	Recommendation on Data Minimisation		
	Document type	Recommendation	Drafting date
	Document reference		Approved by
	Version	1	Approval date
	Drafting date	July, 2024	Status

## RECOMMENDATION ON DATA MINIMISATION

**July, 2024 Written by Security & Privacy Committee**

### 1. Introduction

Data minimisation is a fundamental principle in data protection and privacy law, emphasising the collection and processing of only the essential data required for a specific purpose. This principle aims to mitigate risks associated with data breaches and misuse by ensuring that unnecessary personal data is neither gathered nor retained.

The data minimisation principle is prescribed by various regulations, all expressing that personal data must be "adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed" (e.g., Article 5(1)(c) of the GDPR, Article 4(1)(c) of Regulation (EU) 2018/1725, the minimum necessary rule of HIPAA, and as best practice in the NIST SP 800-122 guide to protecting the confidentiality of personal identifiable information (PII)).


### 2. Background

Under the current Data Use Agreement signed by WMDA members, compliant member organisations act as both data controllers and data processors: data controllers of the data generated and collected by themselves, and data processors of the data generated, collected, and shared with them by other member organisations. While WMDA strongly encourages all member organisations to apply data minimisation principles to all their communication channels, these recommendations are specific to communication between those entities engaged in registry-to-registry communication.

With the integration of EMDIS into the WMDA and the development of digital registry-to-registry communication solution, Match & Connect, an opportunity arose to provide recommendations for data minimisation to the membership. These recommendations are designed to ensure compliance with relevant regulations and WMDA Standards, regardless of the communication format. For the time being, these recommendations shall apply to the following stakeholder entities involved in the transplant process: Transplant Coordination, Patient Registry, Laboratories, WMDA, Donor Registry, Donor Centre, Cord Blood Bank, Collection Centre, and Courier.

In summary, the general recommendations for effective data minimisation in the context of registry operations involve:

- Only collecting and sharing essential patient and donor data necessary for matching assessment and transplantation procedures.
- Implementing pseudonymisation techniques to protect the privacy of individuals involved in the process.
- Limiting the scope of data shared during each phase of the registry process to minimise the risk of unauthorised access or disclosure of sensitive information.
- Ensuring compliance with relevant data protection regulations and guidelines to safeguard the privacy and confidentiality of patient and donor data throughout the registry operations.

	Recommendation on Data Minimisation		
	Document type	Recommendation	Drafting date
	Document reference		Approved by
	Version	1	Approval date
	Drafting date	July, 2024	Status

- Ensuring the accuracy and efficacy of the matching process while applying the principle of data minimisation.

### 3. WMDA Recommendations

This chapter delves into the intricacies of data management and data protection, with a focus on data minimisation in the context of transplant coordination. The definitions below offer a structured overview of the types of data exchanged between different stakeholders at various stages of the transplant process from the perspective of the patient (registry). It identifies the data subjects (donor and patient data) and the entities (not necessarily WMDA members) involved in each processing activity. Each processing activity is described and finalised with an assignment of Data Minimisation Levels for patient and donor to be applied to this process.

#### 3.1 Data Minimisation Levels

These definitions help to ensure that the principle of data minimisation is applied to the two relevant data subject domains, patients and donors, appropriately while maintaining the necessary balance between data protection and operational effectiveness.

##### P1: Patient Data with Enhanced Anonymity

Patient data as defined for the specific use case, with the following modifications to enhance anonymity:

1. Patient first name is omitted.
2. Patient last name is omitted.
3. Only the patient's year of birth is provided (instead of the full birthdate).

##### P2: Patient Data with Necessary Personal Identifiable Information (PII)


Patient data as defined for the specific use case, including all personal identifiable information (PII) necessary to ensure patient safety and accurate identification:

1. Patient first name included (optional).
2. Patient last name included (optional).
3. Full birthdate included.

##### D1: Pseudonymised Donor Data for Search

Donor data as defined for the specific use case. In this domain, donor data is pseudonymised by default. Donor personal identifiable information (PII) is not shared among the entities listed in this document.

Donors not requested for the patient (D2) have to be purged from the patient database once the search is stopped.

	Recommendation on Data Minimisation		
	Document type	Recommendation	Drafting date
	Document reference		Approved by
	Version	1	Approval date
	Drafting date	July, 2024	Status

## D2: Pseudonymised Donor Data for Requests

Donor data as defined for the specific use case (request). In this domain, donor data is pseudonymised by default. Donor personal identifiable information (PII) is not shared among the entities listed in this document.

This donor data may contain more up-to-date and more information than D1.

### **3.2 Process Activities in the Context of Data Minimisation**

#### **Search**

This involves entering limited patient information into a form to identify a suitable donor based on specific biological characteristics. The emphasis here is on entering only essential patient data necessary for matching purposes, minimising the amount of personally identifiable information (PII) collected and stored.

- Entering only limited patient information (P1) into a form that will allow identification of a suitable donor based on HLA and non-HLA biological characteristics.
- Performing a search and receiving pseudonymised donor/CBU results.
- Data Minimisation Level: P1-D1


#### **Requests (excluding Work-up)**

Activities such as changing patient status, sending requests to donor registries, and receiving pseudonymised donor information indicate a process where data is exchanged for the purpose of identifying potential matches or to request additional testing of the donor in preparation of next steps. Data minimisation in this context involves limiting the scope of patient data shared during these interactions, providing only the necessary information to facilitate the search process without unnecessary disclosure of personal details.

- Changing the patient status (electronically or manually).
- Sending a donor/CBU-related request with limited patient information to the donor registry/CBB.
- Receiving pseudonymised donor/CBU information relevant to the request.
- In case of centralized search: only send patient info to organisations at which the donor/CBU is registered.
- Data Minimisation Level: P1-D2

#### **Work-up Request**

This phase involves submitting prescriptions, performing tests and examinations on selected donors, and receiving fitness information and collection itineraries. Data minimisation efforts here would focus on ensuring that only relevant patient and donor information is shared during the work-up process, avoiding the unnecessary exchange of sensitive data that is not directly related to the medical assessment and selection of donors.

	Recommendation on Data Minimisation		
	Document type	Recommendation	Drafting date
	Document reference		Approved by
	Version	1	Approval date
	Drafting date	July, 2024	Status

- Submitting a prescription for a source of haematopoietic stem cells (HSC) or other cellular products on behalf of the patient to a donor registry.
- Donor registry and/or collection centre performing workup-related tests and examinations on the selected donor.
- Receiving donor fitness information and stem cell collection itinerary (if the donor is cleared).
- For CBUs, submitting a CBU shipment request on behalf of the patient to a cord blood bank.
- Receiving CBU release testing results from the cord blood bank.
- Data Minimisation Level: P2-D2

### Collection

Activities such as accepting donors based on medical clearance reports, receiving collection itineraries, stem cell products, and related documentation highlight the final stage of the process. Data minimisation in this phase involves limiting the amount of patient and donor data shared during the collection process, ensuring that only essential information required for the successful transplantation procedure is exchanged.

- Accepting the donor based on a medical clearance report.
- Receiving:
  - Collection itinerary/schedule from the donor registry.
  - Stem cell product (i.e., PBSC, bone marrow, DLI, CBU, or ADCU) and extra samples.
  - Related documentation and labels.
- Data Minimisation Level: P2-D2

### 4. Other Associated Activities that Involve Personal Data Outside the Scope of the First Version of this Recommendation

Transplantation, patient follow-up, donor follow-up (including S(P)EAR), possible genetic findings, donor/patient detail exchange, institutional data (contact persons at laboratories, TCs, CCs, CBBs, etc.).

#### Annex 1: Implications for Match- Connect

In the application of this recommendation within Match-Connect, in addition to the information that is absolutely necessary for business processes (mandatory fields), the minimisation of optional information (optional fields) should also be considered. You can view the full list here:

<https://share.wmda.info/x/iYTDH>