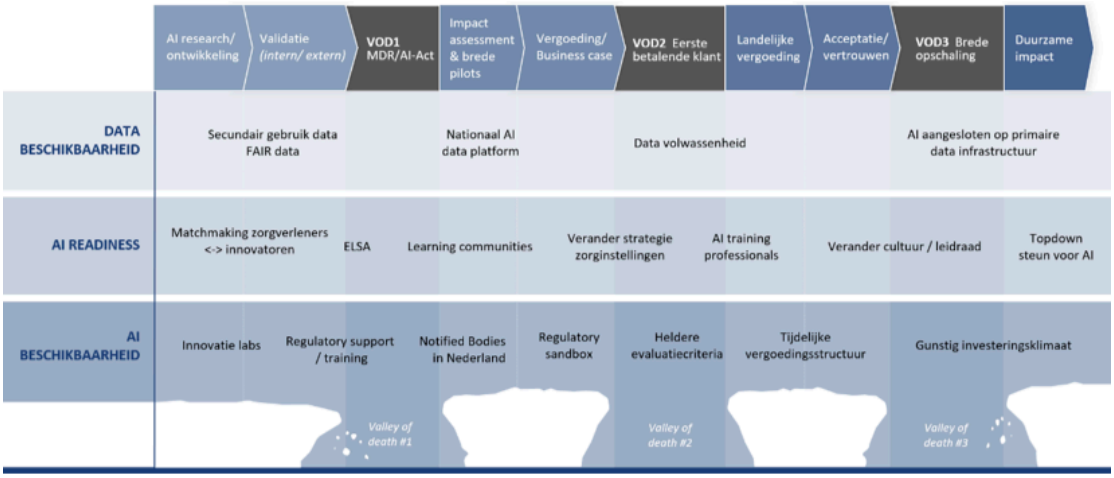
health RI
enabling data driven health & life sciences

Van terpen naar deltawerken voor AI in de zorg

Startnotitie 'AI dataplaformen' (werktitel: AIDA)

1 Aanleiding: oproep voor een nationaal actieplan AI4health

Tijdens de laatste ICT&Health conferentie is een oproep gedaan om te komen tot een nationaal actieplan AI4Health. De kern van deze oproep is dat, ondanks alle lopende initiatieven, er nog steeds veel barrières zijn om data- en AI-gedreven innovaties in de zorg op grote schaal te realiseren. De praktijk wijst uit dat er drie *valleys of death* overkomen (zie W. Gude, P. van Eekeren, en J. Vasseur [1] voor een recent overzicht):



Figuur 1: De drie *valleys of death* die grootschalig gebruik van AI in de zorg in de weg staan.

1. **Van concept tot toegang tot de praktijk.** Voordat grootschalig pilots en marktanalyse mogelijk is moet voldaan worden aan de voorwaarden van de Medical Device Regulation (MDR) en de AI act; 80-90% van de innovaties strandt hier. In de verschillende meetings en workshops die NLAIC georganiseerd heeft met zorginstellingen en innovatoren kwam de MDR/AI ACT bij herhaling als grote bottleneck naar boven (altijd top-3).
2. **Van pilot naar eerste betalende klant.** Dit vereist onder meer een solide business case, betrouwbare toegang tot data en professionele ondersteuning. Dit blijft een hardnekkig probleem, niet alleen voor toepassingen in de ziekenhuiszorg maar komt ook terug bij GGZ en VVT. Binnen de ziekenhuiszorg is het adresseren van deze VoD daarom bv een speerpunt voor de SAZ-ziekenhuizen (Expertisecentrum Zorgalgoritmen).
3. **Van eerste klant naar duurzame opschaling.** Implementatie, acceptatie en validatie ("calibratie") in andere omgevingen dan die van de pilot sites en eerste klant zijn verre van triviaal voor AI-innovaties. De meeste innovaties die de eerste klant weten te bereiken stranden alsnog in deze Valley of Death. Ter verdere illustratie van de huidi-

ge stand van zaken: bij een AI-readiness traject van NLAIC kwam naar voren dat nog geen enkele zorginstelling daadwerkelijk AI-ready is.

2 Behoefte aan een “AI dataplatform” (werktitel: AIDA)

Op dit moment wordt gewerkt aan een nationaal actieplan om deze barrières te adresseren langs vier actielijnen, te weten

1. databeschikbaarheid
2. AI-readiness
3. AI-beschikbaarheid
4. Orkestratie.

Binnen de actielijn databeschikbaarheid is in de afgelopen jaren het nodige in gang gezet, waaronder het systematisch toepassen van FAIR principes, een helder en breed gedragen ethisch en juridisch kader en het realiseren van gedistribueerde toegang tot data. Tegelijkertijd kunnen we constateren dat het ontbreekt aan voldoende gedetailleerde afspraken om te komen tot een ecosysteem van ‘AI dataplatformen’ waarop effectief onderzoek kan worden gedaan, algoritmes kunnen worden ontwikkeld etc. Een dergelijk platform is een geïntegreerd systeem dat AI-ontwikkelaars ondersteunt met toegang tot data, modellen en andere hulpmiddelen om AI-projecten te ontwikkelen en te verbeteren. Dit platform biedt toegang tot essentiële bronnen, zoals datasets voor het trainen van AI-algoritmen, basis AI-modellen en diensten zoals een ELSA-desk voor ethische en juridische vraagstukken.

Dergelijke ‘AI dataplatformen’ zijn in feite specifieke vormen van beveiligde verwerkingsomgevingen zoals in in de datagovernance verordening artikel 2 lid 20 is gedefinieerd:

> “beveiligde verwerkingsomgeving”: de fysieke of virtuele omgeving en organisatorische middelen om te zorgen voor de naleving van het Unierecht, zoals Verordening (EU) 2016/679 (de Algemene verordening gegevensbescherming), met name wat betreft de rechten van datasubjecten, intellectuele-eigendomsrechten, en handels- en statistisch geheim, integriteit en toegankelijkheid, alsook van het toepasselijke nationale recht, en om de entiteit die de beveiligde verwerkingsomgeving biedt in staat te stellen alle gegevensverwerkingsactiviteiten te bepalen en er toezicht op te houden, met inbegrip van het tonen, opslaan, downloaden en exporteren van gegevens en het berekenen van afgeleide gegevens door middel van computeralgoritmen;

Onder de werktitel “AIDA” willen we in de komende periode met experts, belanghebbenden en veldpartijen te komen tot een gecoördineerde realisatie van een dergelijke nutsvoorzieningen. Deze startnotitie en website is bedoeld als interactief discussie document, ter ondersteuning van dit consultatieproces.

Op dit moment zijn er ontzettend veel ontwikkelingen gaande die relevant zijn voor AIDA. In het onderstaande geven we een samenvatting van relevante initiatieven, waarna we een eerste scoping presenteren en vragen formuleren als start voor de discussie.

3 Europese context

3.1 Simpl

Het Europese Simpl is een *"... is an open source, smart and secure middleware platform that supports data access and interoperability among European data spaces."* In januari 2025 zijn gedetailleerde architecturen en functionele beschrijvingen van **Simpl-Open** opgeleverd om, zijnde een open-source software stack waarmee we deze generieke integratie laag op een gestandaardiseerde manier willen realiseren.

De Simpl-Open architectuur is een gedetailleerde uitwerken van bestaande referentie architecturen en is compatible met:

- De Data Spaces Support Center (DSSC) Blueprint (versie 1.5)
- De International Data Spaces Reference Architecture Model (IDS-RAM) (huidige versie 4, draft versie 5)

3.2 AI Factories

Vanuit de EU wordt ingezet op de realisatie van AI Factories, zijnde *"... leverage the supercomputing capacity of the EuroHPC Joint Undertaking to develop trustworthy cutting-edge generative AI models."* Dit initiatief zit meer in de hoek van High Performance Computing, en wordt ook getrokken vanuit de EuroHPC Joint Undertaking om betrouwbare, *state-of-the-art* generatieve AI modellen te ontwikkelen.

SURF is op dit moment penvoerder om namens Nederland een aanvraag in te dienen om een grootschalige Nederlandse AI-faciliteit te realiseren.

3.3 InvestAI

Europa heeft op 11 februari het InvestAI-initiatief aangekondigd om 200 miljard euro aan investeringen te mobiliseren. Dit initatief is o.a. gevoed door CAIRNE, de *Confederation of Laboratories for Artificial Intelligence Research in Europe* dat al langer pleit voor een CERN voor AI. Op dit moment is het nog onduidelijk wat deze initiatieven concreet zullen betekenen voor AIDA.

3.4 TEHDAS2

TEHDAS2 is een *"... joint action prepares [that] the ground for the harmonised implementation of the secondary use of health data in the European Health Data Space – EHDS."* Het is een Europees, zorg-specifiek programma, en veel van de werkpakketten zijn direct relevant voor AIDA. Een van de zaken die nader uitgezocht moeten worden is hoe de generieke architectuur van Simpl Open (sector onafhankelijk) zich verhouden tot de ontwerpprincipes en keuzes die binnen TEHDAS2 zijn gemaakt.

4 Nederlandse context

4.1 Twiin

Twiin is een samenwerkingsverband waarin zorgaanbieders, leveranciers en partners werken aan het Twiin Afsprakenstelsel. Dit Afsprakenstelsel omvat gedetailleerde uitwerkingen over alle lagen van de architectuur voor het beschikbaar maken van gezondheidsgevens. Zo zijn duidelijke keuzes gemaakt om bijvoorbeeld te werken met FHIR-gebaseerde *notified pull*, het gebruik van BSN voor identificatie, het gebruik van eIDAS voor authenticatie en OAuth2 voor autorisatie.

4.2 NUTS

NUTS ontwikkelt en beheert een nutsvoorziening die het delen van zorg-gerelateerde informatie over het Internet mogelijk maakt op een vertrouwelijke, veilige en toegankelijke manier. Het Nuts-netwerk maakt gebruik van internationale standaarden om een vertrouwenslaag op het Internet te realiseren. Die standaarden zijn geïmplementeerd in de Nuts-node: Open Source software die zonder licentiekosten door elke IT leverancier gebruikt kan worden. Leveranciers mogen er ook voor kiezen om zelf de standaarden te implementeren.

4.3 Health RI nodes

Last but certainly not least hebben de Health RI nodes in de afgelopen jaren het nodige ontwikkeld. Binnen de nodes is gewerkt aan verschillende oplossingen en aandachtsgebieden, waaronder het myDRE Trusted Research Environment, het molgenis data platform gericht op wetenschappelijk onderzoek en bioinformatica, het BBMRI-NL beeldanalyse platform om er een paar te noemen.

5 Scope en vraagstelling AIDA

- In analogie: de huidige stand van zaken zijn gefragmenteerde terpen, waarbij AI-gedreven innovaties vaak van worden ontwikkeld op niet gestandaardiseerde infrastructuur (terpen)
- In plaats van terpen, willen we naar een deltawerken voor AI4Health.
  - Deltaplan: het ontwerp van een gestandaardiseerde en interoperabele “AI dataplatformen” waarmee komende jaren generieke, landelijk dekkende voorzieningen gerealiseerd kunnen worden
  - Deltawerken: de realisatie van het Deltaplan, met het perspectief dat er niet één platform is, maar een ecosysteem van platformen die interoperabel zijn. Net zoals dat de Deltawerken een ecosysteem van dijken, waterkeringen is.

Vragen die we willen beantwoorden:

- Hoe komen we tot harmonisatie, en waar nodig standaardisatie van verschillende oplossingsrichtingen op maximale interoperabiliteit te realiseren.
- Wat zijn de essentiële generieke functies om het vertrouwensmodel goed te implementeren?
- …

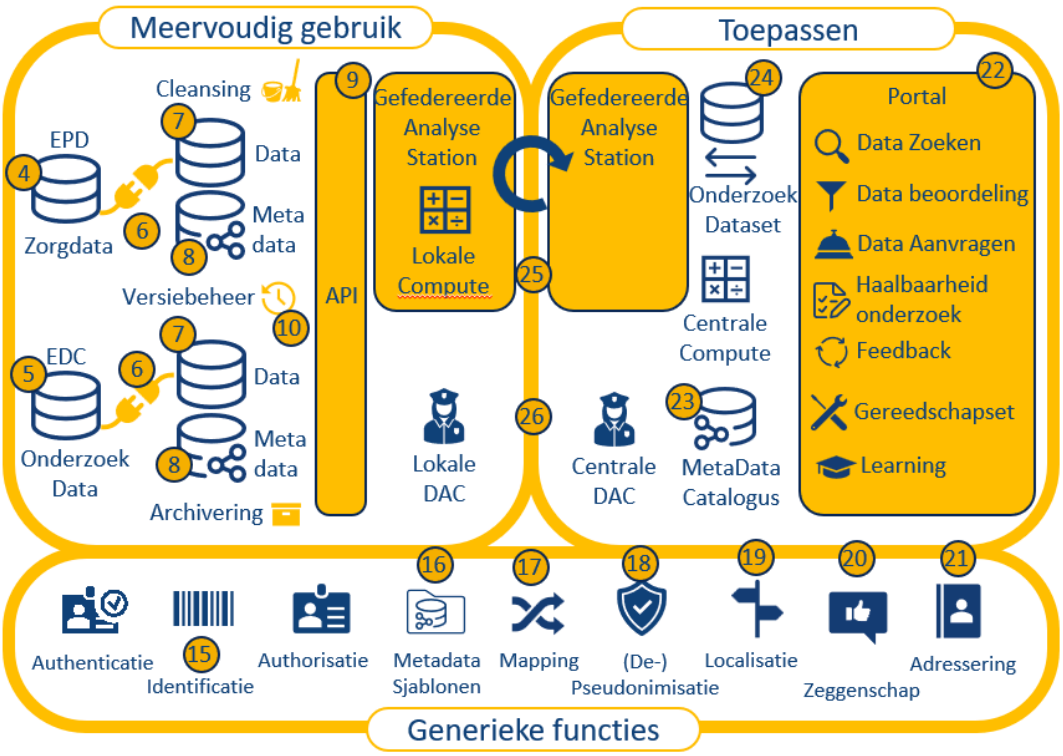
Vooral ook zaak om eenduidige terminologie en component beschrijvingen te gebruiken.

We zien drie thema’s waarlangs we de discussie tav AIDA willen voeren:

1. Onderscheid verschillende vormen van *Secure Processing Environments (SPEs)*
2. Koppelvlak tussen data en SPEs
3. Orchestratie van infrastructuur

6 Thema 1: soorten SPEs

Versie 4 van de Health-RI wiki beschrijft de gezondheidsdata-infrastructuur voor onderzoek, beleid en innovatie. Deze infrastructuur is specifiek gericht op secundair gebruik, en is een verbijzondering van de algemene gezamenlijk gezondheidsdata architectuurmodel. Binnen deze architectuur zijn reeds twee soorten van Secure Processing Environments benoemd, namelijk veilige verwerkingsomgevingen) en gefedereerde verwerkingsomgevingen.



Figuur 2: Conceptuele architectuur voor secundair gebruik

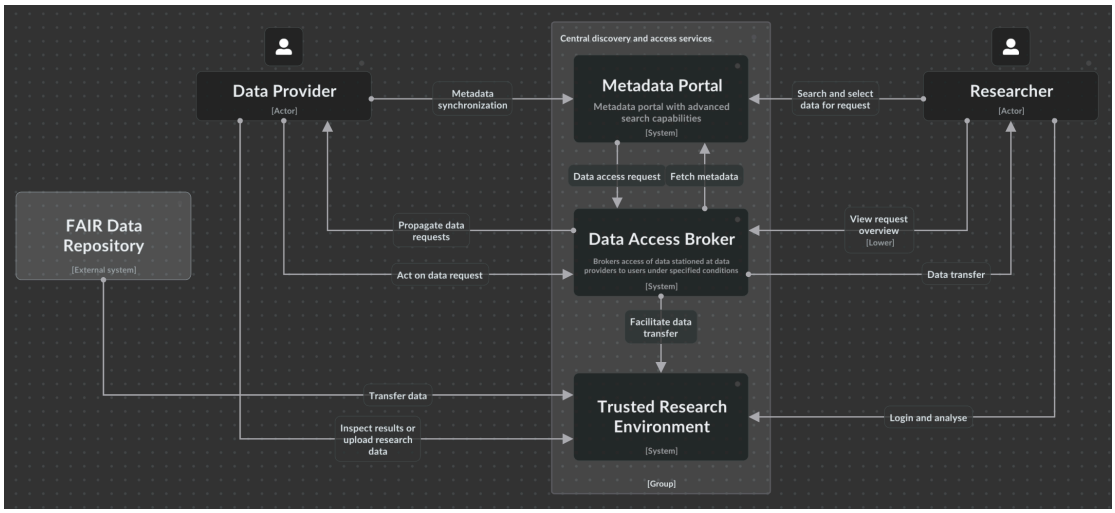
De basis gedachte achter AIDA is dat er *verschillende soorten van secure processing environments (SPEs)* zullen zijn. Daarbij introduceren we een derde type, de hybride SPE. In dit document hanteren we de namen van deze drie typen om expliciet onderscheid te maken; we zullen spreken van SPEs in het algemeen als we alle drie de soorten bedoelen. We geven een korte schets en voorbeelden van elk type.

Tabel 1: Drie soorten van Secure Processing Environments die binnen de scope van AI-DA vallen.

Centrale SPE	• vaak benoemd als Trusted Research Environment • veel bestaande voorbeelden, zie o.a. EOSC-ENTRUST • machine learning op tabulaire data mogelijk • *statistical disclosure control* op output
Federated SPEs	• decentrale benadering cf. personal health train • oorspronkelijk bedoelt voor machine learning • kan ook gebruikt worden voor statistische analyse • moeilijker om mee te werken
Hybride SPE (H-SPE)	• Combinatie van bovenstaande technieken • Nodig om gebruik te maken centrale rekencapaciteit • Gedachte om gebruiksgemak te verbeteren

6.1 Centrale: SURF Secure Analysis Environment (SANE)

SURF Secure ANalysis Environment (SANE) is een virtuele, volledig afgeschermde omgeving waarop met vooraf goedgekeurde analyse software draait en toegang tot sensitive data wordt gegeven (Figuur 3). In onderstaand overzicht is SANE gepositioneerd als TRE, waarmee de data aanbieder controle houdt over de data die ter beschikking wordt gesteld en waarmee de data consumer op een makkelijke manier toegang krijgt. SANE biedt functionaliteiten op het gebied van *Research Analytics*, *Secure Data Zone* en *Data Discovery*. Meer details staan in de blauwdruk van EOSC-ENTRUST.



Figuur 3: Positionering van SANE binnen een generieke data space architectuur.

Belangrijk kenmerk van SANE en andere TREs is dat de data fysiek naar de *Secure Data Zone* wordt gekopieerd. Naast het veilig aanbieden van data (als data houder), is dit ook het mechanisme waarmee data gebruikers hun eigen data mee kunnen nemen naar de TRE, om daarbinnen te koppelen aan andere data. Dit gebeurd vaak met gebruik van pseudonimisering. De CBS microdata omgeving werkt op een vergelijkbare manier.

Binnen de blauwdruk van EOSC-ENTRUST wordt gesproken over *Federation Services* tussen verschillende TREs. Daarbij gaat het om data federation: data wordt (tijdelijk) van de ene naar de andere TRE gekopieerd zodat het daar in combinatie verwerkt kan worden. Data federation als mechanisme is anders dan federated learning: daarbij worden de berekeningen decentraal uitgevoerd en alleen de resultaten centraal gedeeld (zie hieronder). Federated learning is met name nuttig voor horizontaal gepartitioneerde data. Voor verticaal gepartitioneerde data, is data federation zoals beschreven door EOSC-ENTRUST meer geschikt.

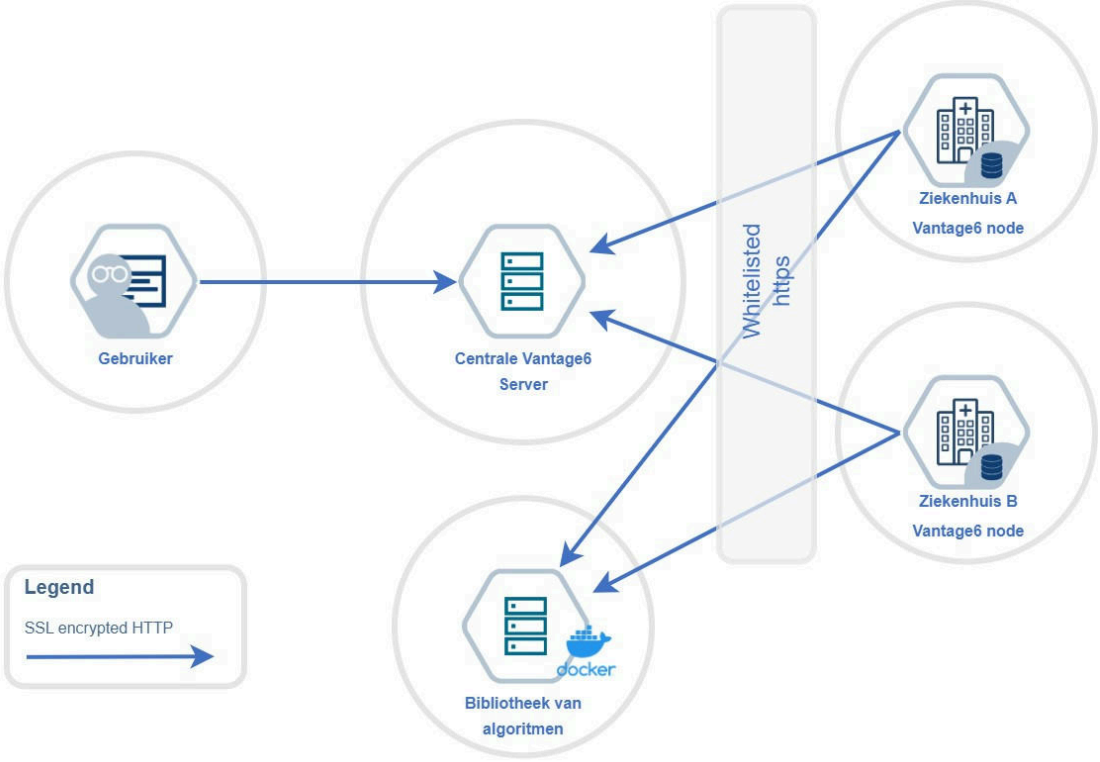
Er zijn meer voorbeelden van centrale SPEs. Zo hebben de meeste *National Statistics Offices (NSOs)* zoals het CBS een microdata omgeving. Alhoewel deze omgevingen zijn opzet voordat machine learning zijn intrede deed, bieden de meeste microdata omgevingen nu ook al de mogelijkheid om 'lichte' algoritmes te trainen op tabulaire data. Een rapport van de Verenigde Naties beschrijft dat deze omgevingen in toenemende mate ook worden uitgebreid met nieuwe AI-technieken, zoals privacy-enhancing technologieën (PETs) ([2]).

Er zijn ook voorbeelden van centrale SPEs specifiek voor de zorg:

- Het Finse Social and Health Data Permit Authority (Findata) biedt met Kapseli een landelijke voorziening aan dat aanvullend is op het Finse NSO.
- Het Mayo Clinic Platform_Discover is een voorbeeld van een platform binnen een netwerk van zorg leveranciers.

6.2 Federated SPEs: PLUGIN/vantage6

Federated learning (FL) als concept staat ook wel bekend als de Personal Health Train (PHT) en wordt in toenemende mate gebruikt in de zorg [3]. De term FL wordt vooral gebruikt om naar het technische concept te verwijzen, terwijl PHT verder gaat in het definiëren van afspraken rondom het gebruik van FL. In Nederland is een actieve community rondom het vantage6 platform dat wordt gebruikt in het PLUGIN project, en internationaal in 50 andere netwerken. Het basis principe is dat bij FL de gegevens op afzonderlijke 'data stations' verschillende apparaten blijven die participeren in de federated SPE. Om deze data te gebruiken voor machine learning, wordt bij elk data station het algoritme lokaal c.q. afzonderlijk getraind. Vervolgens worden alleen de resultaten van het algoritme - bijvoorbeeld geaggregeerde statistieken of de modelparameters van het neurale netwerk - gedeeld met een centrale server. Deze server combineert de resultaten van afzonderlijke modellen tot één model, welke vervolgens met alle deelnemers van het federated SPE gedeeld wordt.



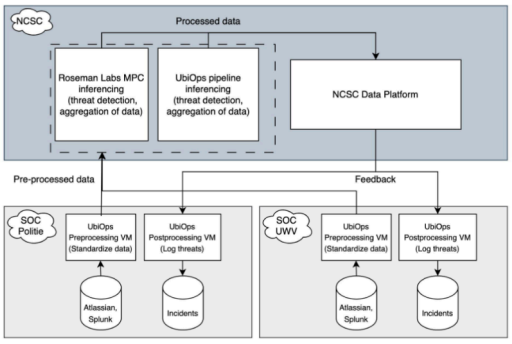
Figuur 4: Overzicht van vantage6 infrastructuur zoals in PLUGIN is gerealiseerd.

Het PLUGIN project heeft een federatieve SPE van tientallen ziekenhuizen gerealiseerd, waarbij gebruik wordt gemaakt vantage6 als platform. Belangrijkste kenmerken van deze opzet zijn:

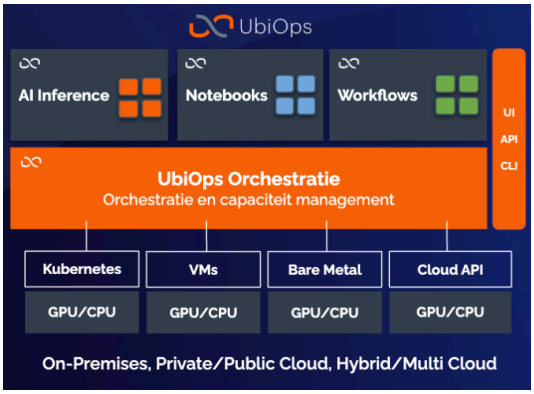
- Sterke nadruk op veiligheid en privacy, door gebruik van beveiligde containers en virtual private networks in de basis infrastructuur
- Ontzorgen van deelnemende ziekenhuizen, waarbij gebruik wordt gemaakt van een generieke Linux server in het IT domein van het ziekenhuis dat als basis dient om de opslag en rekenkracht voor de FLN te realiseren. Afhankelijk of een ziekenhuis mee doet als trainingsziekenhuis of alleen als gebruiker dient een zwaardere resp. lichtere Linux server te worden geconfigureerd
- Voor elk project wordt de berekening c.q. machine learning expliciet 'verpakt' in een Docker container, zijnde de berekening die daadwerkelijk wordt uitgevoerd.
- De generieke Linux server wordt ook gebruikt om dashboard, informatieproducten etc. te hosten binnen het IT domein van het ziekenhuis

Het gebruik van een standaard data model (op de data stations) is een belangrijke randvoorwaarde om federated SPEs te kunnen doen. Naast het gebruik van vantage6 als kerntechnologie, heeft PLUGIN ervoor gekozen om FHIR als data standaard te gebruiken. Hiertoe is een FHIR profiel in ontwikkeling die aansluit op de bestaande ZIBS2020 bouwstenen. Meer achtergrond over de keuze voor FHIR is te lezen in dit artikel. Andere voorbeelden van federated SPEs zijn hier te vinden.

6.3 Hybride SPE: UbiOps en Roseman Labs



Figuur 5: Hybride samenwerking tusssen SOCs



Figuur 6: UbiOps orchestratielaag

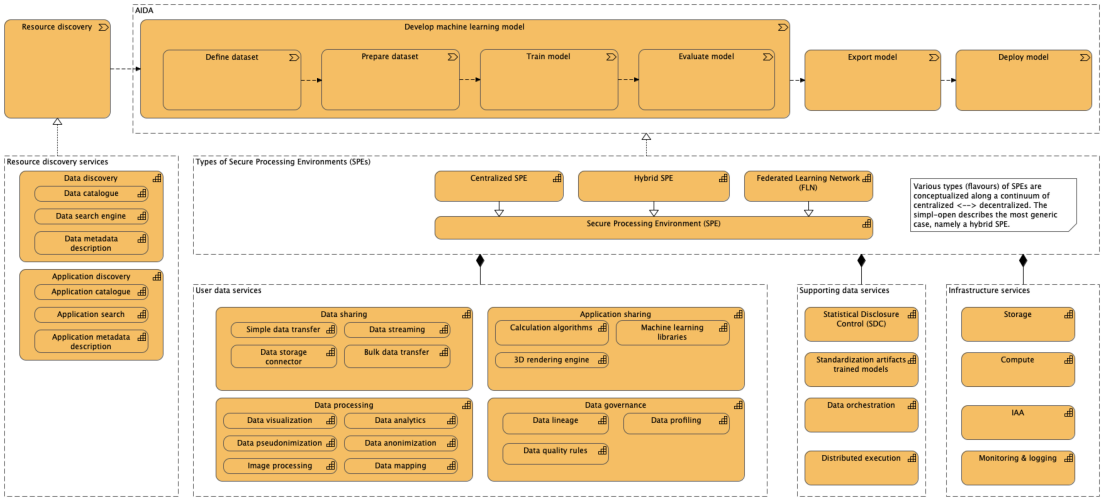
De hybride SPE is een nieuwe oplossingsrichting die we willen verkennen en realiseren in AIDA. Er zijn minder concrete voorbeelden van een dergelijke opzet. UbiOps en Roseman Labs hebben een oplossing die er het dichts bij in de buurt komt (Figuur 5). In analogie met data spaces, gaat het hier om het verbinden van verschillende Security Operating Centra (SOC) in de beveiligingsketen (NCSC, politie, UWV etc.) In een hybride SPE kunnen *compute* (rekenkracht) en *storage* (opslag) zowel lokaal als centraal worden uitgevoerd. In deze architectuur worden bijvoorbeeld pre-processing van data decentraal uitgevoerd in de SOCs in de onderste laag van Figuur 5. De resultaten van deze pre-processing gaan naar het centrale platform, in dit geval het NCSC. Daar kunnen vervolgens ook weer (vervolg-)berekeningen worden uitgevoerd, op de *storage* en *compute* die beschikbaar zijn in de omgeving van de NCSC.

Deze opzet bij de NCSC is mogelijk gemaakt door UbiOps, een platform leverancier die de orkestratielaag biedt waarmee alle *storage* en *compute* centraal wordt beheerd (Figuur 6). Een belangrijk ontwerpprincipe van deze orkestratielaag is dat het verschillende soort fysieke infrastructuur kan managen, variërend van *bare metal* servers, Kubernetes cluster, virtuele machines, public cloud infrastructuur etc.

Een ander onderscheidende kenmerk van deze opzet is dat de centrale dataverwerking ook onder encryptie uitgevoerd kan worden via het Roseman Labs MPC (Multiparty Computation) platform. Door berekeningen *in-the-blind* uit te voeren, zijn de data extra beschermd.

Deze opzet van hybride SPE is in lijn met de recent gepubliceerde Simpl-Open architectuur. Deze aanpak biedt de mogelijkheid om over verschillende SPEs tot harmonisatie en interoperabiliteit te komen. Denk bijvoorbeeld aan een situaties waarbij een analyse kan worden uitgevoerd over verschillende Health-RI nodes heen. In Hoofdstuk 8 gaan we hier dieper op in.

6.4 Strategy view op AIDA



Figuur 7: De Strategy view als startpunt voor de discussie.)

Gegeven deze verschillende soorten SPEs is een eerste *strategy view* van AIDA geschetst in Figuur 7. De *value stream* elementen zijn beschreven in termen van het ontwikkelproces van CRISP-DM. Deze *value stream* kan worden gerealiseerd met behulp van verschillende soorten SPEs. De modulaire *capabilities* zijn de verschillende functionele bouwblokken die in een SPE gebundeld/aangeboden kunnen worden. De gedachte is dat elke SPE, afhankelijk van de context, doelgroep etc. een eigen configuratie van *capabilities* heeft.

7 Thema 2: koppelvlak datastores en SPE

- Resource discovery binnen Simpl Open
- Onderscheid tussen datastores en datasets: FAIR gaat alleen over datasets
- Voor real-world data wil je toe naar standaard manier om snel te verkennen of een bepaalde datastores interessant is voor een toepassing –> verkenner functie
- Elke keer dat je de query runt, krijg je een iets andere datasets omdat nieuwe datapunten kunnen zijn binnengekomen. Maar de logica van inclusiecriteria is hetzelfde

Voorbeelden hoe je op gestandaardiseerde manier datasets kan definieren vanuit een datastore

- FHIR ecosysteem: Bulk FHIR en SQL-on-FHIR: je kan subsets en queries definieren
- openEHR ecosysteem: Archtetype Query Language (AQL)
- OMOP gebruikt SQL (geen OMOP-specifieke query language) direct op de relational database

8 Thema 3: orchestratie van infrastructuur

Kenmerken van het NCSC platform zien we daarin terugkomen als ontwerpprincipes, waaronder:

- Het gebruik van *agents* als mechanisme voor het orkestreren van allerlei *compute* en *storage* binnen een data space en tussen een data space
- Mogelijkheid om over verschillende fysieke locaties een data space op te zetten

- Sterke nadruk op Identificatie, Authenticatie en Autorisatie (IAA) functies, waarvoor standaarden gebruikt moeten worden
  - Tier 1: IAA van gebruikers
  - Tier 2: IAA voor machine-to-machine orkestratie
- Naast gebruik van catalogi voor data en applicaties wordt ook het gebruik van een infrastructuur voorgeschreven, zodat daarmee inzichtelijk is welke *compute* en *storage* beschikbaar is binnen het netwerk.

Bibliografie

[1] W. Gude, P. van Eekeren, en J. Vasseur, 'AI Monitor Ziekenhuizen 2024', 2024. [Online]. Beschikbaar op: https://mxi.nl/uploads/files/publication/ai-monitor-2024.pdf

[2] 'The PET Guide', 2023. Geraadpleegd: 22 januari 2025. [Online]. Beschikbaar op: https://unstats.un.org/bigdata/task-teams/privacy/guide/

[3] Z. L. Teo *e.a.*, 'Federated Machine Learning in Healthcare: A Systematic Review on Clinical Applications and Technical Architecture', *Cell Reports Medicine*, vol. 5, nr. 2, p. 101419-101420, feb. 2024, doi: 10.1016/j.xcrm.2024.101419.