Paper RE04

Use-Case: Ensuring Governance and Traceability of RWD from Source to Regulatory Submission

Michael Kolzet, Eqty Life Sciences, Chapel Hill, North Carolina
Berber Snoeijer, ClinLine, Leiderdorp, The Netherlands

ABSTRACT

The goal of real-world data (RWD) is to be used as evidence (RWE) in regulatory submissions. The governance and traceability of this RWD are paramount, ensuring integrity, reliability, and compliance for regulatory submission. This paper explores challenges and best practices associated with governing RWD throughout its lifecycle, from collection at the source to submission, providing regulators proof of source reliability without regulators needing to access third-party source data.

Building upon the ideas of multiple sponsors and regulators through working group collaborations, we developed a method to demonstrate principles and best practices in data governance, quality, and traceability. Utilizing a data standard, code, and software-agnostic tool that created cryptographic certificates for each data set and then weaved them together to form a verifiable data mesh, an Alzheimer cohort was created for a mock submission. Based on patients selected from FHIR electronic health record (EHR) resources, data was traced through its transformation to OMOP+ then anonymized, simulating a data vendor process. Subsequently, fit-for-purpose selection and then transformation to SDTM was conducted simulating sponsor/CRO processes.

Through this paper, we will demonstrate how data reliability is now verifiable by reviewers and how new open-source cryptographic technologies automate data lineage and contemporaneously document adherence to governance controls, providing the highest confidence for data and process reliability.

INTRODUCTION

Our paper supports an open-source, platform-agnostic deterministic approach for regulators to verify data reliability during capture, curation, mapping, and transformations (i.e. anonymization, statistical or AI/ML). By focusing on a specific RWE use-case, we demonstrate how cryptographic certificates mathematically prove the integrity of data for regulatory submission, as well as automate data lineage and document contemporaneous all tasks down to the individual datapoint level. With verification of data, code or actions down to the hardware level, this method proves a sponsor's compliance to regulations and supports transparency and explainability of complex data workflows.

Like fingerprints, cryptographic certifications generate unique derivates systematically, making any data point generated by DHTs, applications, or systems a trusted source of truth. Weaving these encrypted and immutable certificates together, a verified data layer is created over entire RWE/AI workflows. Without the need to access third-party data, regulatory reviewers are provided an end-to-end audit trail for submitted data, fundamentally shifting how data reliability can be now proven while preserving privacy and ensuring utilization rights.

Certifying data, transformations and controlling data utilization rights at the variable level based on flexible patient consent, from capture through submission, sponsors, CROs and data providers now have the tools to prove to reviewers they acted responsibly. Providing auditors read-only rights to a sponsor's cryptographically verified data mesh, reviewers now have the capability to seamlessly backward data map, click into data tables, trace data and processes backward to the source. Seeing data provider, CRO and sponsor adherence to pre-specified governance controls, which should be determined during protocol creation, auditors now have end-to-end lineage that is verifiable at code or hardware levels. By providing reviewers the tools to trust yet verify data, the highest confidence is given to sponsors RWE, and reviewers may be able to answer many queries themselves, accelerating review timelines.

USE CASE DESCRIPTION

Although adaptable to provide lineage, traceability and governance across transformation workflows, including AI/ML based abstraction, for this simplified use-case we mimicked patient data from an EHR being licensed to create submission-ready datasets. We used FHIR patient files generated from Synthea data [1] and mapped them to structures similar to OMOP [2] for further selection and fit-for-purpose assessments. Aligning to observational research requirements, data vendors often utilize OMOP common data model (CDM) or similar structures. This exemplifies the transformation of source Electronic Health Records (EHRs) to a CDM, enabling the execution of identical queries (without any substantial modifications) on multiple datasets [3]. After the cohort and fit-for-purpose selections of the patients, the data of the patients used for submission was transformed to SDTM for study analysis and submission purposes.

USING OMOP AS A CDM FOR PATIENT AND DATA SELECTION

As described in the FDA guideline for Assessing Electronic Health Records (EHR) and Claims data [3], it is important to standardize data from a variety of EHR data sources into a common format to ensure interoperability across all sites providing data. Although FHIR is a good standard for data exchange, many EHR systems limit FHIR extraction to a file per patient, which limits its capability for use in selection and fit-for-purpose assessments. Therefore, for this purpose we used the OMOP [2] observational CDM to transform the data for these purposes.

This approach was favored above the direct transformation from FHIR to SDTM for multiple reasons.

1) Transformation directly from FHIR to SDTM implies cumbersome transformations of data needed for selection and data source fitness for purpose evaluation but not for submission. It would also include the transformation of patient data that are not included in the study to be able to assess whether they are fit or not.
2) Although beneficial for the selection of patients, electronic health data includes several variables that are not included in SDTM. While, for traceability purposes, OMOP includes source as well as standardized values which improves the ability of selecting and doing bias assessments regarding source collection practices or data standardization practices. This also aids the regulatory requirement to have adequate processes in place to ensure confidence in the resultant data like electronic documentation [4].
3) OMOP structure and comparable data vendor structures are fairly basic and once understood, easy to use for selecting data and patients.

USE CASE PROCESS

The data flow process that aligns with our use case is presented in Figure 1.

Step 1- The different steps included in the proof of concept start with the selection of patients from the source at the health care location that is holding the electronic health records (EHR). This selection will be based on the FHIR files available at the source.
Step 2- Once selected and aligned with the health care providers, the files can be transferred to the data provider
Step 3- At the location of the data provider, the FHIR data will be extracted and mapped to an OMOP-like structure for easy selection, mapping and storage.
Step 4- The data in these files will be further deidentified using hashing techniques and date shifting. When needed, this technique can be utilized again on the source data to subsequently get the same anonymized ids and thus enable traceability back to the source.
Step 5- Based on a sponsor request, a subset of the data is selected
Step 6- Data is sent to the sponsor
Step 7- The sponsor can then apply additional filtering based on data inspections, apply imputations, and perform matching with the interventional arm.
Step 8- Finally the data of the selected patients will be mapped to SDTM for integrated analysis with the interventional trial arm data.

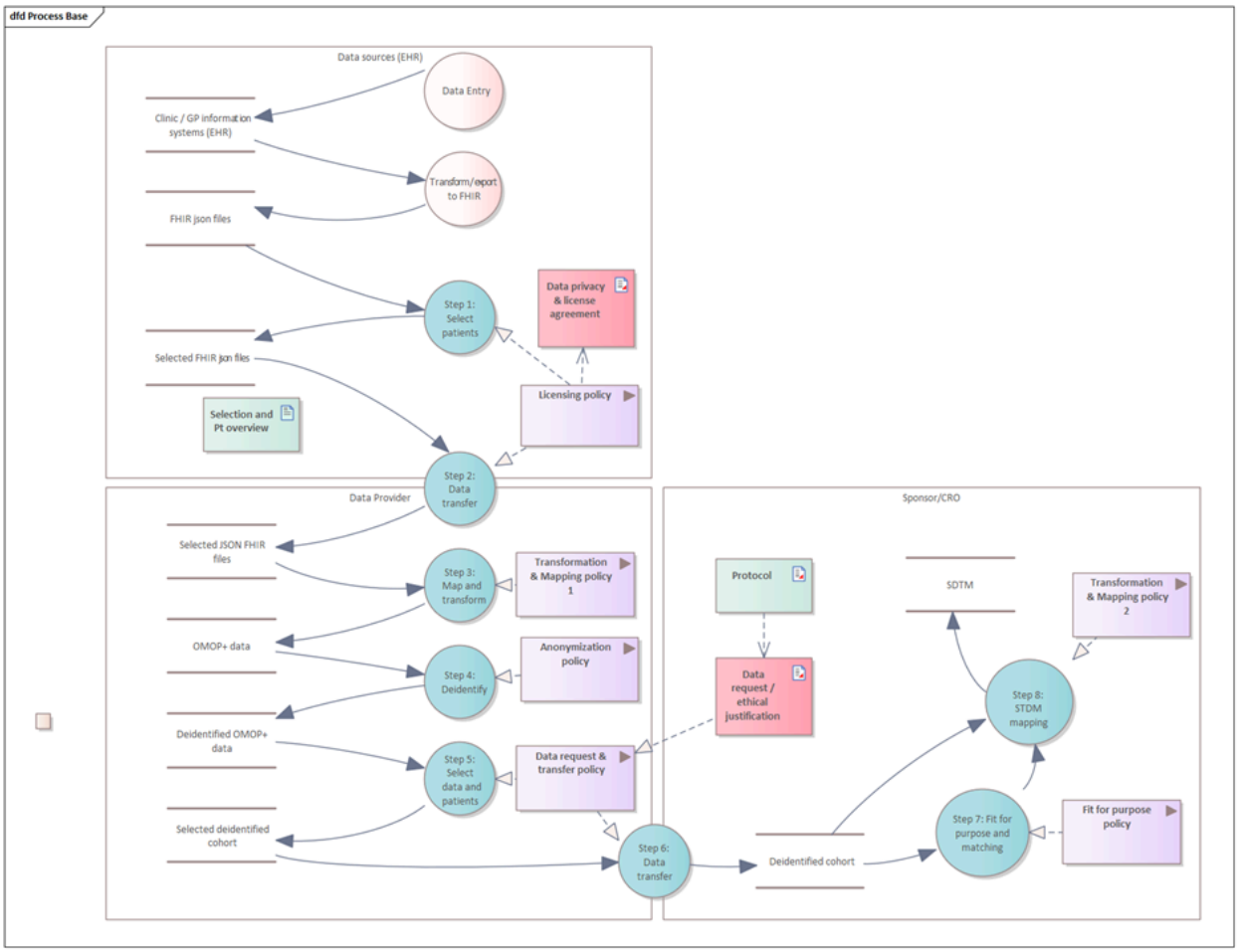


Figure 1: Data flow process from source to submission-ready datasets

SOURCE DATA SELECTION

The data from the Synthea source [1] is provided in FHIR format. The FHIR exchange format is in JSON and it includes 1 patient per JSON file. The set of available patient FHIR files at the source was automatically inspected using R code to select patients that matched the specified SNOMED indication codes. See code below:

```
# install package findR if it is not already installed

# read in library
library(findR)

# set working directory to folder containing all patients (both Non-Alz and Alz
patient files - saved as .txt files not as JSON files
setwd("C:/temp/FULLPOPTXT")

# copy files that match for snomed code 26929004 - Alzheimer
findtxt(pattern = "26929004", case.sensitive = TRUE, show.results = TRUE, copy =
FALSE, folder = "C:/temp/found_alzpop", overwrite = TRUE )

# copy files that match for snomed code 230265002 - Familial Alzheimer
findtxt(pattern = "230265002", case.sensitive = TRUE, show.results = TRUE, copy =
FALSE, folder = "C:/temp/found_alzpop", overwrite = TRUE )
```

The advantage of using R in for source patient file selection is that it can easily be run within foreign environments without licensing issues. This version used for the proof of concept is still fairly simple but can be optimized by using more specific finding patterns and outputting a list of selected patients for governance verification purposes.
Based on this code a total of 159 synthetic Alzheimer patients were selected from the EHR to represent the patient population dataset.

DATA FLOW-TRANSFORMATION FHIR TO OMOP

For the transformation of FHIR to the OMOP-like tabular structure, we tried a number of open-source and investigated proprietary AI based abstraction tools. However, either a lot of mapping information still had to be provided to those open source tools available, not all information was automatically mapped or the mapping tools themselves were a blackbox, causing issues with the backward compatibility. Therefore, we chose to use the SAS® JSON option in the LIBNAME statement [5]. This ensured that all the information from the source FHIR files was extracted and we could select what we needed.
In addition to the JSON files, a number of mapping files were used to allow for automated transformation from FHIR to OMOP and from source dictionaries to standardized dictionaries. For the dictionaries, the full path towards CDISC was directly provided to show the full trail from source to submission values and to avoid any re-mapping issue in that regard (See Table 1).

TABLE 1: DICTIONARY MAPPING EXAMPLE

	Synthea / FHIR		OMOP				CDISC		
Codelist	Value	Code	concept_id	Code	Name	Vocabulary	Codelist	Codelist code	CT
Employment	full-time	0	4053118	160903007	Full-time employment	SNOMED	C111108	C52658	FULL-TIME
Employment	part-time	1	4059634	160904001	Part-time employment	SNOMED	C111108	C75562	PART-TIME
Employment	unemployed	2	4251171	73438004	Unemployed	SNOMED	C111108	C75563	NOT EMPLOYED
Employment	retired	3	4022069	105493001	Retired	SNOMED			

FHIR Data mapped:
Not all data from the original FHIR files was mapped. Because of proportionality reasons, data that is not necessary for further processing or traceability should not be included. Therefore, before mapping, the data vendor needs to assess what information might be relevant for clinical research, representative of both negative and positive lineage. As a result, for this proof of concept, the following FHIR resource types were included in the mapping:

- Patient
- Observation
- Condition
- AllergyIntolerance
- MedicationRequest
- Immunization
- Procedure
- Encounter
- Location

**Note in actual practice a data vendor might want to address more resources to ensure consistency and drug accountability checks.*

OMOP like datasets (“OMOP+”)
The created OMOP like datasets including supplemental variables to hold the received FHIR content as is, then later retrieve them using either a JSONb or XML path for any GET or POST operations, were based on the FHIR information available and the potential needs for clinical research. In this proof of concept, the following OMOP like datasets were created:

- Person
- Death
- Visit_occurrence
- Condition_occurrence
- Procedure_occurrence
- Measurement
- Observation
- Fact_relationship

DATA ANONYMIZATION

To ensure adherence to patient privacy regulations, the data was anonymized with proof at the processor level of transformations and anonymization methods, which documented the R factor below .09 for legal standing. Before being then utilized in downstream clinical study purposes, the licensing agreement for each data set was verified.

For regulatory purposes, traceability back to the initial source record needs to be maintained. To address this lineage to provenance issue along with the complexity of regulators accessing third-party data, the following was accounted for in this proof of concept:

- Cryptographic certifications were used as deidentification measure for patient, location and provider IDs. This enabled tracing from source to end but not the other way around. Hence, one needs to know the patient IDs in the source to restore the connection to the deidentified data.
- Date shifting was applied by a maximum of 2 years. Shifts were applied consistently per patient to keep the consistency of the data within a patient.
- Sensitive deidentifying observations like questions on migration status, jail, address and income question were deleted.

Not conducted in the reduced scope, in practice it is recommend to review the full list of assessments included in a source, gauging sensitive and documenting its inclusion or exclusion for clinical study purposes, which then is traceable. Furthermore, per variable, the distribution of values within and between subjects should be assessed to evaluate whether this poses any deidentification risk and ensure data is not duplicated.

FEASIBILITY AND COHORT SELECTION

For this proof of concept, we attempted to identify the most common RWE workflow, mimicking a sponsor licensing a real-world data set from a data vendor to submit a safety control data set. Our dataset would have augmented this dataset as it followed these basic subject selection criteria:

- Patients with a diagnosis of Alzheimer's disease
- Males and Women of reproductive age of at least 50 years of age
- An MMSE score between 10 to 23
- Minimal 1 continuous observation period of 6 months after the selection criteria are met.

Based on these criteria out of the 159 patients with Alzheimer's disease selected from the EHR source, 138 met the MMSE score criteria and of these 138 patients, 129 had a continuous observation period of 6 months after the selection criteria were met.

In addition, we evaluated whether the relevant data elements were available in the source data sets. In non-synthetic RWD source data, multiple codes for the same assessment can be used. Therefore, it is important to look at the variety of codes that can apply to the target assessment. Having standardized all the data to OMOP, the standard OMOP concept_ancestor table aids this selection by linking the medical code associated with an assessment, to all related children codes that might be applicable and used in the source.

WINDOWING AND PATIENT SELECTION

Index date

A specific and difficult challenge when designing RWE external control arms for clinical trials is specifying the index date (also called *time zero* or *zero time*), which is the start of the observation period for assessing endpoints [6]. In this proof of concept, we defined the index data as the first visit date that all criteria were met. All calculated visit days and the corresponding windowing were defined based on this index date.

Windowing

To align with the interventional trial arm the following windowing was applied to the real-world source data (See Table 2).

Interventional trial visit day			Day calculated based on index date	
Visit	**Week**	**Planned visit Day**	**WindowLower Day**	**WindowUpper Day**
1	-2	-14	-180	-1
2	-0.3	-2	**DO NOT**	**INCLUDE**
3	0	0	**INDEX DATE**	7
4	2	14	7	20
5	4	28	21	34
7	6	42	35	48
8	8	56	49	69
9	12	84	70	97
10	16	112	98	125
11	20	140	126	153
12	24	168	154	174

13	26	182	175	188

Table 2: Visit day comparison between interventional and real-world data control arm

Gaps between the windows were avoided to make sure all data within 6 months after the index date was included. Since this is real-world data, a patient could have more EHR visits within a window. All data of the multiple EHR visits are included in the final datasets to enable the use of the correct value for a specific assessment. For each measurement, we used the non-missing observation closest to the planned visit date for analysis. The number of patients with data available per visit in the proof of concept study is presented in Figure 2.

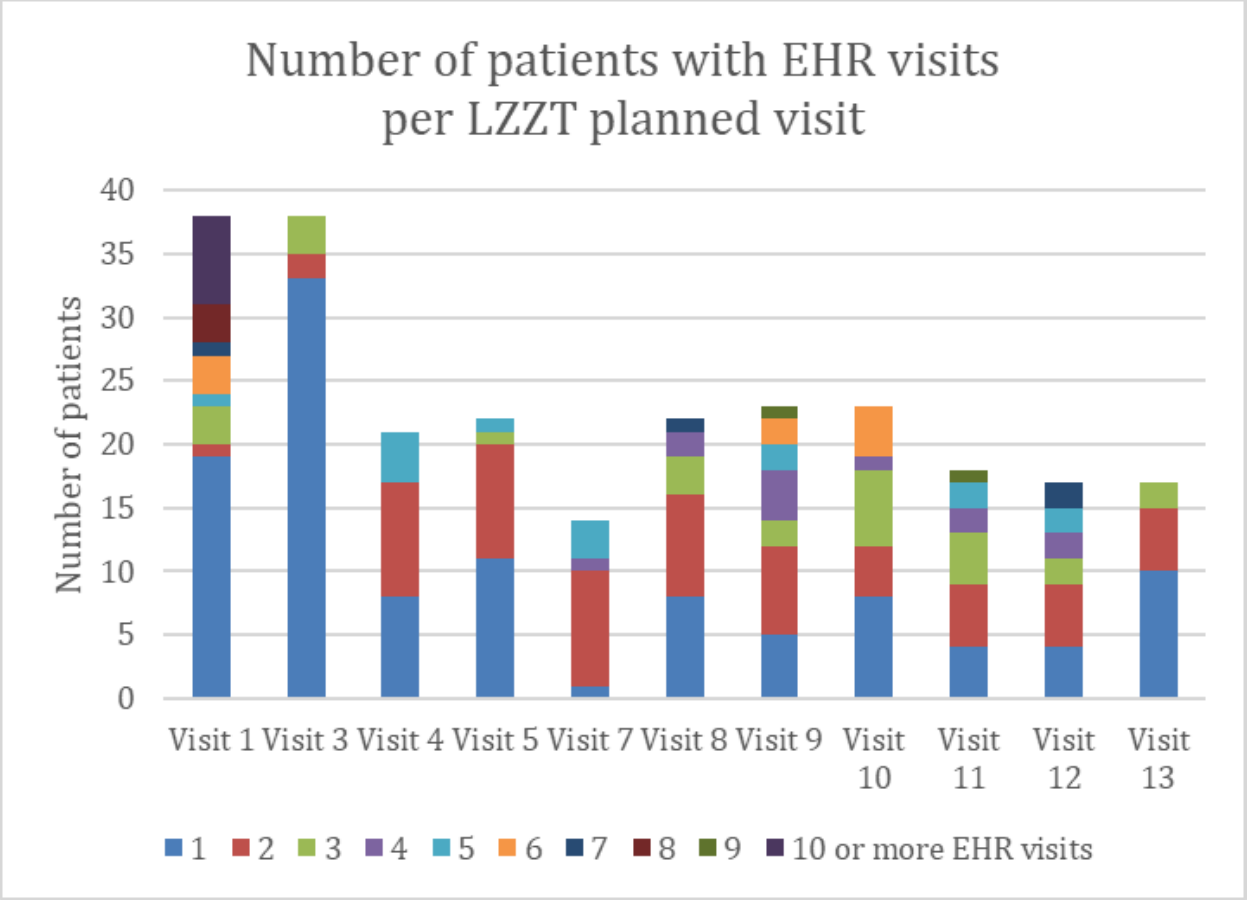


Figure 2: Number of Patients with EHR visits per LZZT planned visit

Fit-For-Purpose Assessments

The sponsor evaluation included a further check on the usability of the study and whether imputations were necessary. In this proof of concept, we simplified this step and defined the following two additional criteria for patients to be included in the study:

- Patients need to have data available for visit 8 or higher
- Data needs to include safety lab data to allow for comparison with the interventional study arm

Based on the visit 8 or higher criteria a total of 56 patients were selected. Of these patients, only 38 patients had safety lab data available during these visits and therefore could be included in the external control arm. The corresponding attrition diagram is shown in Figure 3.

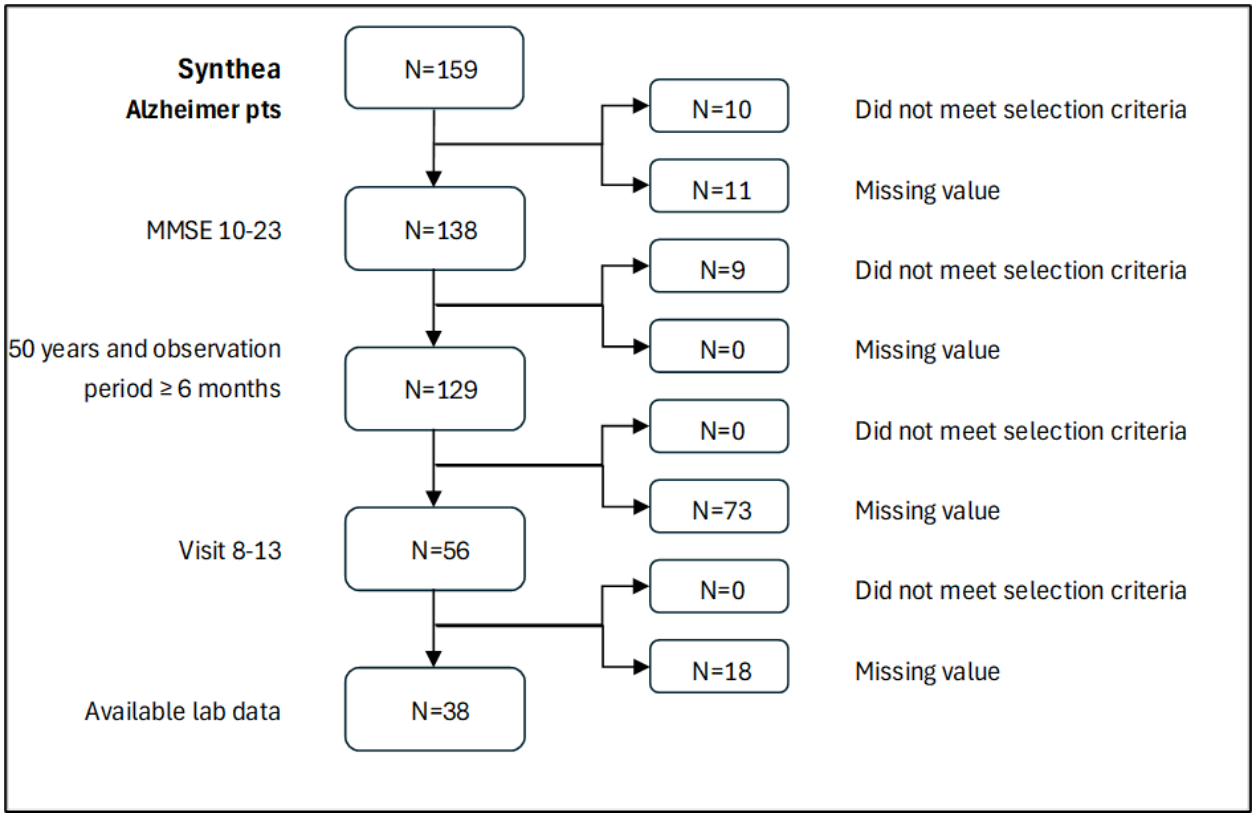


Figure 3: Proof of concept attrition diagram

Imputations and matching
In this proof of concept, imputation and matching were not applied. However, were this an actual real-world data study, it would be mandatory to obtain a substantiated well-balanced control group. A few examples that could be applied to this data are:

- Use matching algorithms to match the real-world patients to interventional patients based on baseline characteristics such as age, gender, ethnicity, and MMSE score.
- Apply LOCF for assessments that are not available at visit 1 and are not likely to be variable. An availability check per parameter needs to be done to see whether this is needed.
- Impute derived lab parameters used in the interventional trial like absolute counts to ratios.

TRANSFORMATIONS FROM OMOP TO SDTM

Like for the transformation from FHIR to OMOP like datasets, for each resulting SDTM dataset [7] a mapping file was created indicating the exact transformations needed to convert to SDTM data sets. These transformation files, along with the dictionary mapping file, were used to automate the mapping from OMOP to SDTM. In our proof of concept, we included the mapping to the following SDTM domains that serve as good representation of the full set of SDTM domains required for submission for a safety control arm:

- DM
- SV
- VS
- SC
- AE
- MH
- CM
- LB
- QS
- Multiple supplemental datasets

Important to note, there were two special cases where mapping of real-world data to SDTM submission datasets is generally more challenging and requires pre-configured governance. This was the case in determining whether conditions should be mapped to the Adverse event (AE) or Medical History (MH) domain. Our decision was based on

the index date. Hence, all conditions before the index date were mapped to MH, while all conditions after the index date were mapped to AE. In case relatedness information is available in source we could add that to the data. However, this is based on the data collection practices at the source. When a MedDra licence is available, OMOP includes a mapping dictionary from SNOMED to MedDra which allows for the mapping of most conditions directly to MedDra. For the Concomitant Medication (CM) mapping such a mapping is not available. However, this can be partly handled by directly matching substance and drug names to the corresponding WHO drug codes needed for submission. In addition, the OMOP concept_relationship and drug_strength databases can aid the mapping of other CM variables considerably.

GOVERNANCE AND DATA LINEAGE

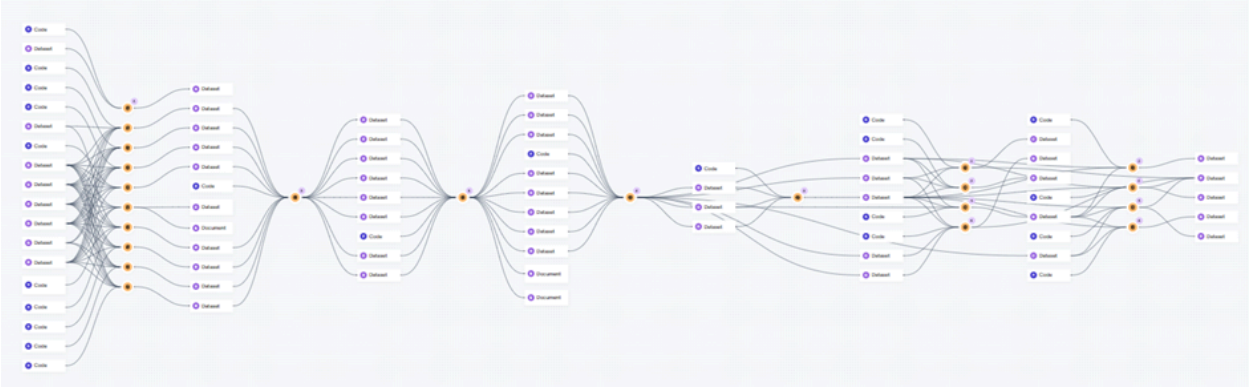
For each step in the process, the governance policies were defined to describe the requirements for provenance, traceability and quality control. Cryptographic integrity was applied to verify the whether processes were followed from data source to SDTM. This ensures authenticated proof of data and processes across organizations and systems, enabling complete lineage, unified governance, and granular traceability.
The following governance policies and computes were included in the lineage process:

Policy	Policy Rules	Policy Criterion
RWD licensing: Select data at source and transfer	(1) Verify transfer contract in place and signed (2) Verify correct run of code to select Alzheimer patients and approval by data owner (3) Verify and encrypted transfer via secured channels to data vendor (4) Verify data deletion at data vendor site within licensing period	(1) Contract includes definition of cohort including selection specifications (ie indication codes) (1) Legal review of contract (1) Signature by EHR data owner / Data vendor (2) R program to select patients based on batch of Json files in version controlled Github (2) QC of R program run by second programmer (2) Review and approval of output by EHR data owner (3) Apply encryption before sending (3) Verify secure channels/method used for sending data (acc to contract) (3) Verify data unchanged after sending to data vendor (4) Verify original (non-anonymized) data is deleted at data vendor site within 1 year of contract date
Transformation & mapping policy 1 (FHIR-OMOP)	(1) Mapping input created as input (2) Main programmer creates mapping programs from FHIR to OMOP+ (3) QC procedure	(1) Mapping files created directly linking from FHIR content to OMOP+ (1) Mapping files transferred to version controlled GitHub (2) Follow good programming guidelines (2) Input of latest version of mapping files and OMOP concept library (2) Validate against mapping specifications (2) Verify correct run of Fhir to OMOP+ programs (2) Notify when programs are ready (3) Verify alignment with OMOP concept library (3) Verify all patients from source are included (3) Verify correct run of FHIR to OMOP+ programs (3) Verify no data is changed by mapping backwards (3) Verify that programs are both signed off by programmer and QC
Anonymize Patient Data	(1) Define scope of anonymization (2) Perform anonymization according to scope (3) Verify anonymization according to scope (4) Verify secured storage of deidentification information	(1) Define shifting of dates and time variables (1) Define anoymization of location variables (1) Describe rationale for not anomyzing of certain variable for regulatory purposes (sex, age, race, country ethnic etc) (1) Define removal of potential sensitive information (pregnancy, mental health, family conditions etc) (2) Apply encryption of ID variables (2) Remove variables identified as sensitive (2) Apply shifting of date variables (3) Verify data unchanged after sending to data vendor (3) Prove Compliance with Privacy Regulations (SHA-256) (4) Compliance with Cryptographic Standards (4) Data Integrity and Consistency Checks (4) Audit and verification (SHA-256)

Data cohort selection and transfer	(1) Verify ethical approval for sponsor request is in place (2) Verify selection based on Sponsor requirements and approval (attrition diagram) (3) Verify encrypted / unchanged transfer of data to Sponsor	(1) Contract includes (ref to) data cohort requirements, ethical review requirements and proportionality requirements (1) Signatures of sponsor and data vendor on contract (1) Ethical approval in place (2) Selection specifications based on codes provided by sponsor and aligning with contract definitions (2) Program to select the patients based on criteria (2) QC of program to select patients based on criteria (3) Apply encryption before sending (3) Verify secure channels/method used for sending data (acc to contract) (3) Verify data unchanged after sending to data vendor
Fit for purpose	(1) Verify correct fit for purpose assessment based on eligibility criteria of study (2) Verify correct run of programs for fit for purpose (3) Verify selection of subset of matched patients	(1) Define selection / eligibility criteria (1) Selection / eligibility criteria reviewed and approved by content knowledge experts (2) Follow good programming guidelines (2) Validate against fit-for purpose specifications (2) Verify correct run of fit for purpose programs (2) Notify when validation is ready and programs are both signed off by programmer and QC (3) Align output with content knowledge experts
Transformation & mapping policy 2 (OMOP-SDTM)	(1) Mapping input created as input (2) Main programmer creates mapping programs from FHIR to OMOP+ (3) QC procedure	(1) Mapping files created directly linking from anonymized OMOP+ content to SDTM (1) Mapping files transferred to version controlled GitHub (2) Follow good programming guidelines (2) Input of latest version of mapping files and indicated SDTM CT version (2) Validate against mapping specifications (2) Verify correct run of OMOP+ to SDTM programs (2) Notify when programs are ready (3) Verify alignment with SDTM CT concept library (3) Verify all selected patients coming out of the fit for purpose assessment are included (3) Verify correct run of OMOP+ to SDTM programs (3) Verify no data is changed by mapping backwards (3) Verify that programs are both signed off by programmer and QC

LINEAGE

Based on these and the corresponding input, programs and output, the following lineage graph was created:
This graph shows the lineage between the different policy steps (yellow nodes), documents, mapping files, programs, and outputs. The graph is created by the governance tool from Eqty Life Sciences which links and controls the whole process enabling traceability and verifiability using modern but well-recognized techniques like hashing.



BACKWARDS MAPPING

The linkage from FHIR source to the final SDTM datasets and the corresponding mapping files ensure that the data can be mapped backward to the original FHIR datasets. Based on the mapping files and de-anonymization, most of the original FHIR message could be recreated. The FHIR JSON code snippet below shows what could be reconstructed in black.


```
 "resource": {
"resourceType": "Observation",
 "id": "b02036b7-943d-abea-16f3-ac146af2eddb",
 "meta": {
 "profile": [ "http://hl7.org/fhir/us/core/StructureDefinition/us-core-bmi" ]
 },
"status": "final",
 "category": [ {
  "coding": [ {
    "system": "http://terminology.hl7.org/CodeSystem/observation-category",
    "code": "vital-signs",
    "display": "Vital signs"
  } ]
 } ],
"code": {
  "coding": [ {
    "system": "http://loinc.org",
 "code": "39156-5",
    "display": "Body mass index (BMI) [Ratio]"
  } ],
  "text": "Body mass index (BMI) [Ratio]"
},
 "subject": {
 "reference": "urn:uuid:ad4c1e30-ddd7-5a4b-6af1-efcb19d8d96d"
 },
"encounter": {
  "reference": "urn:uuid:110a54bd-0ef2-1d33-9a4d-acf6cd109be1"
},
"effectiveDateTime": "2021-08-23T08:19:34+01:00",
"issued": "2021-08-23T08:19:34.512+01:00",
   "valueQuantity": {
  "value": 29.36,
  "unit": "kg/m2",
  "system": "http://unitsofmeasure.org",
```

```
        "code": "kg/m2"
      }
    },
    "request": {
      "method": "POST",
      "url": "Observation"
    }
}
```

Information that was not reconstructed (in red) was not mapped in the first place because of proportionality or confidentiality reasons or was deemed superfluous.

CONCLUSION

Cryptography serves as the foundation of modern audit tools by providing regulators with the highest level of confidence that real-world evidence has been responsibly captured, standardized, anonymized, and analyzed without bias. When data providers, vendors, and sponsors adopt open-source verification methods, they demonstrate control over their data and processes, offering regulatory reviewers verifiable proof of data quality and integrity.
As these stakeholders begin creating fit-for-use datasets, cryptographic certificates ensure the reliability of real-world data, enabling auditors to confidently accept sponsor submissions.

REFERENCES

[1] "Synthea TM," [Online]. Available: https://syntheticheath.github.io/synthea/.

[2] "OMOP Common Data Model," [Online]. Available: https://ohdsi.github.io/CommonDataModel/cdm54.html.

[3] C. O. U.S. Department of Health and Human Services FDA CDER, "Real-World Data: Assessing Electronic Health Records and Medical Claims to Support Regulatory Decision-Making for Drug and Biological Products," July 2024. [Online]. Available: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/real-world-data-assessing-electronic-health-records-and-medical-claims-data-support-regulatory.

[4] F. C. a. C. U.S. Department of Health and Human Services, "Data Standards for Drug and Biological Product Submissions Containing Real-World Data," December 2023. [Online]. Available: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/data-standards-drug-and-biological-product-submissions-containing-real-world-data.

[5] S. Institute, "LIBNAME Statement: JSON Engine," SAS Institute, [Online]. Available: https://documentation.sas.com/doc/en/pgmsascdc/9.4_3.5/lestmtsglobal/n1jfdetszx99ban1rl4zll6tej7j.htm. [Accessed June 2024].

[6] F. C. C. a. O. U.S. Department of Health and Human Services, "Considerations for the Design and Conduct of Externally Controlled Trials for Drug and Biological Products (Draft Guidance)," February 2023. [Online]. Available: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/considerations-design-and-conduct-externally-controlled-trials-drug-and-biological-products.

[7] CDISC, "CDISC SDTM," [Online]. Available: https://www.cdisc.org/standards/foundational/sdtm. [Accessed June 2024].

CONTACT INFORMATION (HEADER 1)

Your comments and questions are valued and encouraged. Contact the author at:

Author Name: Michael Kolzet
Company: EQTY Life Sciences
Address: Innovate Carolina Junction- 136 E Rosemary St, Chapel Hill, NC 27514:
Email Mike@eqtylab.io:
Website:www.eqtylab.io

Author Name: Berber Snoeijer
Company: ClinLine
Address: Van der Valk Boumanweg 15
Work Phone: +31 6 21197621
Email: b.snoeijer@clinline.eu
Website: www.clinline.org