NDTRS Technical Standard for Secure Electronic Data Submission and National Integration

1. EXECUTIVE SUMMARY: THE NATIONAL DATA ASSET

The **National Drug Treatment Reporting System (NDTRS)** is the primary national epidemiological database for treated problem drug and alcohol use in Ireland. Funded by the Department of Health and managed by the Health Research Board (HRB), it informs national policy and fulfils Ireland's international reporting obligations to the **European Union Drugs Agency (EUDA)**.

Recognising requests by service providers to transition to electronic data exchange, this guidance document outlines a process to maintaining the highest standards of data integrity for a publicly funded resource.

This document sets out **high-level technical and governance principles only**. Detailed operational, legal, and technical arrangements will be defined in:

- Memorandum of Understanding (MoU), Data Sharing Agreement
- Data Protection Impact Assessment (DPIA).

2. PII GOVERNANCE: THE "SILOED VISIBILITY" MODEL

The HRB recognises that epidemiological data exports often contain **Personally Identifiable Information (PII)** such as names and addresses. To balance epidemiological data utility with research privacy, the NDTRS employs a **siloed partitioning architecture** within the LINK interface:

- **Service Provider View:** Authorised staff at the originating service can view and edit the PII (Names, Addresses, etc.) for their own service users within the LINK portal.
- **NDTRS View:** All PII is filtered through an **Anonymisation Layer**. HRB staff see only pseudonymised "Statistical IDs." They have **zero visibility** of certain PII fields (such as names and addresses). However, client numbers and IHI (where populated) are visible.

3. TECHNICAL SPECIFICATIONS

To be considered for participation in electronic submission, the service provider's IT vendor must configure your export tool to match these "Hard Standards":

Feature	**Requirement**
File Format	CSV (Flat file)
Character Encoding	**UTF-8** (Mandatory for Irish fadas and special characters)
Schema Version	**Schema to be made available on request**
Mapping	Local values must be programmatically mapped to HRB numeric codes. **Reference Data:** The HRB will provide all required reference tables, code sets, and data dictionaries. These will include format specifications (e.g. field length, permitted values, date formats). **Validation Framework:** High-level validation rules will be defined within this standard, with detailed validation constraints, rejection rules, and error thresholds specified in the MoU and supporting technical documentation.

Essential requirements	• **Episodic cases:** All assessment and treatment data must be recorded and submitted on an episodic basis, in full compliance with NDTRS protocol specifications in order to meet national reporting obligations to the EUDA. • **Episodic Data Transformation:** Where service provider systems do not natively support episodic structures, transformation rules must be applied to derive NDTRS-compliant episodes. The high-level definition of an episode is outlined in the NDTRS Data Collection Protocol. System-specific transformation logic, including rules applied during upload processing, will be agreed and documented as part of the MoU. • **NDTRS LINK Data Items:** In general, all current NDTRS LINK tabs and associated data items are required, with the exception of the Drug-Related Intimidation and Mental Health tabs. In certain circumstances, other arrangements may be acceptable and will be specified in relevant Memorandum of Understanding. • **Geocoding:** Geocodes must be recorded to support national-level service planning, resource allocation, and Sláintecare monitoring requirements. • **Address Data Governance:** Service providers are fully responsible for ensuring that all address related data, including geocodes, are accurately recorded and reported. These variables are critical for Sláintecare monitoring and population-based analysis/funding. As address fields are encrypted, the NDTRS has limited capacity to verify or validate this information once submitted. Accordingly, the accuracy and integrity of all address related data, rest solely with the service provider.

PII Field Requirements

The following fields are accepted via direct entry to LINK only and are subject to "Siloed Visibility" rules:

- **First Name / Surname:** Plain text (Visible to service provider only).
- **Full Address:** Plain text (Visible to service provider only).

3.1 PII Governance: 'Siloed Visibility' Model

The detailed governance, responsibilities, and escalation procedures supporting this model will be defined within the Memorandum of Understanding (MoU) and associated Data Protection Impact Assessment (DPIA).

The NDTRS operates a strict “siloed visibility” model, whereby HRB staff do not have access to directly identifiable personal data (PII) such as names and addresses at any stage of the data submission, upload, or validation process.

This model reflects the principles of:

- Data minimisation
- Privacy by design and by default
- Role-based access control

Under this model:

- Service Providers retain full visibility and responsibility for all identifiable data relating to their service users within their own systems and within the LINK interface. They remain responsible for to ensure that accurate data is provided to inform national policy and EU data reporting requirements.
- HRB Staff, operate on pseudonymised data, including statistical identifiers and associated non-identifiable variables.

Operational Implications:

- All data validation, troubleshooting of upload issues, and resolution of data quality queries involving identifiable data must be undertaken by the service provider within their local system and the LINK interface.
- The HRB will provide technical guidance, validation outputs, and structured feedback, but cannot directly inspect or correct identifiable records.
- Where issues arise that cannot be resolved through pseudonymised data alone, resolution will rely on collaborative engagement with the service provider, who retains the ability to view and amend the underlying identifiable data.

This approach ensures that:

- The integrity and confidentiality of personal data are maintained at source
- The HRB does not process identifiable data beyond what is necessary for its statutory function.

4. THE 4-STAGE ONBOARDING PATH

No service is permitted to upload live data without passing through these four "Quality Gates":

Step 1: The Readiness Pack

Submit a **Technical Mapping Document** and a **DPO Audit**. This demonstrates that the service provider’s system is technically compatible with NDTRS requirements and that the data extraction and submission processes comply with applicable data protection legislation, including:

- The General Data Protection Regulation (GDPR), in particular:
    - Article 6 (lawful basis – legal obligation and public task)
    - Article 9 (processing of special category data for healthcare, public health, and research/statistical purposes)
- The Data Protection Act 2018 (including requirements for suitable and specific safeguards)
- Relevant statutory instruments governing the functions of the Health Research Board

It further confirms that appropriate safeguards are in place, including data minimisation, purpose limitation, secure processing, role-based access controls, and adherence to agreed data sharing and governance arrangements, as outlined in the NHIS Data Protection Impact Assessment (DPIA).

Step 2: Sandbox Stress Test

The service provider shall be granted access to the HRB *Sandbox* environment, which functions as a user-acceptance-testing (UAT), non-production environment. For the purposes of the sandbox test, **success is defined exclusively as the technical validation of the file structure against NDTRS minimum dataset specifications.**

The service provider must demonstrate the ability to successfully perform **repeated uploads**, including corrections and re-submissions, reflecting real-world operational conditions.

The service provider must upload a minimum dataset comprising **100 synthetic service user episodes**, supplied by the HRB. A **100% structural success rate** is required; that is, all records must be accepted by the system with zero structural or formatting errors.

Note: The sandbox test verifies only the technical compatibility and structural conformity of bulk-upload files. A file may meet structural requirements yet still contain inaccurate, incomplete, or poor-quality data. The sandbox test therefore does **not** provide assurance regarding the substantive quality or accuracy of the data submitted.

Step 3: Governance Agreement (MoU)

Prior to the commencement of live data submission, the service provider shall enter into a formal Memorandum of Understanding (MoU) with the HRB. This MoU defines the governance, compliance, and quality-assurance framework governing ongoing NDTRS bulk-upload activity.

For ongoing compliance, **success is defined by the quality, completeness, validity, and timeliness of submitted data**, not solely by the technical success of file uploads.

The MoU shall include a **Two Strike Policy**, whereby:

- If the minimum dataset quality score falls below **98%** for two consecutive monthly reporting

periods, third party upload permissions will be suspended.

- The 98% threshold refers to the proportion of records meeting defined data quality criteria, including:
    - Completeness
    - Validity (compliance with formats and permitted values)
    - Consistency across related fields
    - Timeliness of submission
    - The detailed calculation methodology will be specified in the MoU.
- Following suspension, the service provider will be required to immediately revert to manual data entry via the LINK interface until data-quality standards are restored and verified.

All NDTRS data must adhere to episodic reporting requirements as set out in NDTRS protocols. Monthly uploads are mandatory; however, more frequent uploads are permitted and encouraged where feasible. For example, all episodes (entries and exits) relating to January 2026 must be submitted no later than the end of February 2026.

To ensure the NDTRS can verify accuracy and compliance with the 98% data-quality standard, the MoU shall explicitly permit the conduct of **periodic audits**, post live migration (Step 4 below). These audits will be undertaken collaboratively by the service provider's management and the NDTRS team. Audits constitute the only reliable mechanism for validating the substantive quality of uploaded data; without them, it is not possible to assess data accuracy or determine compliance with quality-assurance thresholds.

Step 4: Live Migration

During the initial live period, all uploads will be subject to enhanced monitoring. Data will be processed in the LIVE environment, however formal acceptance of data quality will only occur following review by the NDTRS team.

At all times, the service provider must continue to enter data into LINK until written confirmation is issued by the HRB advising of the outcome of the audit and any resulting recommendations.

5. FUTURE-PROOFING: EUDA & TDI

The NDTRS follows the European Treatment Demand Protocol (TDI) as determined by EUDA. This protocol is subject to reviews from time to time by EUDA. Service provider's should be aware that the last TDI protocol took place in 2012 and also give consideration to the possibility that data requirements may change in the future in line with TDI protocol requirements, and therefore impact ability to make

electronic submissions. Note, EUDA plan a TDI protocol review in 2027.

6. SERVICE PROVIDER RESPONSIBILITIES

- **Roles and Responsibilities**: Each service provider must designate:
    - A Data Lead responsible for data quality and validation
    - A Technical Contact responsible for system integration

  These roles will act as primary contacts for NDTRS and are responsible for ensuring compliance with this standard.

- **Error Reporting and Resolution:** The HRB will provide structured feedback on errors and validation issues for uploaded files only. Detailed error reporting formats and support processes will be defined in the MoU. Service providers must ensure that:
    - Errors are reviewed after each upload
    - Corrections are made in the local system
    - Corrected data is re-submitted in subsequent uploads

- **Local Correction:**
    - All data upload errors must be corrected in service provider's **local system** and data re-uploaded.
    - Where corrections are made in LINK, corresponding updates must also be applied to the local system, to prevent discrepancies in future uploads.
    - The HRB will not manually "fix" CSV data. Service providers must ensure that appropriately trained staff are available to investigate and resolve data issues requiring access to identifiable records, particularly where upload failures or data inconsistencies occur.
    - The HRB will not accept responsibility for delays arising from the service provider's inability to access or resolve issues in identifiable data.
- **LINK Updates:**
    - All data gaps (outside of minimum dataset) must be manually input by the service provider directly in LINK, e.g. Geocodes, Drug Related Intimidation and Mental Health tabs.
    - All LINK validations must be appropriately addressed in LINK.
    - The HRB will share updated reference tables with the service from time to time. The HRB will share updates within 2 weeks of LIVE LINK implementation. The service provider must then ensure that all reference tables updates are implemented within their system no later than two weeks from the date of issue.
    - The Service Provider must agree to not edit references tables relating to the upload unless directed to do so by the HRB as part of an update.
- **Vendor Management:** The HRB provides the specification, but the service provider provides the solution. Support for local software is the responsibility of the service provider and their IT vendor.