



Traceability and Verification System

# DATA ACCESS RULES

---

**Version: 02.00** (16 January 2026)

## Document control

Version	Date	Author	Changes
00.01	20 Oct 2021		Working Version v1.0.0: Data Sharing Task Team
00.02	11 Oct 2022		Working Version v2.0.0 PMU
00.03	May 2023	Alexander Blecken	Working draft under new main editor
00.05	June 2023	Alexander Blecken	Draft version circulated to core team
00.06	July 2023	Alexander Blecken	Update after review by Pierre Dane, inter alia removed non-system roles from this document
00.10	27 July 2023	Alexander Blecken	Document shared with Data Sharing Task Team, VTI Steering Committee and other stakeholders
00.19	18 October 2023	Alexander Blecken	Updated version including all comments and feedback received from Data Sharing Task Team, VTI Steering Committee and other stakeholders
00.20	22 November 2023	Alexander Blecken	Revised version shared with Data Sharing Task Team, VTI Steering Committee and other stakeholders
01.00	13 March 2024	Alexander Blecken	Final version
02.00	16 January 2026	Richard Wilder	Revision including comments from current EA signatories

# Table of Contents

<b>Document control .....</b>	<b>2</b>
<b>Table of Contents .....</b>	<b>3</b>
<b>1 Introduction .....</b>	<b>4</b>
<b>2 Data Types .....</b>	<b>5</b>
2.1 Product Master Data .....	5
2.2 Location Master Data .....	6
2.3 Market Authorization Data .....	6
2.4 Product Pack Data (PPD) .....	7
2.5 Serial Number .....	7
2.6 Verification Request .....	7
2.7 Verification Response .....	8
2.8 Aggregate Trend Data .....	8
2.9 Traceability Event Data .....	8
2.10 Dashboard and System Data .....	9
2.11 Metrics and Audit Logs .....	9
<b>3 User Roles .....</b>	<b>9</b>
3.1 Users with global access .....	10
3.1.1 System Admin .....	10
3.1.2 TRVST System Provider / Service Desk .....	10
3.1.3 Program Management Unit .....	11
3.2 Users with selected access .....	12
3.2.1 Country Authority .....	12
3.2.2 Onboarding Partner .....	12
3.2.3 Stakeholder .....	13
3.2.4 Verification Application User .....	13
<b>4 Data Access Matrix .....</b>	<b>13</b>

# 1 Introduction

The Traceability and Verification System (TRVST) is a digital platform developed through collaboration by a multi-stakeholder group called the Verification and Traceability Initiative (VTI). This platform enables countries to verify the authenticity of health products and improve end-to-end traceability across supply chains. TRVST is a powerful tool that significantly reduces the risks of falsified and diverted health products and supports the move toward national traceability of vaccines, medicines, and other health items.

TRVST is not intended to replace national traceability systems; instead, it functions as a global interoperability hub, connecting manufacturers, regulatory agencies, and national systems. The platform allows product verification where national systems are not yet established and supports traceability throughout the upstream supply chain before reaching the country level.

By design, TRVST facilitates compliance with regulations of National Drug Regulatory Authorities (NDRAs) pertaining to product verification and by providing transparency into product logistics. Additionally, it grants access to patient information leaflets (PILs) via barcode scanning. This feature supplies healthcare providers with accurate, up-to-date product information, facilitating informed decisions regarding patient care. Patients can also use this feature to authenticate their medications and access essential information about the proper administration of their health products.

Manufacturers upload product master data, batch and lot numbers, expiry dates, and serial information into TRVST. These data are used to authenticate products when authorized users scan barcodes. Verification can be done directly through mobile or web interfaces or via data exchange between national systems and the TRVST Repository. The TRVST Repository acts as a central database that stores all product information and enables verification. This data exchange is managed through the TRVST Application Programming Interface (API), which facilitates secure communication and data sharing among systems. Data sharing and security are core to TRVST's design. The platform complies with strict data governance and information security standards to protect the confidentiality, integrity, and availability of all exchanged data. These measures promote trusted collaboration among stakeholders while ensuring adherence to relevant data protection and privacy laws.

TRVST plays a crucial role in safeguarding the integrity of health supply chains, strengthening regulatory oversight, and enhancing patient safety.

The TRVST System Provider is responsible for the system's technical development and maintenance.

UNICEF functions as the TRVST Organization and legal entity overseeing the management, governance, and stewardship of the data. This includes supervising system use, ensuring compliance with regulations, and managing the data shared on the platform.

More general information on TRVST is available in the [TRVST document repository](#).

This document defines:

- the different types of data held and generated by TRVST and the individual data elements that make up each type of data,
- the various user roles that interact with TRVST, and
- which data each role has access to.

Many of the data are high-risk and could be used by criminals to create falsified barcodes, and thus access to these and other data are strictly controlled.

TRVST does not store any patient data.

Terms and abbreviations used in this document are defined in the Enterprise Agreement.

## 2 Data Types

“Data” or “data” has the meaning given to it in the Enterprise Agreement and, in the context of this document, encompasses any data, in whatever form entered into the TRVST System by a TRVST User Organization, its Authorized Representative or by any other party with access to the TRVST System, and communications made within the TRVST System (including but not limited to notifications and alerts).

Data can be distinguished by data types and associated data elements. The data types and elements stored and processed in TRVST are described in this section. A more detailed definition of all data elements is available in the TRVST Master Data Guide, which is accessible through the [OBP-E API Interface documentation](#).

### 2.1 Product Master Data

Data element	Description
<b>GTIN</b>	Standard GS1 14-digit Global Trade Item Number
<b>Name</b>	Concatenated name: name + strength + pharmaceutical form
<b>Common Name</b>	International Non-proprietary name (INN) or the usual common name of the active substance(s), if part of the full name of the health product.
<b>Form</b>	The physical form of the pharmaceutical item using ISO 11239 or the US FDA Structured Product Labelling, using the plural form if appropriate ( <a href="https://standardterms.edqm.eu/">https://standardterms.edqm.eu/</a> ) – currently only the English terms are supported. For multi-component medicinal product use the Combined Pharmaceutical Dose Form CV published by the European Directorate for the Quality of Medicines & HealthCare (EDQM), a Directorate of the Council of Europe.
<b>Strength</b>	The pharmaceutical strength of the product. This should be consistent with the quantity stated in the quantitative composition and the posology. (Will be a repetition of what is entered as part of the full name)
<b>SeparableDoseUnits</b>	The number of re-packable dosage units in the pack. Where the pack is not readily re-packable, the value should be set as ‘1’. e.g. a pack of tablets that can be readily re-packed and therefore this value will represent the number of tablets in the pack. A powder or syrup cannot be readily re-packed and therefore, regardless of volume, the pack size will be set as ‘1’. If the pack could not be split, e.g. a 28 day supply of contraceptive, the value is 1.
<b>Pack Size (Net Content)</b>	The quantity (or quantities) of the product contained in the package along with its unit of measure typically printed on the label for the country or market where the product is sold
<b>Classification (ATC)</b>	<b>The code and schema for classification of the product as per</b> Anatomical Therapeutic Chemical Classification System ( <b>ATC</b> )

<b>Classification (UNSPSC)</b>	The code and schema for classification of the product as per United Nations Standard Products and Services Code® (UNSPSC)
<b>Classification (GPC)</b>	The code and schema for classification of the product as per the Global Product Classification system (GPC) created by GS1.
<b>Pack Level</b>	The type of packaging that carries the pack-level (serial number) or batch-level identifier in a barcode, and also, in most cases, in human-readable format.
<b>Brand Owner</b>	The Brand Owner is the entity registering the GTIN. They are represented in our system by the Onboarding Partner.
<b>Target Market</b>	The code that identifies the target market. The target market is at country level or higher geographical definition and is where a trade item is intended to be sold. Target Market Information can be supplied to provide additional market-level master data that may be of use for reporting and analysis purposes.

## 2.2 Location Master Data

Data element	Description
<b>GLN</b>	Global Location Number as established by the GS1 GLN Allocation Rules Standard and contained GLN Management Rules
<b>Name</b>	Description of the party location, business entity or function
<b>Location Data</b>	Physical address and geocoordinates. Location Master Data can be added for a site contained within a site or Sub-site detailing the Primary function and business function of the sub-site.

## 2.3 Market Authorization Data

Data element	Description
<b>Market</b>	Two-letter country code from ISO 3166-1 alpha-2 defining the local market for the product. One ISO code per market.
<b>Market Authorization Holder</b>	Name of market authorization holder authorized to import into recipient market
<b>National Code</b>	Optional national code. Could be NHRN or any other code required.
<b>Pharmacovigilance Code</b>	Pharmacovigilance code, e.g. market authorization number.

## 2.4 Product Pack Data (PPD)

Data element	Description
<b>Batch Id/ Lot Id</b>	Batch or Lot number as printed on the pack
<b>Batch Expiration Date</b>	Expiry date of the serialized batch represented by six (6) numeric digits in the form YYMMDD. For backward compatibility of existing products, where the day element is not provided in the human-readable format, the value of DD can be set to 00 (e.g. 190200 is February 2019). Market/Company rules apply.
<b>Batch Production Date</b>	Production date of the serialized batch represented by six (6) numeric digits in the form YYMMDD. For backward compatibility of existing products, where the day element is not provided in the human-readable format, the value of DD can be set to 00 (e.g. 190200 is February 2019). Market/Company rules apply.
<b>Batch Manufacturer Details</b>	Details of the physical manufacturer of the batch. Registered Manufacturer ID, if available, or a GLN, with physical address

## 2.5 Serial Number

Data element	Description
<b>Serial Number</b>	Up to twenty (20) alpha-numeric characters or single case (i.e. upper or lower case not both) according to the GS1 Specifications. The combination of the GTIN and Serial Number makes an item globally unique.

## 2.6 Verification Request

Data element	Description
<b>Transaction Id</b>	Unique identifier of the verification request
<b>Date/Time</b>	Date and time that the product was scanned
<b>Coordinates</b>	Latitude and Longitude of the scan as per device GPS
<b>Geolocation Country</b>	Country where the scan occurred, calculated using geocoordinates
<b>Persona Role [O]</b>	User entered role selected from list e.g., Healthcare Professional, Regulatory Authority Official
<b>Persona Location [O]</b>	User entered location in free text, GLN or name
<b>Device ID</b>	Hashed identifier of the scanner device
<b>Source Application</b>	Identifier of the source system, according to the API credentials issued to the system by TRVST

## 2.7 Verification Response

Data element	Description
Alert Id	The unique identifier of the generated alert
Response Code	The response code generated by the system (see Response Codes)

## 2.8 Aggregate Trend Data

Data element	Description
Verification Event Count	The count of events by the selected dimension
Date/Time Dimension	Date range for the aggregate report
Country Dimension [I]	Country Name
Product Dimension	GTIN
Response Code Dimension	Response code
Manufacturer Dimension	OBP or Manufacturer Name
Batch Dimension	Batch ID

## 2.9 Traceability Event Data

Data element	Description
SSCC	Serial Shipping Container Code - contained in aggregation event of the EPCIS bundle
PPD (with serial)	Product Pack Data comprising a list of serial numbers to be provided to country systems for products received at port of entry
EPCIS Event (no serial)	EPCIS event information at the batch level, e.g. a shipment
EPCIS Event (Pack level - with serial)	EPCIS event information at the pack level including serial numbers, e.g. commissioning, aggregation, and shipping



## 2.10 Dashboard and System Data

Data element	Description
<b>Organization Details</b>	Identifying details of the participating organization
<b>Dashboard User Details</b>	Login credentials of the dashboard user (name, email address, title etc.)
<b>Dashboard User Activity Audit Log</b>	Dashboard interaction log per user e.g., pages visited, reports run

## 2.11 Metrics and Audit Logs

Data element	Description
<b>Performance Metrics</b>	System performance metrics e.g., average response time and percentiles, number of requests per second
<b>Upload Metrics</b>	Summary of data uploaded to the system, e.g., number of GTINs, Batches and serial numbers, number o uploads per OBP
<b>System Audit Logs</b>	Detailed system logs

## 3 User Roles

Data access is detailed in this document which specify that user data must be kept confidential and stored securely, and that participants who create data own that data. Access to data held by TRVST is distinguished by user roles and data access is allowed for each role only where there is sufficient rationale. Unless a user is assigned one of the user roles described in this chapter, they do not have access to any TRVST data.

User roles can be distinguished in two broad categories:

1. **Users with global access:** These include System Administrator, Program Management Unit, and TRVST System Provider / Service Desk user roles
2. **Users with selected access:** These include Country Authorities<sup>1</sup>, Onboarding Partners, Stakeholders (e.g. funders/donors, procurement agents and others), Verification App Users

As a general principle, users have access to the data they provided to the TRVST system or which they have generated. Additionally, certain roles will have access if that access is necessary, for instance to identify and investigate falsified vaccines or other health products or for system maintenance and

---

<sup>1</sup> The terms "National Competent Authority" and "Country Authority" are used interchangeably in the context of the TRVST governance documents

development as described in this Chapter. Figure 1 shows at a high level and in a simplified version the access of different user roles to certain data.

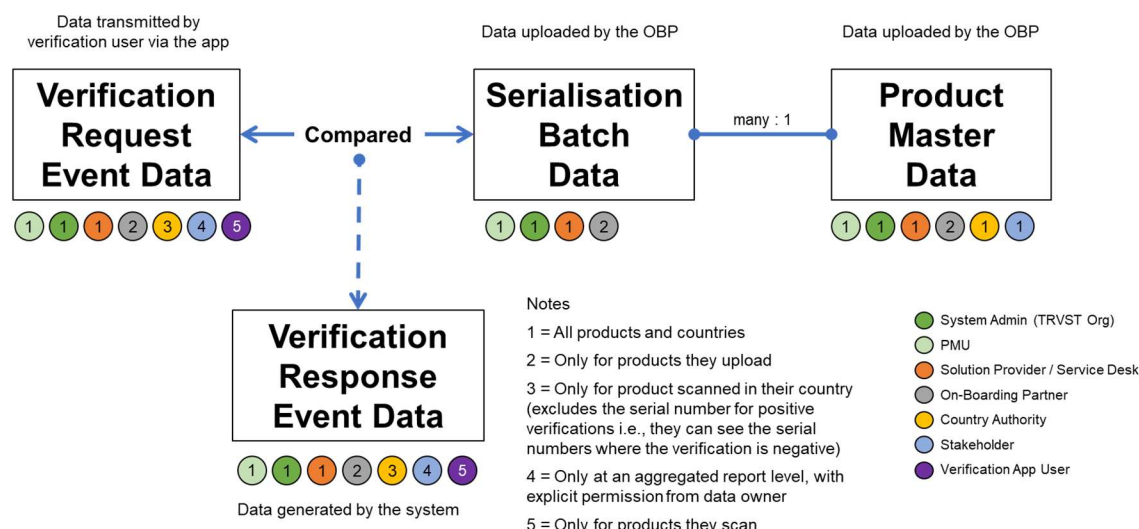


Figure 1: High-level overview over data access by user role (simplified)

In the following sections, each user role type is described, their access to data outlined and a rationale for the data access given. A detailed overview over data access by user role is provided in Section 4.

## 3.1 Users with global access

### 3.1.1 System Administrator

<b>Description</b>	The system administrator is the overall manager of TRVST operations. They are the primary interface with the TRVST System Provider and are responsible for ensuring that system Service-Level Agreements are adhered to, and that technical, operational and business issues are identified and resolved.
<b>Data Access</b>	All data
<b>Rationale</b>	System administrators are responsible for proactively monitoring and identification of system, operational and business issues. They need to be able to respond to 'red flag' events and ensure user compliance.

### 3.1.2 TRVST System Provider / Service Desk

<b>Description</b>	The TRVST System Provider has system administrator access. The TRVST System Provider is responsible for day-to-day management of all operations of the platform on behalf of the TRVST participants. This role is technical in nature, and members will be part of the technology solution vendor technical team.
--------------------	---

	<p>The TRVST System Provider needs access to all data stored and generated by the TRVST. This data should be used for monitoring of system performance and follow up of performance issues or data issues reported by users.</p> <p>Data must not be accessed outside of a formal monitoring/audit process or instruction from the System Administrator and should only be accessed where necessary to respond to queries or follow-ups.</p> <p>The TRVST System Provider also operates a Service Desk. The Service Desk Operator is responsible for onboarding users and integration of external systems (such as manufacturer data feeds), as well as responding to user queries, password reset requests and any other first line support. In addition, the operator will be responsible for monitoring the resolution of suspect activity which have been alerted to the Service Desk.</p>
<b>Data Access</b>	All data
<b>Rationale</b>	<p>The TRVST System Provider requires access to all data to facilitate the daily operations of the TRVST, and to respond to System Administrator support requests.</p> <p>The Service Desk Operator performs a range of functions for which full data access is required. This includes user onboarding and maintenance, first line support, response to use support requests. The Service Desk Operation will also notify users regarding downtime, <del>suspicious user activity</del>, changes to the Terms of Use, etc.</p>

### 3.1.3 Program Management Unit

<b>Description</b>	<p>The Program Management Unit is the team which defines and implements day-to-day tasks, coordinates with the Steering Committee and Technical Task Teams, and reports on progress and challenges. The PMU provides necessary structure and facilitation for handling the execution of the complex, multi-organization, multi-stakeholder program. The PMU works with the three (3) Technical Task Teams as well as the membership of the VTI SteerCo to manage and align workplans and deliverables across the whole governance structure.</p>
<b>Data Access</b>	All data with the exception of Audit Logs
<b>Rationale</b>	<p>The PMU acts at the direction of the VTI SteerCo, escalating and forecasting issues, supporting consensus building, and facilitating decision making across the initiative's multi-stakeholder governance structure. The PMU develops and manages workplans, including for the three Technical Task Teams; provides day-to-day management for the overall project and Task Teams; facilitates VTI SteerCo calls; brings on SME participation, as needed or requested by VTI SteerCo.</p>

## 3.2 Users with selected access

### 3.2.1 Country Authority

<b>Description</b>	A Country Authority is the National Regulatory Authority or Ministry of Health participating in TRVST. A Country Authority user will access the dashboard to track, monitor and respond to verification events and the corresponding suspect activities.
<b>Data Access</b>	Country Authorities have access to the data they own or to which access is granted from another owner. Additionally, they are referenced in the EPCIS message for Batch & Serial and some Traceability Event Data. They do not have access to Metrics and Audit Logs, and EPCIS Events.
<b>Rationale</b>	Country authorities can be involved in the investigation of suspect activity and failed verification events. The identification of sites in their country where verifications are failing is important to inform them about possible training issues, hardware configuration failures or to investigate suspect fraudulent activities.

### 3.2.2 Onboarding Partner

<b>Description</b>	The Onboarding Partner Role Type is assigned to Onboarding Partner Organizations (OBPs). OBPs are organizations that are represented as the brand owner of the product and are expected to be the organization that will supply Barcode Batch and Serial Identification Data to the TRVST. Non-manufacturers which carry out the serialization for the OBP, such as packers, will submit these data to the TRVST via the OBP.
<b>Data Access</b>	The Onboarding Partner has access to the data owned or granted to them, e.g. Product Master Data, Barcode Batch and Serial Identification Data for the organization's products. They also have access to most data associated with Verification Event Requests. For the avoidance of any doubt: An OBP does not have access to the data of other OBPs.
<b>Rationale</b>	The OBP owns and needs to supply Master Data, Barcode Batch and Serial Identification Data for the OBP's products to TRVST. Data associated with Verification Event Requests enables OBP's to monitor the integrity of their supply chains.

### 3.2.3 Stakeholder

<b>Description</b>	A Stakeholder is any other participating member of TRVST which is not an OBP, Country Authority or one of the user roles with global access. These could include funders/donors, procurement agents, VTI Steering Committee members, or others.
<b>Data Access</b>	<p>Access to stakeholders is limited. These can mostly access specified data (e.g. active in region for specified GTINs). Data granularity is limited to the Aggregate Data and Product Catalogue Report.</p> <p>For a stakeholder to be granted access to certain data, the owner of the data needs to agree in writing. This agreement can be obtained informally, e.g. i.e. via email from the representative of the TRVST User organization which owns the data.</p>
<b>Rationale</b>	Stakeholders may require access to aggregate data specific to the GTINs and Countries that they have been granted access to see.

### 3.2.4 Verification Application User

<b>Description</b>	Mobile Verification Application Users scan product barcodes using the TRVST mobile application. These verification events are submitted to the TRVST and a response indicating verification success or failure is returned by the TRVST. The users will use the TRVST mobile verification application.
<b>Data Access</b>	<p>Access to all data which they submitted to the TRVST, as well as the response codes of their requests.</p> <p>No access to Traceability Event Data, Dashboard &amp; System Data or Metrics &amp; Audit Logs.</p>
<b>Rationale</b>	Mobile Verification Application Users need access to the history of their event submissions, and access to the response code to identify whether the verification was successful, or in the event of a failed verification or suspect activity alert, the reason for the alert or failure.

## 4 Data Access Matrix

The following chart details data access rights for each data element per role. Data elements are marked as optional or inferred where appropriate and color-coded to indicate whether a role has access to all data of that type, just the data that is owned by the role, or data from the countries where they are active and have the relevant permission.

For example, OBPs have access to all information on their own products (blue), but not for products from other OBPs. Country Authorities may see data generated by users in their verification sites (purple), but not information from other countries. System administrators have access to all data, regardless of who generated them (green). Stakeholders may see data from the countries they are active in (orange).

R2.1 - TRVST Data Access & System Permissions			System Role / Organisation Type						
			Global access			Selected access			
			System Admin (TRVST.org)	PMU	Solution Provider / Service Desk	Country Authority	Onboarding Partner	Stakeholder	Verification App User
Verification Use Case	Master Data	Product Master Data [PMD]	✓	✓	✓	✓	✓	✓	✓
		Location Master Data [LMD]	✓	✓	✓	✓	✓	✓	
		Market Authorization Data	✗	✗	✗	✗	✓	✗	✗
	Batch & Serial #	Batch Data	✓	✓	✓	✓	✓	✓	✓
		Serial Number	✓	✓	✓	✓	✓	✗	✓
	Verification Event Request	Transaction Id	✓	✓	✓	✓	✗	✗	✓
		Date/Time	✓	✓	✓	✓	✓	✓	✓
		Coordinates	✓	✓	✓	✓	✓	✗	✓
		GeoLocation Country [I]	✓	✓	✓	✓	✓	✓	✓
		Source Application	✓	✓	✓	✓	✓	✗	✓
		Persona/Device Info [PDD]	✓	✓	✓	✗	✗	✗	✓
	Verification Event Response	Alert Id	✓	✓	✓	✓	✓	✗	✓
		Response Code	✓	✓	✓	✓	✓	✓	✓
		Aggregate Trend Data	✓	✓	✓	✓	✓	✓	✗
Visibility/Traceability Use Case	Master Data	Product Master Data (PMD)	✓	✓	✓	✓	✓	✓	✗
		Location Master Data	✓	✓	✓	✓	✓	✗	✗
	Batch & Serial #	BatchId/Lot Id	✓	✓	✓	↔	✓	✓	✗
		Serial Number	✓	✓	✓	↔	✓	✗	✗
	Traceability Event Data	SSCC	✓	✓	✓	↔	✓	✓	✗
		Modality E PPD (with serial)	✓	✓	✓	✓	✓	✗	✗
		EPCIS Event (Logistics - no serial)	✓	✓	✓	↔	✓	✓	✗
		EPCIS Event (T&T - with serial)	✓	✓	✓	✗	✓	✗	✗
Administrative Data	Dashboard & System Data	Organisation Details	✓	✓	✓	✓	✓	✓	✗
		Dashboard User Details	✓	✓	✓	✓	✓	✓	✗
		Dashboard User Activity Log	✓	✓	✓	✓	✓	✓	✗
	Metrics & Audit Logs	Performance Metrics	✓	✓	✓	✗	✗	✗	✗
		Upload Metrics	✓	✓	✓	✗	✓	✓	✗
		System Audit Logs	✓	✗	✓	✗	✗	✗	✗

Permission Legend:

- ✓ Access allowed to all data or full functionality
- ✓ Access allowed to data owned by or granted to participant
- ✓ Access allowed to specified data (e.g. Active in region for specified GTINS)
- ✓ Access allowed on an alert basis (for owned data, or data granted access to)
- ✓ Access allowed against purchase orders raised or funded

[O] - Optional Field

[I] - Inferred Field

- ↔ Organization is referenced in the EPCIS message (One-up, One-down)
- ✗ Access by explicit permissions from the data owner
- ✗ No Access/Not Applicable

Figure 2: Data Access Matrix (R2.1)