GTR Data Sharing Protocol

2021-10-20 - Working Version v1.0.0: Data Sharing Task Team

Introduction

The Global Trust Repository (GTR) is a software platform set up to detect falsified COVID-19 vaccines and protect the safety of supply chains. To do this, vaccine manufacturers submit product pack batch ids and serial numbers to the GTR, and barcode scans by users of the vaccines are validated against these data. Verification is carried out either on mobile devices interacting directly with the GTR, or through data exchange between existing country verification and traceability information systems and the GTR Application Programming Interface (API).

This document defines the different types of data held and generated by the GTR, the individual data elements that make up each type of data, the various user roles that interact with the GTR, and which data each role has access to. Many of the data are sensitive and could be used by criminals to create falsified barcodes, and thus access to these and other data are strictly controlled when necessary. The document is based on the 9 core principles of the GTR.[1]

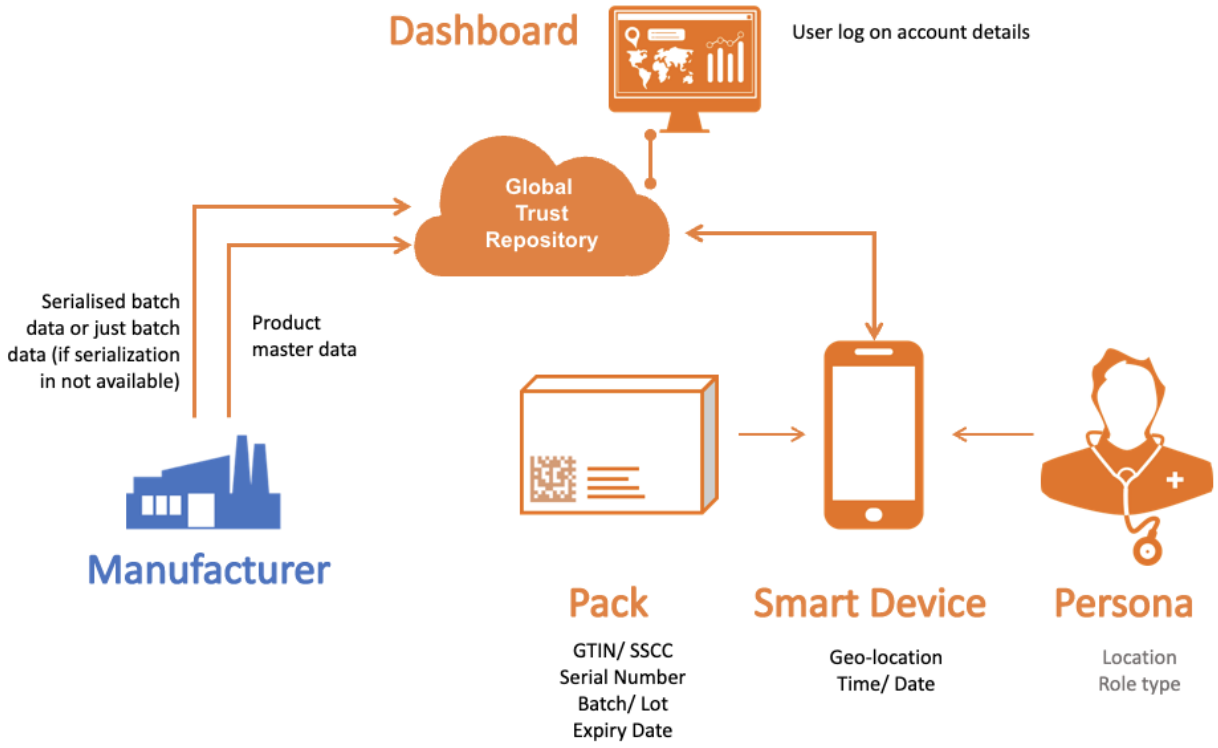

Figure 1: GTR Data Flow

[1] 9 Core Principles of the GTR

Data Definitions

Administrative Data

Administrative data consist of information that is used and generated by the software platform as part of normal operations and is not related to the verification of products. Data include monitoring, performance and audit information, and information used to enable users to login to the system and to determine which data each user should have access to.

Illustrative Data Elements: Username, Password (encrypted), User Role, User Contact Details, Activity History

Aggregate Trend Data

Aggregate Trend Data are data generated from counts and sums of the number of verification events sliced by one or more facets. These data can be used to identify trends and provide participants with data to monitor the performance of the GTR while not exposing sensitive event level data such as serial numbers

Illustrative Data Points: Number of events by day or by country. Data will be disaggregated by facets – Date/Time, Country, Location, Product, Response Code, Manufacturer and Batch

Barcode Batch and Serial Identification Data

Batch and Serial Identification Data are encoded into the barcode by the packer or manufacturer, or during national serialization. These data are submitted to the GTR by the Onboarding Partner (OBP).

Illustrative Data Points: GTIN, Batch Identifier, Serial Number, SSCC, Expiry Date

Configuration Data

Configuration data contains thresholds for alerts and notifications, and validation rules.

Illustrative Data Points: Number of verification error responses triggering an alert

Manufacturer Master Data

Master manufacturer data include business details about the onboarding partner.

Illustrative Data Points: Business Address, Organization Name, Contact Email Addresses, Contact Telephone Number

Product Master Data

Product Master Data are generally available and describe a products identification and attributes, based on GS1 standards.

Illustrative Data Points: Global Trade Item Number (GTIN), Product Description, Brand Owner, Information Provider Global Location Number (GLN).

Suspect Activity Data

Suspect activity data is generated as verification events are submitted to the GTR and these events trigger configured alert rules, for example multiple verification events for the same serial number in different geographies, or verification events where the product expiry data is different to the expiry date supplied by the OBP. Investigation workflows will be triggered for authorized parties who subscribe to these alerts.

Illustrative Data Points: Linked list of unique event ids, Alert Code

Verification Event Request Data

Verification Event Request Data are transactional data generated by verification users either using a mobile application or a 3rd party system to scan a product barcode. These data are submitted and stored by the GTR and are the core records used to determine if products are suspected to be falsified. Geo-coordinates are sensitive and sharing will need to be discussed with country authorities, and lack of these data will mean geographic checks may not be possible.

Illustrative Data Points: Barcode Batch and Serial Identification Data, Event Identifier, Datetime, Coordinates, User Role Type [Optional], Location [Optional], Request Source

Verification Event Response Data

Verification Event Response Data are transactional data that consist of the identifier of the submitted event, and the response code detailing the success of the verification, or the reason for failure.

Illustrative Data Points: Event Identifier, Response Code

Data Element Definitions

User Role Type: The user's role, e.g., verification user, system administrator

User Organization: Optional field detailing the organization of the user e.g., Ministry of Health of Rwanda

Response Code: A coded response indicating whether the verification was successful or the reason for the verification failure or alert.

Event Identifier: A globally unique event id generated for every verification event.

Coordinates: The latitude and longitude captured via GPS for each verification event.

Location: A location code inferred from the coordinates (e.g., closest facility)

Request Source: The source of the verification event, either Mobile Application or the API Verification Organization 3rd-party platform name

Alert Code: A code indicating suspect activity for a product

Role Definitions

GTR User Roles fall into one of four broad types: No Access, Onboarding Partner, Dashboard User, Mobile Application Verification User, and API Verification Organisation. The 'No Access' type specifies that members have no access to any data, and all organizations and users that are not explicitly members of ither roles have 'No Access' as a default. For example, unauthenticated public users and users from research institutions and law enforcement agencies have no access, and any requests for data would need to be submitted to the GTR SteerCo according to the appropriate operational policy.

API Verification Organization Role Type

API Verification Organization

Definition: An API Verification Organization manages and/or develops a 3rd-party application that submits verification events to the GTR, and receives verification response codes, via the GTR API. The organization manages users scan product barcodes using 3rd-party application, and data are stored within this application.

Data Access: Verification Event Request Data and Verification Event Response Data generated by all users using the 3rd-party application

Purpose for Access: Organizations and/or countries may have existing verification systems that will leverage the verification service of the GTR, or they may want to develop new '3rd Party' mobile or other applications for this purpose. An example of such a 3rd-party application is an existing country logistics management information system (LMIS) that includes functionality to scan barcodes.

Dashboard User Role Type

Country Authority Dashboard User

Definition: A Country Authority Dashboard User will access the dashboard to track, monitor and respond to verification events and the corresponding suspect activities.

Data Access: Users with this role will need access to Aggregate Trend Data. They may also need access to specific Batch and Serial Identification Data to work with manufacturers to trace suspect activity.

TBC: Country access to serialization

Purpose for Access: The country authority is involved in the investigation of suspect activity and failed verification events, and the identification of sites in their country where verifications are failing, possibly due to hardware configuration or training issues.

Onboarding Partner Dashboard User

Definition: The Onboarding Partner (OBP) is the brand owner of the product, who supplies the batch and serial identification information to the GTR. This role is responsible for investigating suspect activity.

Data Access: The OBP will have access to Aggregate Trend Data for products they have supplied. These data will have product, country, response code and alert codes, and location facets included. In cases where suspect activity needs to be investigated, detailed granular event information may be necessary.

Purpose for Access: This role needs information to investigate suspect activity and verification failures, as well as to monitor GTR operations involving their products.

Procurement Agent Dashboard User

Definition: A procurement agent is an organization that actively procures products that are supported by the GTR platform.

Data Access: Aggregate Trend Data with Product, Country, and Response Code facets for products the organization has procured.

Purpose for Access: This role will access verification event trends and suspect activity to monitor supply of procured products.

System Administrator

Definition: The System Administrator is responsible for day-to-day management of all data in the platform on behalf of the GTR participants. This role is technical in nature, and members will be part of the technology solution vendor technical team.

Data Access: The system administrator needs access to all data stored and generated by the GTR.

Purpose for Access: This role requires access to all data to facilitate the daily operations of the GTR, and to respond to user support requests.

Supply Chain Champion / Funder Dashboard User

Definition: A Supply Chain Champion / Funder is an organization that is funding, directly or indirectly, the product and devoting significant resources, including technical assistance, for product roll-out and administration.

Data Access: The Supply Chain Champion will require access to Aggregate Trend Data with Batch and Country facets for the countries they are active in.

Purpose for Access: The Supply Chain Champion will link Aggregate Trend Data to other data sources, which specify the intended destination of products, to identify diverted products. Linked data can also be used to calculate Supply Chain Velocity, to determine time taken for products to reach their destination.

Mobile Application Verification User Role Type

Mobile Application Verification User

Definition: Mobile Application Verification Users scan product barcodes using the GTR mobile application. These verification events are submitted to the GTR and a response indicating verification success or failure is returned by the GTR. The users will use the GTR mobile verification application.

Data Access: Verification users will have access to all data which they submitted to the GTR, as well as the response code of the request

Purpose for Access: Mobile Application Verification 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.

Onboarding Partner Role Type

Onboarding Partner Organization (OBP)

Definition: The Onboarding Partner Organization is the organization that is represented as the brand owner of the product and is expected to be the organization that will supply Barcode Batch and Serial Identification Data to the GTR. Non-manufacturers which carry out the serialization for the OBP, such as Packers, will submit these data to the GTR via the OBP.

Data Access: Product Master Data, Manufacturer Master Data, Barcode Batch and Serial Identification Data for the organization’s products.

Purpose for Access: These data are generated, owned and submitted by the OBP.

Data Access

To ensure that data generated and submitted by verification users and the OBPs are kept secure, data access will be allowed for each role only where there is sufficient rational. Data access is detailed in this document and follows the core principles of the GTR which specify that patient and user data should be kept confidential and stored securely, and that participants who create the data own that data.

Users of the dashboard and the verification applications will be required to accept an end user license agreement detailing how any data they generate may be used. Non-disclosure agreements will be signed by participants, detailing that data may not be shared or used for purposes other than those specified and agreed to.

It should be noted that the product serialization data is highly confidential and should not be shared as these data can be used to create fake barcodes.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, Manufacturers have access to all information on their own products (blue), but not for products from other manufacturers, and country authorities may see data generated by users in their verification sites(green), but not information from other countries. System administrators have access to all data, regardless of who generated them (green). Procurement agents and Supply Chain Champions may see data from the countries they are active in (orange).

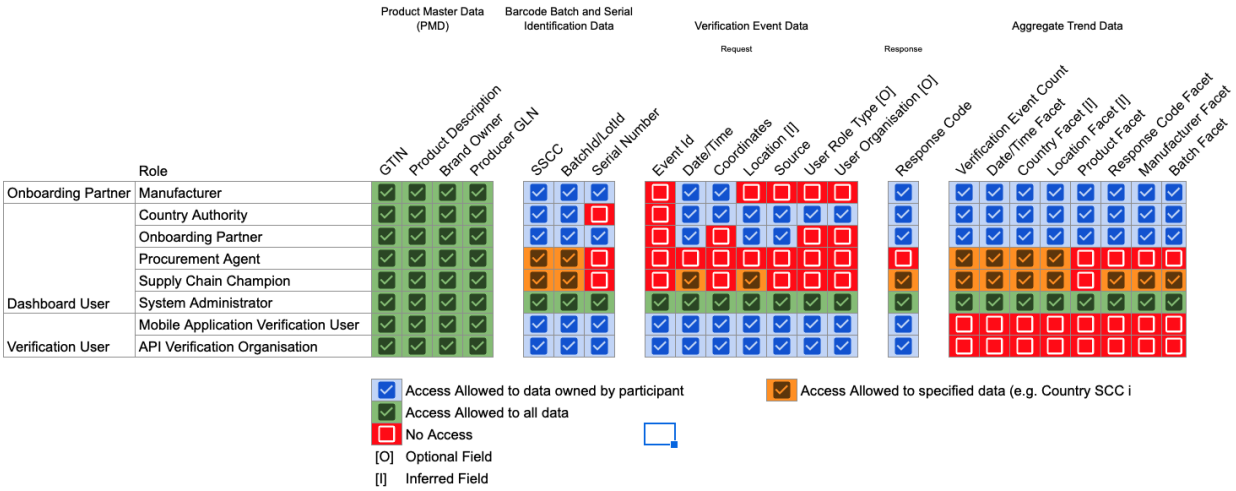

Figure 2: Data Access Matrix

In summary, serial numbers are not shared and trend data giving information on the number of events per product and/or country are sensitive as well and will not be shared without explicit permissions being provided.

Change Management Process

Changes to this Data Access Protocol shall be made according to the Data Governance Protocol.

New data elements may need to be collected as the functionality of the GTR expands, new roles may need to be added, or more granular data access permissions may need to be developed.

Data Protections

It should be noted that UNICEF has privileges and immunities that will protect GTR data from access by governments or third parties in the event that these parties request exceptional access. These immunities and privileges are specific to UNICEF as a UN agency. If and when the GTR is hosted by another entity, this should be taken into account.

Appendix A: Aggregate Trend Data Examples

Total of Alerts per Country

ABSOLUTE: TOTAL OF ALERTS PER COUNTRY

	2021 - Week 31			2021 - Week 32			2021 - Week 33			2021 - Week 34		
Country	# of Alerts	Total Scans	Rate %	# of Alerts	Total Scans	Rate %	# of Alerts	Total Scans	Rate %	# of Alerts	Total Scans	Rate %
	758	5,771,184	0.01%	838	5,644,704	0.01%	683	5,859,962	0.01%	779	5,772,216	0.01%
	6,010	6,405,322	0.09%	5,836	6,094,516	0.10%	5,008	6,068,841	0.08%	5,690	6,552,503	0.09%
	5,383	2,050,459	0.26%	4,741	2,440,617	0.19%	4,454	2,079,726	0.21%	4,254	1,950,942	0.22%
	498	613,026	0.08%	450	482,422	0.09%	394	358,510	0.11%	631	604,158	0.10%
	742	6,638,337	0.01%	835	6,898,227	0.01%	640	7,031,371	0.01%	667	7,279,478	0.01%
	40,070	37,189,483	0.11%	38,685	35,365,913	0.11%	56,847	36,536,078	0.16%	48,487	36,159,423	0.13%
	3,350	2,170,987	0.15%	1,480	2,334,199	0.06%	1,267	2,345,013	0.05%	4,174	2,354,006	0.18%
	128	802,983	0.02%	149	782,655	0.02%	141	635,922	0.02%	65	719,428	0.01%
	254,768	30,581,018	0.83%	239,603	28,880,174	0.83%	221,608	28,126,486	0.79%	237,136	30,851,074	0.77%
	768	1,967,370	0.04%	766	1,912,507	0.04%	711	1,956,998	0.04%	746	1,916,692	0.04%
	5,558	1,848,930	0.30%	4,181	1,658,883	0.25%	4,309	1,734,165	0.25%	3,955	1,831,606	0.22%
	453	2,771,499	0.02%	441	2,946,174	0.01%	493	2,768,999	0.02%	445	2,807,115	0.02%
	894	7,318,939	0.01%	4,441	7,788,745	0.06%	910	6,135,852	0.01%	863	7,062,221	0.01%
	1,343	1,085,782	0.12%	1,951	1,158,146	0.17%	1,458	1,184,071	0.12%	1,965	1,220,581	0.16%
	78	102,779	0.08%	98	113,502	0.09%	111	112,933	0.10%	248	118,621	0.21%
	4	375	1.07%	0	844	0.00%	4	642	0.62%	0	1,483	0.00%
	617	1,677,896	0.04%	823	1,640,422	0.05%	613	2,232,457	0.03%	736	1,906,259	0.04%
	482	1,247,925	0.04%	227	1,238,215	0.02%	237	1,247,875	0.02%	152	1,166,567	0.01%
	121	199,236	0.06%	104	205,719	0.05%	88	214,845	0.04%	91	238,715	0.04%
	1,477	184,556	0.80%	3,373	184,574	1.83%	1,547	191,140	0.81%	2,658	186,151	1.43%
	60,481	6,376,250	0.95%	56,932	6,225,892	0.91%	61,927	6,376,050	0.97%	59,744	6,408,518	0.93%
	293	2,161,757	0.01%	328	2,301,529	0.01%	309	2,507,986	0.01%	583	2,495,431	0.02%
	11,321	28,707,323	0.04%	12,293	29,651,717	0.04%	10,302	28,795,507	0.04%	12,285	29,127,534	0.04%
	28,838	4,470,016	0.65%	8,221	4,050,488	0.20%	14,434	3,910,364	0.37%	9,530	3,966,548	0.24%
	3,569	10,351,968	0.03%	3,873	10,551,531	0.04%	3,535	9,776,547	0.04%	3,005	8,611,169	0.03%
	926	3,628,714	0.03%	738	3,765,841	0.02%	833	3,999,856	0.02%	944	4,158,088	0.02%
	280	822,013	0.03%	200	815,998	0.02%	239	824,121	0.03%	111	838,597	0.01%
	320	4,048,680	0.01%	401	4,282,706	0.01%	351	4,210,147	0.01%	241	4,155,868	0.01%

Total Scans and Percentage Alerts