groter zijn dan 0 dagen.
- **Check input datadrift**
  Dit is een van de meest effectieve benaderingen. Monitor inputdata en onderzoek of deze zijn veranderd. Adresseert data- en datapipeline drift. Dit kan goed door een check uit te voeren op statistische variabelen. Kijk of data ranges, “data sparsity”, gemiddelde, median, standard deviatie, max/min waarden zijn veranderd tussen oorspronkelijke testset en huidige dataset. Het is verstandig om criteria vooraf te definiëren waarop je meet op basis waarvan je verschillen gaat meten
- **Check op conceptdrift**
  Kan op dezelfde manier als bij datadrift.

BEST PRACTICES VOOR MONITOREN VAN MODELLEN

- Onderken dat model monitoring een andere aanpak, eisen en andere tooling vereist dan traditionele software en IT infrastructuur monitoring.
  Wanneer het monitoren wordt belegd bij de IT afdeling zal er extra opleiding nodig zijn (datascience, statistiek – zie boven).
  Een andere mogelijkheid om monitoring onder te brengen is bij de data scientists. Ook deze zullen geschoold moeten worden; zo mag een zorginstelling van een ‘willekeurige’ data scientiste niet verwachten dat hij/zij de klinische impact van modellen volledig kan doorgronden of een beeld heeft bij de klinische diagnostiek. Samenwerking met materiedeskundigen (in dit geval medisch personeel) is van belang.
  Essentieel is dat er één functioneel verantwoordelijke komt voor het monitoren van de performance van het AI-model. Deze dient de juiste competenties te hebben, de benodigde tijd om de monitoringactiviteiten uit te voeren, de juiste faciliteiten te hebben (traditionele IT tooling en ervaringen om infrastructuren te monitoren zijn niet geschikt voor model monitoring - gaat veel sneller, is niet gebaseerd op statistische methodieken ed.) en het juiste mandaat te hebben.
- Gecentraliseerde aanpak.

- Monitor alle modellen die in productie zijn vanaf 1 centrale plek. Dit voorkomt silo's en vergroot consistentie. Het creëert een beter beeld welke modellen in gebruik zijn, door wie, waarvoor etc.
- Ontwikkel een consistente set van KPI/metrics om de gezondheid van de modellen te meten. Definities moeten voor iedereen helder zijn.
- Adresseer trends. Meet regelmatig over langere tijd om de model degradatie blijvend in de gaten te houden.
- Automatiseer zoveel als mogelijk. Voordelen: schaling, consistentie in metingen en data scientists kunnen hun tijd besteden aan ontwikkeling ipv het uitvoeren van monitoring activiteiten.

‘RESPONSIBLE AI’ EN KWALITEITSEISEN

De ‘Whitepaper On Artificial Intelligence – A European approach to excellence and trust [5]’ adresseert de EU de potentie van AI en beschrijft dat betrouwbaarheid en het veilig gebruik van AI geborgd moet zijn.

RESPONSIBLE AI

In de eisen die de EU stelt in [5] en ’Ethics guidelines for trustworthy AI [6]‘ staat ethisch gebruik, het respecteren van menselijke autonomie, privacy, reproduceerbaarheid, traceerbaarheid en verifieerbaarheid van AI centraal. In bepaalde toepassingen (bijvoorbeeld een medische toepassing) vereist de wetgeving dat de beslissing waar AI-algoritmen toe komen herleidbaar moeten zijn: op welke basis is het AI-algoritme tot de keuze gekomen. Door de wijze waarop AI-algoritmen worden getraind is dit een uitdaging.

In [5] staan de beleidsregels die de toegankelijkheid en participatie bij ontwikkeling en toepassing van de technologie voor alle sectoren en actoren (overheid, bedrijfsleven en burgers) in de maatschappij mogelijk moet maken. De EU formuleert de zeven belangrijke eisen waar een AI-toepassing aan moet voldoen. Het is zaak dat de governance over het AI-model en de bijbehorende data die implementeert en ook herleidbaar maakt dat er aan die eisen is voldaan. De EU formuleert deze zeven eisen in Ethics guidelines for trustworthy AI [6].

1. Respecteren en ondersteunen van menselijke autonomie en ondersteunen bij het nemen van beslissingen. Mensen moeten geïnformeerd beslissingen kunnen nemen over AI-systemen. De kennis en tools om AI te begrijpen, overzien en ermee te kunnen werken moet ondersteund worden door de toepassing.
2. Technische robuustheid en veiligheid aantonen. Hierbij gaat het erom dat AI-systemen ontworpen moeten zijn o.b.v. risico mijdende werking.
3. Privacy en data governance borgen. Data governance gaat over de kwaliteit en integriteitsbewaking van data, het borgen van de toegang tot data en beschermen van data.
4. Transparantie betreft transparantie hoe beslissingen van AI-modellen tot stand komen (uitlegbaarheid).
5. Diversiteit, niet-discriminatoir en fair.
6. Sociaal en milieu veilig (duurzame AI, zowel sociaal als ecologisch).
7. Accountable. Mechanismen moeten zijn geïmplementeerd zodat verantwoording kan worden afgelegd over AI-systemen en de resultaten van AI, voorafgaand, gedurende en na ontwikkeling, deployment en gebruik.

Omdat AI een hoge mate van autonomie kan hebben is het verantwoord gebruik soms vereist en/of gewenst (meer dan bij ‘standaard software’[12]) zodat:

- de organisatie zich kan verzekeren dat het model wordt ingezet op de manier waarop het was bedoeld (eis in medische toepassingen);
- en de organisatie verantwoordelijkheid kan nemen over inzet en gebruik van het model.

[12] Hoewel de grondlegging van AI in de jaren ’40 – ’50 van de vorige eeuw was, waren de AI-toepassingen tot voor kort oplossingen waarin de kunstmatige intelligentie in standaard software regels was geprogrammeerd. Daarmee verschilden de oplossingen niet fundamenteel van andere “standaard” software programma’s. In de huidige vorm van datagedreven AI zijn de AI-systemen nu zelflerend geworden en hebben de potentie om, situationeel afhankelijk, autonoom beslissingen te nemen.
Meer dan bij ‘standaard’ software zullen AI-oplossingen onderworpen daarom worden aan audits waarbij de uitlegbaarheid, nauwkeurigheid en correctheid van het model aantoonbaar moeten zijn.

Dat houdt in dat ze inzicht moeten hebben in en verantwoordelijkheid nemen over wie en in welke processen het model wordt gebruikt, wat de rol is van AI en die van mensen in het nemen in het beslissingsproces en of aan alle wet- en regelgeving wordt voldaan (zowel voor wat betreft gebruik van het model als de data die het model gebuikt).

Traceability op het voldoen aan deze eisen zowel tijdens de ontwikkeling van het model en gedurende het gebruik en beheer daarvan is onderdeel van het kwaliteitsbeleid. Daar dient de organisatie op toe te zien via interne en externe controles. Dat is complex en moet al tijdens de ontwikkeling van het AI-model worden geadresseerd.

Deze zeven eisen spelen een belangrijke rol in sectoren met een hoog risico (zorg, transport, energie en delen van de publieke sector) en het ontstaan van Responsible AI. Bij het verantwoord gebruik van AI is het van belang dat het ontwerp van een AI-model op een verantwoorde manier is opgezet (intentie) en dat een organisatie daar ook verantwoording over kan en moet afleggen (accountability).

Intentie must haves	Accountability must haves
■ Bewijs dat modellen ontworpen zijn en zich gedragen op de manier waarop het is bedoeld door de organisatie. ■ Verzekering dat data die is gebruikt van een betrouwbare bron komt, dat het betrekken van de gegevens voldoet aan wet- en regelgeving. ■ Voldoende ingebouwde checks om mogelijke bias tegen te gaan. ■ Model is uitlegbaar door mensen.	■ Centrale controle en centraal belegd management en de mogelijkheid om de organisatie te auditen. ■ Geen schaduw IT. ■ Overal beeld welke teams welke data, welke model(versies) gebruiken en hoe. ■ Vertrouwen in betrouwbare data, op een manier verkregen in overeenstemming met wet- en regelgeving. ■ Algemeen en centraal eenduidig beeld en begrip welke modellen worden gebruikt voor welk business proces.

Menselijke benadering voorziet tevens in de juiste tooling en training.

Tabel 2: Traceability 26 eisen voor responsible AI

KWALITEITSEISEN

Zowel de MDR als de IEC 62304 zeggen iets over kwaliteitsmanagement voor medische software. Er zijn algemene eisen die van toepassing zijn bij het ontwikkelen van medische software (en dus ook voor AI-toepassingen in de zorg).

- **MDR**

  De MDR legt deze eisen op voor het maken van medische software hulpmiddelen door fabrikanten die ze op de markt brengen en voor eigen ontwikkelde software. De MDR eisen zijn ook zinvol voor ingekochte software en het toepassen daarvan omdat de zorginstelling uiteindelijk eindverantwoordelijk blijft voor de goede zorg en daarmee het goed functioneren van de AI-oplossing.

  - Een kwaliteitsmanagementsysteem is verplicht (Art 10 MDR Een goed dekkende basis is ISO13485:2016).
    Fabrikanten moeten aantonen te beschikken over een goedwerkend kwaliteitssysteem conform de MDR. Ook voor zorginstanties (die niet zelfontwikkelde software op de markt brengen) is het van belang een goed kwaliteitsmanagementsysteem te hebben om zo de risico's van het implementeren en gebruik van AI in de zorg goed te managen.
  - Risico's moeten beheerst worden door een risicomanagementproces (ISO14791).
    Hieronder vallen de risico's die worden geïntroduceerd door de verkeerde werking van het AI-

model en de risico's in het werkproces. Daarbij gaat het om het uitvoeren en beheersen van risico's in het werkproces waarin het AI-model wordt toegepast/ingezet. Zo kan het data-inzicht dat voortkomt uit performancemonitoring naast noodzakelijke aanpassingen in het AI-model zelf, ook aanpassingen vereisen in het *gebruik* van het model. De opvolging en implementatie dient geborgd te blijven.

- Software moet zijn geclassificeerd (MDR – zie boven). Voor zorginstellingen betekent dit dat als AI-oplossingen verwerven zij moeten verifiëren of de aangegeven classificatie overeenkomt met de toepassing waar zij de AI oplossing voor gaan inzetten.

- **IEC 62304**

  De IEC 62304 definieert de eisen voor de lifecycle van medische software. De extra dimensie die data toevoegt bij AI is nog niet in de IEC 62304 afgedekt. Ontwikkeling van AI resulteert in extra procesactiviteiten.

  - Requirements analysis
    In deze fase moet een zorginstelling aangeven wat de eisen zijn voor de databeschikbaarheid en data toegankelijkheid.
  - Architectural design, detailed design
    Tijdens het ontwerp (architectural design, detailed design) moet je aangeven wat je data-architectuur is. Dat is ook relevant bij de implementatie van het model in de productieomgeving. Waar bevinden zich welke databestanden (data deployment architectuur) en hoe werkt je model (data streaming versus batch processing)? Je ETL-proces en code (data opschonen, modellering, feature selectie (welke features baseer je het model op), hoe je de features selecteert uit de data, je data verrijking (samenvoegen van databronnen).
  - Unit implementation en verification
    In deze fases moet je aangeven hoe het model is getraind (hoe wordt de training dataset, test dataset en validatie dataset bepaald). Testresultaten en datasets moeten met een versie worden bewaard om verantwoording en audits (herleidbaarheid) te kunnen afleggen. Deze verplichting geldt ook bij ingekochte AI-modellen (zie paragraaf 'responsible AI').
  - Herleidbaarheid
    Over herleidbaarheid stelt IEC 62304 dat "traceability" vereist is tussen systeemeisen, software-eisen, softwaresysteemtest en risicomaatregelen (controls) geïmplementeerd in de software. De standaard dekt niet de performance degradatie en risico's af die worden veroorzaakt door mogelijke bias in de ontwikkelfase en concept- en datadrift die ontstaan in de gebruiksfase. Deze worden veroorzaakt door de toevoeging van de datacomponent en niet door de software code zelf. Het implementeren van "tracability" en risico controls in het model zelf is daardoor lastig en moet worden opgevangen in de governance van de lifeycleprocessen.
  - Validatie is buiten de huidige scope van de IEC62304.

GOVERNANCE EN VERANTWOORDELIJKHEDEN

AI Lifecycle Management kan niet worden los gezien van de governance over het AI-model. Het is onmogelijk een model lifecycle te managen, risico's te beheersen en waarde te leveren zonder een goed governance proces. Governance dient te borgen dat gedurende alle fases van de lifecycle de volgende activiteiten zijn geborgd:

- informatieveiligheid en toegang tot data bewaken;
- risicomanagement beleggen en uitvoeren;
- configuratiemanagement activiteiten uitvoeren (registreren en bijhouden van gegevens);
- kwaliteitsbeheersingsmaatregelen uitvoeren (ontwikkelproces en implementatieproces – IEC 62304;
- regie voeren over beheerprocessen;
- bewaken van relevante wet- en regelgeving (MDR, Wkkgz, richtlijn productaansprakelijkheid (85/374/EEG), GDPR/AVG, ISO27001/NEN7510, [general safety and performance requirements], EU ethics guidelines for trustworthy AI).

Bij het toepassen van AI zijn veel rollen betrokken. Het is een multidisciplinair proces en het risico bestaat dat uiteindelijk niemand de eindverantwoordelijkheid heeft. Het is van belang om één proceseigenaar (verantwoordelijk voor de toepassing van het AI-model in het werkproces) en één producteigenaar (die de technisch inhoudelijke kant adresseert) te benoemen.
Als de ontwikkeling en het gebruik van een AI-model bij een andere organisatie is geoutsourcet en wordt uitgevoerd (opdrachtnemer), de afnemende organisatie (opdrachtgever) eindverantwoordelijk blijft voor het gebruik van het AI-model. Dat betekent dat de opdrachtgever verantwoordelijk is voor de het verantwoord gebruik van het model, de herleidbaarheid, aantoonbaarheid van de correctheid van het model en alle daarbij behorende wet- en regelgeving.

GOVERNANCE STAPPEN

Elke organisatie en elk vraagstuk kent een eigen governance. Toch zijn er ook zes algemene governance stappen te benoemen.

1 **Classificeer de use-cases van het gebruik van AI**

Identificeer de use-cases en bepaal welke governance eisen er zijn door het beantwoorden van onderstaande vragen.

- Welke wet- en regelgeving is van toepassing en wat is de impact?
- Wie neemt de resultaten van het model af? Publiek, één of meerdere interne gebruikers?
- Welke service requirements gelden er? 24x7, real-time scoring of batch scoring, ad-hoc runs?
- Wat is de impact van fouten en inefficiënties van het model? Juridisch, financieel, persoonlijk, imago?
- Hoe vaak komen er nieuwe versies van het model?
- Wat is de lifetime van het model?
- Hoe snel is de kwaliteit van het model aan veroudering onderhevig?
- Welke eisen zijn er met betrekking tot uitlegbaarheid en transparantie van het model?

2 **Stel een ethisch standpunt vast**

- Welke ethische aspecten zijn van belang? Gelijkheid, privacy, mensenrechten, werk, democratie, bias?
- Wat is de impact op menselijk en psychisch welzijn?
- Is er een standpunt vereist op financiële impact?

- Hoe transparant moet het beslisproces van het model zijn?
- Hoe graat mag het maximale risico zijn welke de organisatie wil accepteren als het gaat om fouten die door het model worden gemaakt? Wat is het maximum verantwoordelijkheidsniveau?

3 Ken verantwoordelijkheden toe

- Gebruik zoveel mogelijk bestaande structuren.
- RACI-tabel voor het gehele AI Lifecycle Management proces.

Taken	Business stakeholders	Business analysten	Data scientists	Risico / audit	DevOps	Productie exploitatie	Resource admin / architect
Identificatie eisen/doelen/risico's	A/R	C		I			
Data voorbereiding	C	A/R	C				
Data modelering	C	A	R				
Model acceptatie	I	C	C	A/R			
In productie nemen		C	A/R	I	C		
Kapitalisatie			R		R		A
Integratie in bestaande systemen					A/R		
Globale orchestratie		C			R	A	
Gebruikers acceptatie tests	A/R	R	C		I		
Deployment					R	A	I
Monitoring	I	C				A/R	I

Tabel 3: RACI-tabel voorbeeld

4 Stel governance maatregelen vast

Neem classificatie van stap 1 in gedachten. Welke governance maatregelen heeft de organisatie nodig voor elke use-case? Bij governance spelen een aantal overwegingen bij het vaststellen van governance maatregelen: reproduceerbaarheid en traceability, audit en documentatie, preproductie verificatie, transparantie en uitlegbaarheid, bias en testen, monitoring, datakwaliteit, compliance aan wet- en regelgeving.

5 Integreer verantwoordelijkheden in het AI Lifecycle Management proces

Als de governance maatregelen zijn vastgesteld voor alle use-case klassen moeten de maatregelen die ze implementeren opgenomen worden in het AI Lifecycle Management proces.

6 Selecteer de tooling voor centraal governance management → het DSML-platform

Het traceerbaar maken van zowel de ontwikkeling van het model, als de uitvoering van alle governance maatregelen is ingewikkeld. Dit is effectiever als er sprake is van één systeem dat

- het governance proces voor alle analytics use-case klassen centraal definieert en vastlegt;
- de uitvoering van het complete governance proces afdwingt en registreert;
- voorziet in een single point of reference;
- het samenwerken van teams ondersteunt, en dan vooral de overdracht van werk tussen teams;
- integreert met bestande tooling.

7 Kennis overdragen

8 Monitoren en verfijnen

Monitoren van het governance proces start met het begrijpen van de KPI's en de te behalen doelen.

MEER INFORMATIE

Heeft u vragen, wilt u meer weten over AI Lifecycle Management neem dan contact op met Richard Sitters

- richard.sitters@mxi.nl
- 06 30 71 84 19

BIJLAGE 1 BRONNEN

- [1] - Introducing MLOps – how to scale machine learning in the enterprise. Mark Treveil, Dataiku.
- [2] – Requirements to achieve MLOps – Luke Marsden, DotScience (https://www.youtube.com/watch?v=hqxQO7MoQIE&list=PL3vkEKxWd-uvXEsuCAEfQhdvDRc7X_jOx).
- [3] - Deploying Machine Learning Models: A Checklist (https://twolodzko.github.io/ml-checklist).
- [4] - DevOps for ML with Dotscience (https://www.youtube.com/watch?v=HJycJJStXK4).
- [5] – Whitepaper On Artificial Intelligence - A European approach to excellence and trust (https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf).
- [6] – EU – ethics guidelines for trustworthy AI (https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top).
- [7] – Magic Quadrant for Data Science and Machine Learning Platforms Feb 2020 - Gartner https://www.gartner.com/doc/reprints?id=1-1YCR6NY7&ct=200213&st=sb.
- [8] – Gartner's 3-stage MLOps framework- https://www.gartner.com/doc/reprints?id=1-250NWBUX&ct=210113&st=sg.
- [9] – MDR – medical device regulation - Medical Device Regulation - https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32017R0745.
- [10] https://ec.europa.eu/health/sites/health/files/md_sector/docs/md_mdcg_2019_11_guidance_qualification_classification_software_en.pdf.
- [11] – AI Impact Assessment - ECP; https://ecp.nl/wp-content/uploads/2018/11/Artificial-Intelligence-Impact-Assesment.pdf.
- [12] – handreiking nieuwe regelgeving medische hulpmiddelen - https://www.igj.nl/binaries/igj/documenten/brochures/2017/12/12/handreiking-nieuwe-regelgeving-medische-hulpmiddelen-en-in-vitro-diagnostica/040+166+VWS_Med+Hulpmiddelen_Opmaak_V2.pdf".
- [13] – NFU - SW als medisch hulpmiddel - https://www.nfu.nl/qa-software-mdr-ivdr-software-als-medisch-hulpmiddel.