

Interoperable CCE Data Transmission

Last updated: March 30, 2025

Scope

Monitoring cold chain equipment (CCE) is critical to ensure safe vaccine storage. The value and utility of CCE monitoring data increases when that data is connected to country decision-making processes and I.T. systems. To that end, the WHO PQS EMS specifications (i.e., Clause 5 of the **WHO/PQS/E006/DS01** specification) require manufacturers of connected CCE equipment to send CCE data to the country data-owner, at the country's request. However, the low-level details of these transmissions are not specified in the **E006/DS01** standard. The requirements in this document clarify the existing EMS requirements in **WHO/PQS/E006/DS01.2, Clause 5 – Data Delivery to External Systems**. They are provided to promote a common approach for CCE data delivery between [Data Suppliers](#) and [Employers](#). Note that these requirements were developed as a supplement to the existing EMS specification, but they are applicable to both EMS and non-EMS (i.e., RTMD) platforms.

Terms and definitions

Requirements terms

This document uses specific requirement keywords to establish **mandatory** and **optional** obligations. The definitions below clarify the intent behind each term:

"**Shall**" indicates a **mandatory** requirement. Compliance with "shall" statements is **compulsory** and enforceable. Failure to adhere to a "shall" requirement constitutes non-compliance with this specification.

"**May**" indicates an **optional** feature or practice. Compliance with "may" statements is **permitted but not required**. Suppliers have discretion in implementation, and deviations do not constitute non-compliance.

Where appropriate, "**should**" is used to indicate a **recommended but not mandatory** practice. While not strictly required, non-compliance with "should" requirements may impact performance, reliability, or interoperability.

Definitions

[Appliance](#): The cold chain appliance or device that is the subject of monitoring. This may be a vaccine refrigerator, freezer, cold room, refrigerated vehicle, transportable storage, or other device.

CCE Data: CCE temperature and/or performance data collected by an EMS logger, RTMD, or other digital CCE monitoring device.

Data object: A standardized identifier of a unique administration, performance, use or environmental metric that is used to record and analyse data.

Data Supplier: The legal manufacturer or reseller of cold chain monitoring equipment (esp., RTMDs and EMS-compliant CCE), who is responsible for providing remote CCE monitoring services to the employer.

Datetime: Data that represents a specific point in time, including both date (year, month, day) and time (hour, minute, second).

Employer: The organization responsible for ownership and/or utilization of an appliance or device within an immunization programme, health system or initiative.

Employer System: A networked, server-based system which is operated by (or on behalf of) the employer and which receives CCE Data from the Remote Data System.

Equipment Monitoring System (EMS): The general term used to describe the associated components, sensors, devices, appliances, and data systems that enable cold chain equipment monitoring.

Equipment Monitoring Device (EMD): A device that functions to 1) retrieve data from the appliance's logger and other onboard sensors and 2) store, analyse and communicate data, errors, and alarms, and is the subject of specification **WHO/PQS/E006/EM01**.

Host: The party responsible for managing the Remote Data System. Generally, this is the legal manufacturer or reseller, but could be a contracted third-party.

Legal manufacturer: The natural or legal person with responsibility for the design, manufacture, packaging and labelling of a product or device before it is placed on the market under their own name, regardless of whether these operations are carried out by that person or on their behalf by a third party.

Logger: A data recording device that is integrated within an appliance or transport device and is the subject of specification **WHO/PQS/E006/DL01**. It stores data for use and analysis and provides access to its data.

Remote Data System: A networked, server-based storage system for the collection, management, and communication of CCE data. The Remote Data System is managed by the host.

Remote Temperature Monitoring Device (RTMD): A temperature monitoring device with integrated data logging, which uses network communication (mobile network, GPRS, UHS, satellite, etc.) to periodically transmit data to a remote data system. RTMDs are the subject of specification **WHO/PQS/E006/TR03**.

Reseller: A commercial entity, licensed to act on behalf of a legal manufacturer, and which carries product liability and warranty responsibilities no less onerous than those carried by the legal manufacturer.

Data delivery requirements

1. General

- 1.1. **Data supplier** shall transmit CCE data as UTF-8-encoded JSON via HTTPS POST to the **employer system**.
- 1.2. **Data supplier** shall specify the content type and character encoding of the request body using the Content-Type HTTP header (e.g., `Content-Type: application/json; charset=utf-8`).
- 1.3. **Data supplier** shall, at **employer's** discretion, authenticate against **employer system** by either:
 - Posting an access token in an HTTP header specified by the **employer** (e.g., `x-api-key`). The name of the HTTP header should be configurable on a per-country basis, OR
 - Using HTTP Basic Authentication (`Authentication` header)
- 1.4. **Data supplier** shall limit the size of HTTP request bodies to a maximum of 1 megabyte (1MB), measured after any applicable content encoding (e.g., compression) is applied.
- 1.5. **Data supplier** shall expect the **employer system** to use standard HTTP `2xx`, `4xx`, and `5xx` response codes, corresponding to their conventional meanings. **Data supplier** may receive JSON in the response body, containing additional details.
- 1.6. If **employer system** supports it, **data supplier** may transmit binary Gzip-compressed request bodies with a corresponding HTTP Content-Encoding header (i.e., `Content-Encoding: gzip`). When transmitting compressed request bodies, **data supplier** shall NOT further encode (e.g., Base64) the binary request body.
- 1.7. **Data supplier** may include custom HTTP headers in their requests. The name of a custom header can be any reasonable value that doesn't conflict with the names of well-defined HTTP headers.
- 1.8. **Data supplier** should NOT send duplicate data to **employer system** except under the following conditions:
 - Data is retransmitted at the explicit request of the **employer**.
 - Data is retransmitted following a delivery failure or when delivery status is ambiguous.
 - A system malfunction, outage, or recovery process necessitates re-sending data to ensure data integrity.

2. Rate limiting and transmission timing

- 2.1. To prevent excessive load on the **employer system**, the **data supplier** shall, by default, deliver CCE data serially (i.e., no more than one in-flight request at a time). **Data supplier** may increase concurrency if **employer** and **data supplier** mutually agree on a concurrency limit and if **data supplier** strictly adheres to the agreed limit.
- 2.2. **Data supplier** may transmit **CCE data** in batches on standard intervals. Ideally, **data supplier** should transmit **CCE data** (batched or not) to the **employer** within a few minutes after it is received by the **remote data system**.

- 2.3. **Data supplier** shall send CCE Alarm notifications to **employer** no more than 15 minutes after the notification is received by the **remote data system**. When transmitting CCE alarm notifications, **data supplier** shall include all **CCE data** that was collected since the last attempted transmission of **CCE data** for the affected CCE device.

3. JSON payload format

- 3.1. When sending **CCE data** to **employers**, **data supplier** shall adopt the Data Objects naming conventions and definitions from **WHO/PQS/E006/DS01, Annex 1: Cold Chain Data Objects**, plus the following additional Data Object definitions:

Object ID	Data Object	Type	Required
transferId	ID to uniquely identify data transmission (and allow for identification of re-transmissions)	string	Required
transferSrc	Source of the data transmission (e.g., data supplier URI)	string	Required
transferType	Type of transmission (ems , rtm) EMS-compliant devices should specify the ems transferType, while non-EMD RTMD should use rtm transferType.	string	Required
schemaVersion	Transmission schema version (e.g., 0.7.2), located in the \$id field of the transmission schema (see Attachment 1: Schema for Interoperable CCE Data Transmission)	string	Required
transferredAt	Datetime of data transmission in ISO8601 format with explicit timezone offset (e.g., 2023-11-14T13:01:01.420373Z)	string	Required

- 3.2. **Data supplier** shall transmit JSON messages that can be validated according to the JSON schema published in **Attachment 1: Schema for Interoperable CCE Data Transmission**. If there are discrepancies between this document and the JSON schema published in Attachment 1, the JSON schema shall take precedence.
- 3.3. Although the JSON-Schema treats many **data objects** as optional – due largely to variation between monitoring systems – **data supplier** shall transmit all defined EMS **data objects** that they collect, including those that are marked as optional. **Data supplier** should also transmit all custom **data objects** that are collected, unless **employer** agrees to the exclusion of those data in part or whole.
- 3.4. **Data supplier** shall transmit **CCE data** at the same time resolution the data was recorded on the **logger**. For example, if a **logger** records data on 15-minute intervals, then the transmitted **CCE data** shall preserve and reflect that same 15-minute time resolution. **Data supplier** may provide aggregated or summarised data in addition to the full-fidelity records.

4. Monitoring and error handling

- 4.1. **Data supplier** shall retry **CCE data** transmissions that do not receive an HTTP **2xx** response from the **employer system**.
- 4.2. **Data supplier** shall continue to retry failed transmissions at least 6 times over a 24-hour period before abandoning retransmission attempts. Failed transmissions shall NOT block the transmission of other pending or undelivered data (e.g., a single bad payload should not cause data delivery attempts for *other* payloads to be blocked for 24 hours).
- 4.3. **Data supplier** should immediately abandon transmissions that receive a response code from the **employer system** that is generally associated with a permanent failure condition, as indicated below:
 - HTTP **501** – Not Implemented error
 - HTTP **505** – HTTP Version Not Supported error
 - All HTTP **4xx** errors, except for HTTP **404**, **408**, **409**, and **429**
- 4.4. When retrying failed transmissions, **data supplier** shall schedule retransmissions using either: exponential backoff with jitter or a uniform backoff interval that is sufficiently long (e.g., multiple minutes) to minimize load on the **employer system**. For the avoidance of doubt, “exponential backoff with jitter” indicates a scheduling approach where the interval between transmission attempts increases according to an exponential function and random jitter is added to each delay to avoid synchronized retries from multiple clients. In contrast, a “uniform backoff interval” uses a static interval to schedule all retry attempts. **Data supplier** shall describe their selected retry scheduling approach to the **employer**.
- 4.5. In the special case where **data supplier** receives an HTTP **429** response that include a **Retry-After** value, **data supplier** shall schedule the next retry based on whichever interval is longer: the **Retry-After** value or the **remote data system’s** own computed (or configured) backoff interval.
- 4.6. **Data supplier** should log all failed transmission attempts, including the response code and error message, for analysis and troubleshooting.
- 4.7. **Data supplier** shall provide the **employer** with an email address to communicate problems or request technical assistance. **Data supplier** may provide additional communication channels (e.g., phone number, WhatsApp contact, Slack or Discord channel, etc.) at the mutual agreement of **data supplier** and **employer**. The **data supplier** shall provide **employer** with a Service Level Agreement (SLA) to document **data supplier’s** response-time obligations on provided channel(s).
- 4.8. **Data supplier** shall monitor the status of **CCE data** transmission to **employer system**.
- 4.9. **Data supplier’s** monitoring processes shall notify **data supplier** staff when **CCE data** transmission failures exceed a configurable threshold (e.g., failure rate exceeds 10% over a rolling 60-minute period). **Data supplier** shall notify affected **employer(s)** within 48 hours when **data supplier** detects an elevated rate of CCE data transmission failures.

5. Data retransmission

- 5.1. At the request of the [employer](#), [data supplier](#) shall retransmit [CCE data](#) that was captured within the most recent six months of time. This is intended primarily as an emergency option for the [employer](#) (e.g., in cases where [employer system](#) is offline for an extended period; or for populating new systems with historical data).
- 5.2. [Data supplier](#) shall be able to filter the retransmitted [CCE data](#) to include only a specific time range within the indicated six-month period. For example, employer shall be able to request retransmission of data for one or more CCE during a period of time specified by a beginning and an ending date or [datetime](#).
- 5.3. [Data supplier](#) shall be able to filter the retransmitted data to include either: all [CCE data](#), including [CCE data](#) that was previously sent successfully, or only [CCE data](#) that was never transmitted successfully.

Attachment 1: Schema for Interoperable CCE Data Transmission

Given that Microsoft Word is not suitable for presenting JSON data, the JSON schema is provided as a separate document.

Attachment 2: Country Guidance

The CCE Data Delivery Requirements, defined above, detail the responsibilities that data suppliers must fulfil. Although there is no PQS pre-qualification process for country implementations, countries have a similar and corresponding set of responsibilities to ensure reliable exchange of CCE data.

This section articulates a set of considerations that countries are encouraged to satisfy when implementing systems and processes for CCE data delivery.

System considerations

Countries must have capacity to handle the expected data processing loads. It is the country's responsibility to provision and maintain sufficient system capacity to support normal CCE data processing operations, including retransmissions and catch-up work resulting from temporary disruptions.

Countries are encouraged to create system capacity plans that account for expected peak loads, including:

- Burst traffic from retry mechanisms following transient failures.
- Increased request volume due to catch-up processing after an outage.
- Regular fluctuations in transmission rates based on business cycles.

Country is also encouraged to perform load testing on their system to confirm performance limits and behaviour under extreme load. Such testing would allow the Country to communicate clear concurrency limits and capacity expectations to data suppliers, to facilitate responsible traffic management.

The proper behaviour of data supplier systems is partially dependent on the proper behaviour of the country system, including the following considerations:

- Country system should respond to data supplier HTTP POSTs using standard 2xx, 4xx, and 5xx response codes, corresponding to their conventional meanings. Country responses could optionally include JSON in the response body to communicate additional details.
- When country system is overloaded, it should send an HTTP 503 response, which is commonly used to indicate a temporary overload condition. Alternatively, a country system could send HTTP 429 - Too Many Requests responses, provided those responses include an explicit `Retry-After` value. If the `Retry-After` value is not provided, country should prefer a more generic HTTP 503 response.
- Country system should validate the JSON in the HTTP request body *before* responding to Supplier, which allows the employer system to communicate problems with the JSON payload using HTTP response codes. For example, non-JSON payloads and JSON syntax errors might receive an HTTP 400 "Bad Request" response; while semantic errors, including and especially *failures to validate against the JSON Schema in Annex 1*, might receive an HTTP 422 - Unprocessable Entity response.

- Country system should accept and gracefully handle duplicate data received from the data supplier.
- Country system should not expect data suppliers to guarantee that data is always sent in order. When all systems are healthy, data suppliers will usually deliver data in order. But normal error handling and retry behaviour will ensure that data is sometimes delivered out of order. This is unavoidable without significant implementation complexity, so countries should expect that their systems will sometimes receive out-of-order data.
- Country system should use valid SSL/TLS certificates that do not require data suppliers to install intermediate certificates or private root material.

Management considerations

The Country is responsible for authorising access to their own sovereign systems, so the country is responsible for issuing and maintaining credentials that allow data suppliers (or data supplier systems) to authenticate against country system(s).

Countries and data suppliers have a mutual obligation to establish clear, effective communication channels between their respective organizations. Countries should provide data suppliers with an email address or other suitable communication channel (e.g., phone number, WhatsApp contacts, Slack or Discord channel, etc.) that data suppliers can use to communicate problems or request technical assistance. Countries are encouraged to respond promptly to data supplier communication on these channels.

Countries should monitor the status of the systems and software that receive and process CCE data transmissions from data suppliers. Countries should be able to automatically detect when the system receiving CCE data is offline or when JSON validation errors exceed a configurable threshold (e.g., JSON validation failure rate exceeds 10% over a rolling 60-minute period). Countries should notify affected data suppliers promptly (ideally, within the day) whenever they detect that the receiving system is offline, or an elevated rate of JSON validation errors is detected.