D1.2 Progress report on the implementation of a secure registry-to-registry communication system

Grant Agreement number: 881553
Project acronym: SAVDON
Work Package number: WP1

Organisation: **World Marrow Donor Association (WMDA)**
LEAR: Lydia Foeken
Project coordinator: Lydia Foeken
Tel: 0031 88 505 7900
E-mail: lydia.foeken@wmda.info
Organisation website address: www.wmda.info

Co-funded by
the Health Programme
of the European Union

"This Deliverable D1.2 of an activity received funding under an operating grant

Table of Contents

1. Introduction 3
   1.1 Background 3
   1.2 Requirements 4
2. Progress and Achievements 6
   2.1 Data migration to secure cloud service 6
      2.1.1 Former ICT landscape 6
      2.1.2 New developments 6
      2.1.3 Why APIs? 6
      2.1.4 Business requirements 7
      2.1.5 Best practices 8
      2.1.6 Challenges encountered during migration 8
      2.1.7 Outcome 9
   2.2 Search API 9
      2.2.1 Alternative Algorithms 9
      2.2.2 Side loading 10
   2.3 Connect API 14
      2.3.1 Approach to deliver the goal – EMDIS Proxy 15
      2.3.2 User Engagement – Work-up requests 16
      2.3.3 Integration of EMDIS into WMDA 18
   2.4 Security and Privacy 20
   2.4.1 Current projects 20
3. Project plan for 2021 22
   3.1 Search API 22
   3.2 EMDIS-Connect 22
   3.3 Security & Privacy 25

Appendix 1 – HAP-E and ATLAS Algorithm Requirements 26

Appendix 2 – Sideloading Requirements for WMDA's Search & Match Service 29

Appendix 3 – Conversation Guiding Questions investigating Donor Workup Requests 31

Appendix 4 – Proposed Governance, Financials and Technical blueprint of EMDIS integration 32

Appendix 5 – Security Essentials and Assessment Questionnaire 36

Abbreviations

API = Application Programming Interface

BMDW = Bone Marrow Donors Worldwide

CBB = Cord Blood Bank

CBU = Cord Blood Unit

CPU = Central Processing Unit

DKMS = Deutsche Knochenmark Spenderdatei

DMZ = Demilitarized zone (sometimes referred to as a perimeter network or screened subnet)

EMDIS = European Marrow Donor Information System

FHIR = Fast Healthcare Interoperability Resources

GDPR = General Data Protection Regulation

HL7 = Health Level 7

HLA = Human Leukocyte Antigen

IaaS = Infrastructure as a service

ICT = Information and Communications Technology

IDM = Infectious Disease Markers

IP = Internet Protocol

JSON = JavaScript Object Notation

NoSQL = Stores information in JSON documents instead of columns and rows used by relational databases

PaaS = Platform as a service

PHP = Hypertext Pre-processor

QA = Quality Assurance

RDP = Remote Desktop Protocol

SaaS = Software as a service

SIEM = Security Information and Event Management

WMDA = World Marrow Donor Association

ZKRD = Zentrales Knochenmarkspender-Register Deutschland

1. Introduction

This progress report on the implementation of a secure registry-to-registry communication system details the process and achievements the WMDA and international partners, including EU member states, have made towards implementing a secure registry-to-registry communication system in 2020. This report allows analysis of progress by all parties involved and will enable them to focus their efforts on areas of identified weaknesses. In addition, this report includes a clear roadmap on the future developments and improvements that will guide efforts in 2021.

This Deliverable *D1.2 Progress report on the implementation of a secure registry-to-registry communication system* is part of the 2020 work programme of the World Marrow Donor Association (WMDA) for the EU Third Health Programme (2014-2020).

1.1 Background

WMDA took over the operation of the Search & Match Service (known as BMDW) on January 1, 2017. At that time phase 1 had just been implemented and phase 2 was in progress and would be completed in April 2018. The key features of the phase 1 and phase 2 development projects are summarised below:

2016 (phase 1):

- Introduced predictive matching algorithm
- Modern, user friendly service web site
- Cleaned up who has access to the service
- Secure code, robust hosting

2018 (phase 2):

- Automated data upload (through API or web upload)
- Transition to XML data schema
- Introduced extended dataset
- Improved data quality and good insight on capabilities of registries

The implementation of a secure registry-to-registry communication system (Connect), or Phase 3, requires input from the whole community. WMDA has actively promoted participation in the project through Stem Cell Matters (Membership newsletter every three weeks) and during the last three WMDA biannual conference meetings. Under the remit of the WMDA's 'Pillar 1' strategic theme, an outline was presented at the WMDA conference meetings in November 2017, June 2018 and November 2018.

The WMDA community was canvassed via online surveys several times during 2018. Feedback confirmed a demand to 'democratise' the global donor pool and a desire to improve the functionality of the Search & Match Service. At the WMDA November 2018 meeting, delegates were presented with the latest iterations of the proposed Phase 3 plans (coined Connect) and they provided strong approval to the ability to connect to all registries via a single communication platform.

As well as direct member feedback, several external ICT experts, who volunteered to help and are active in other industries, have commented that the project is feasible and will not have a significant impact on the financial resources of registries. Nevertheless, a number of member ICT experts saw barriers and did not feel well informed. These concerns were explored and considered in the design for a customizable solution to help all registries in facilitating transplants in their respective countries.

1.2 Requirements

WMDA strives to significantly reduce the time needed for information processing in the donor/CBU search and request processes and to create fully transparent data exchange - including actual process status - across all registries.

To achieve this, and underpin a safe and sustainable supply of cellular products for its members, WMDA works across three main themes:

1. **Search:** Optimise Search

Ensuring that patients are informed quickly about their chances for transplant is a prime task for WMDA member organisations.

WMDA will actively contribute to this by ensuring:

- All WMDA member organisations are able to search the best available global donor and cord blood data, which is recognised as 'the single version of truth' for all patient searches.
- The proper selection of donors and cord blood products at each moment in time is based on the confidence that donor and cord details presented are up-to-date and checked by WMDA.
- Involving WMDA member organisations where possible. WMDA will further strengthen the relationship with and between WMDA member organisations to ensure that good quality data are available in the global file.
- All patients have equal rights to health treatment. WMDA supports this by striving towards a high-quality data source for all patient searches.

2. **Match:** Find the best Match

WMDA identifies best practices in donor search and supports the operations of member organisations. To operate the Search & Match Service a probabilistic matching algorithm will be offered that is accessible in different ways.

WMDA facilitates this by ensuring:

- Search coordinators and transplant centres can register their patients manually, run their search and find the best stem cell source through a variety of filter options in the Search & Match Service.
- Search coordinators and transplant centres can register their patients electronically, run their search and find the best stem cell source through a variety of filter options in the Search & Match Service.
- Search coordinators can automatically run the search from the local software application, receive a match list electronically and use their local settings to select the best stem cell source.
- Search coordinators receive status updates and updates about new potential matches and donor availability.

3. **Connect:** Be connected

Safeguarding and promoting patient and donor care are the ultimate goals of all WMDA members' operations. WMDA will keep in contact with member organisations to ensure that their needs are understood and considered. WMDA members strive collectively to improve the communication between member organisations to ensure transparency and efficiency and to reduce the time to facilitate requests from transplant centres.

WMDA will support this through:

- Accommodating private and secure communication connectors for search coordinators.
- Facilitating easily accessible operational information of member organisations.
- Implementing traceability mechanisms to help search coordinators to keep track of their requests.
- Facilitating low maintenance data exchange for donor/CBU search, testing, typing and work-up requests.
- Allowing registries to make their business decisions and to connect in a well-governed manner.
- Supporting several mechanisms, e.g., web interface and API, to facilitate communication.
- Provide adequate tools for minimising data entry, reducing data errors.

The details of the requirements are outlined on WMDA Share in the secure Working area of the WMDA Connect group. In 2019, WMDA mainly investigated and handled the requirements to optimize search. To learn more about the WMDA's efforts to optimize search, please consult Deliverable *D1.2 Progress report on data quality in EU Member States* for 2019.

Chapter 2. Progress and Achievements, details on how WMDA handles these requirements are provided.

2. Progress and Achievements

2.1 Data migration to secure cloud service

One of the key elements for successful implementation of a secure registry-to-registry communication system is a robust and resilient environment. This allows WMDA to facilitate registries exchanging communication messages through API developments and the EMDIS message exchange proxy. On the other side, WMDA needs to be sure that the envisioned environment is affordable and easy to maintain for the WMDA IT team. Cost control and maintainability are important drivers.

Principal business needs were defined as:

- Maintainability
- Availability
- (Data) Integrity
- Resilience
- Security

2.1.1 Former ICT landscape

The WMDA ICT infrastructure consist of a combination of hosted applications, SaaS applications, locally installed software (for instance at Steiner Ltd) and an Office365 environment via Microsoft Remote Desktop Protocol. These environments are mostly stand alone and not integrated, requiring manual effort to keep them in line. They are organically grown based on individual needs where integration, maintainability and total cost of ownership are questionable.

There were 16 virtual servers defined with a total 196 CPU and 651 GB memory. Maintenance was contracted but the 16 core machines couldn't be replaced within a 2-hour window period. It would've required 24 to 48 hours to replace, which would have impacted a substantial part of the applications. The theoretical availability was less than 99.5%. The IP connectivity was insufficient for data upload-function and caused waiting situations. Furthermore, the Optimatch rematch function is running once a day (night) and consumes CPU (100%). Monitoring and maintenance of the environment was done by the Dutch company, Damecon.

2.1.2 New developments

With the implementation of a secure registry-to-registry communication system through the use of APIs and a Proxy, the ICT solution would require different maintenance than was in place. With the API's, (near)real-time processing becomes possible. This imposes some additional requirements to the ICT infrastructure. Should API services become (temporarily) unavailable, registry systems would need to take care of error handling and reprocessing. The EMDIS proxy is realised in the Microsoft Azure environment using Function Apps (written in .NET Core). New developments provide the opportunity to distribute the web services in different geographic areas providing better response times and having a more robust environment capable of supporting a continuous delivery approach. The function applications are already part of that new cloud native way of working. Other API's and applications need to be restructured to be used that way. For instance, by applying NoSQL and Serverless principles.

2.1.3 Why APIs?

API interfaces are simple program-to-program interfaces taking care of secure and controlled data transactions without any business logic built into them. API's require low maintenance and light-weighted governance once implemented. Development is faster and at a lower cost. A more complex way of communication is using messages via an enterprise service bus (ESB) allowing for embedded business logic and programming but

requires strict governance and a skilled maintenance team (supplier dependency) and does not fit in with our vision. API's can easily be used in ESB environments.

2.1.4 Business requirements

Based on the above-described aspects, the business requirements for the cloud environment is defined as follow:

	Bronze	Silver	Gold
End-user-response times GUI	< 10 sec	< 5 sec	< 3 sec
Support window	08:30-17:30 CE(S)T	7:00-19:00 CE(S)T	24x7
Main maintenance window	08:00-12:00	08:00-10:00	00:00-06:00 (Sunday)
Notify maintenance window	5 days prior [1)]	5 days prior	5 days prior
Execute runbook test	No	Yes	Yes
Availability	> 99%	> 99,5%	> 99,9%
Incident response time	2 hours / next business day	2 hours / next business day	1 hour
Incident fix time	8 hours / next business day	4 hours / next business day	2 hours
Maximum data loss [2)]	4 hours	1 hour	None
Disaster recovery	No	No	Yes
Backup schedule	Daily 07:00 CE(S)T with retention 7 days & 4 weeks. Recovery test 1x annual		
SIEM [3)]	Yes, simple tooling for analysis and auditing		
Monitoring	HW, OS and application use		
Required certification	ISAE 3402, ISO 27001, ISO 9001		
Security levels	OWASP10 compliant, GDPR compliant		

[1)] Except for critical updates, these require alignment between parties

[2)] Snapshots will be created for Bronze and Silver and special tooling will be used for Gold. For Gold applies Recovery Point Object is last committed transaction

[3)] SIEM tooling is envisaged for Data Leakage and Data Loss protection

Moving the data to the cloud required upgrades of the current application landscape (PHP/Laravel and PostgreSQL) before migration could be done. For the Proxy and APIs there was already an Azure tenant present on a pay per use basis. A new infrastructure in the Azure cloud similar to the on-premise configuration was projected at a similar or higher cost (27-35 k€ annually based on a 3-year subscription, including storage and additional transaction costs), not taking a possible non-profit discount from Microsoft into account.

The servers in the cloud have an availability of 99,9% and would suffice for Silver and Bronze level. Gold would still require additional resources. The Optimatch servers however imposed a risk on costs and configuration due to its nature of processing.

Moving to the cloud on a "lift and shift" approach will lead to similar project costs as for enhancing the on-premise environment and a cost implication in the range of 15-25 k€. After migration to the cloud, further optimisation and innovation is possible by transferring the IaaS and PaaS environment into a serverless environment, reducing the effort needed for maintenance and monitoring significantly. A pay per use model for Search, Match & Connect usage could be derived from that.

2.1.5 Best practices

In order to make sure we deploy our new cloud-based environment according to the industry best practices regarding security, privacy and cost efficiency, we have requested offers from several Microsoft Azure certified partners.

These were:

- Arcus IT (https://www.arcusit.nl/)
- Sentia (https://sentia.com/nl/solutions/cloud-foundation/managed-landing-zones/)
- InSpark (https://www.inspark.nl/?gclid=Cj0KCQiA2af-BRDzARIsAIVQUOcafp2KyhzxvGI1EYzlZndbsARN8_KEAkQ-_oDSJftTsKDOxCpWvFAaAlb0EALw_wcB)
- Damecon (https://www.damecon.com/)

All companies were invited to give a demonstration. After the demonstration, they were all given a specified task that was a part of the project.

After careful evaluation of the contents and price of the offers made by these companies, we decided to go ahead with InSpark. We subsequently entered into a process where we agreed upon a high-level design which was according to their best practices regarding security, privacy and cost efficiency.

Experienced InSpark consultants were used to help us set up this environment and perform the necessary knowledge transfer.

2.1.6 Challenges encountered during migration

Initially, the process of adapting the on-premise applications to run efficiently in a cloud environment took more effort than expected. This was mainly due to:

- The inexperience of the WMDA employees regarding Azure infrastructure deployment. In order to overcome this challenge, we requested more help from InSpark engineers. They helped us finish the process within the time constraints and made sure the responsible WMDA employees had the necessary knowledge.
- Changes that needed to be made for the applications in the way scheduled jobs run in a virtual machine versus in an Azure-based web application.
- Code that needed to be rewritten to make use of the better scaling abilities of Azure. This led to a more efficient application which in turn led to search results becoming available faster for the search coordinators looking for the best stem cell product for their patient.
- The server running the Optimatch service couldn't be adapted for efficient cloud use, because it runs software from a member organisation. This software requires all components to be installed on one virtual machine, including the database. It was also mainly written in a language which cannot be run efficiently in a cloud environment as a microservice. We therefore had to perform a "lift and shift" of the software onto an Azure virtual machine which had similar specifications compared to the on-premise environment it was running on before.
- Due to the high demands regarding CPU clock speed we needed to make use of a special "high performance compute" virtual machine for the Optimatch service. The direct costs of hosting this solution went from about €750 per month to €1500 per month. We decided to do this because it enabled us to completely stop using the on-premise environment. Keeping Optimatch on-premise would have meant we still would have needed on-premise firewalls, switches and various other fixed-

costs infrastructure available in the on-premise environment. Because these fixed costs are about € 1000 per month, this made it more cost efficient to run all applications in the cloud instead of keeping Optimatch in the on-premise environment.

2.1.7 Outcome

Migration was started in March 2020 and is expected to be finished by mid-January 2021. It involves three WMDA employees and several InSpark consultants with different expertise sets. In total we migrated 10 applications. Some processes are already running more efficiently than in the on-premise situation. This was measured by the performance achieved for the same amount of costs. For example, we are roughly spending the same amount of resources on our Search application whilst we are running a much more flexible environment with increased uptime and increased peak performance. Furthermore, because deployments are much more flexible in a cloud environment such as Azure, future developments are expected to be quicker. This will bring a better and more efficient experience to our end-users.
Should the need ever arise to drastically decrease the running costs of our current cloud infrastructure, WMDA will be able to do so with very little effort. This will unfortunately reduce performance and significantly extended development cycles, therefore scaling down infrastructure should be critically evaluated and agreed upon by member organisations. It is important to note that the option of scaling down to preserve ICT expenditure was not possible with the on-premise solution without compromising the integrity of the global database.

2.2 Search API

The Patient API was launched in June 2019 which aimed at reducing time, effort and risk of error in creating a donor match list for search coordinators. The API allows Search Coordinators to automatically:

- Add new patients to the Search & Match Service through a registry's system.
- Update existing patient details in the Search & Match Service through a registry's system.
- Update the patient status in the Search & Match Service through a registry's system.

As a natural progression from the workflow facilitated by the Patient API, development of the Search API proceeded that would allow Search Coordinators to automatically:

- Initiate a donor search in the Search & Match Service.
- Receive automated notifications when new search results are available.
- See the results of each international donor and CBU search through a registry's system.
- View a list of all searches performed for a patient through a registry's system.
- Store or re-use search criteria (profiles).
- Define user or transplant centre preferences.

WMDA developed a set of technical standards – fully aligned to EMDIS semantics – and then built and/or sourced existing solutions to communicate seamlessly and securely from internal systems to the Search & Match Service. These technical standards are offered through APIs that allow real-time uploading and downloading of data. The Search API is backward compatible and GDPR compliant.

2.2.1 Alternative Algorithms

Historically, the Search & Match Service uses the Optimatch matching algorithm which provides probability matching using haplotype frequencies calculated using the entire global donor and CBU database as a dataset. Unfortunately, due to licencing constraints, the Optimatch algorithm could not be implemented into the Search API and alternative matching algorithms had to be investigated.

Algorithms from two large member organisations are considered:

- **ATLAS – Anthony Nolan**
  In 2020, Anthony Nolan launched a brand-new search algorithm for internal use, developed in collaboration with Softwire. The aim was to build a world-class search algorithm, incorporating the latest research in HLA matching, and leveraging the power and flexibility of cloud computing. Project ATLAS is a continuation of that work: enhancing the algorithm to make it suitable for the widest possible audience, for the benefit of the global community.

- **HAP-E Search – DKMS**
  The HAP-E Search algorithm has been in use in the DKMS internal donor search system since 2011 and was further optimized in 2018 by adding the ability to perform genotype recalculations (reference: "Urban, C., Schmidt, A. H., & Hofmann, J. A. (2020). Hap-E Search 2.0: improving the performance of a probabilistic donor-recipient matching algorithm based on haplotype frequencies. Frontiers in medicine, 7, 32."). This reinforces confidence and validity in its calculations as they have been verified repeatedly. However, development is required to scale it up to make it robust and accurate when applied to the much larger and more diverse global donor data pool.

Please see Appendix 1 for a breakdown of the algorithm requirements as they pertain to the WMDA Search & Match Service.

2.2.2 Side loading

Currently most information displayed on the WMDA Search & Match service regarding donors and CBUs come from Optimatch. Every night most donor and CBU information is imported from the central WMDA database, that has the complete donor and CBU dataset, to Optimatch.

This has several downsides:

- The information displayed can be up to 24 hours old. This can be especially relevant for status changes or additional or better HLA information becoming available.
- Some information is not sent by Optimatch to WMDA Search & Match with the donor or CBU search results or the full reports. This means that some information cannot be sent to the end user even if the WMDA has that information.
- When new fields are used by WMDA, Optimatch would need to be adapted in order to handle it. Most of the time these fields are irrelevant for matching, but if Optimatch is not changed, the information cannot become available to the end user. This leads to unnecessary work and delays in making this data available.
- Extra processing power is needed in order to supply all this extra information to WMDA Search & Match. This is not very efficient. It would be much more efficient if the matching engine handled only the information that is directly relevant for matching.

The only information needed by any matching engine regarding the donor and CBU data that is relevant for matching is:

  - An identifier known to WMDA
  - HLA typing
  - Ethnicity. This is needed to help impute probable actual HLA type from the ambiguous typing supplied.

- Original information source. (registry that has supplied the donor or CBU). This is needed to help impute probable HLA type from the ambiguous typing supplied.

So, in order to be as flexible and independent from matching engines as possible, sideloading is essential.

Before sideloading:

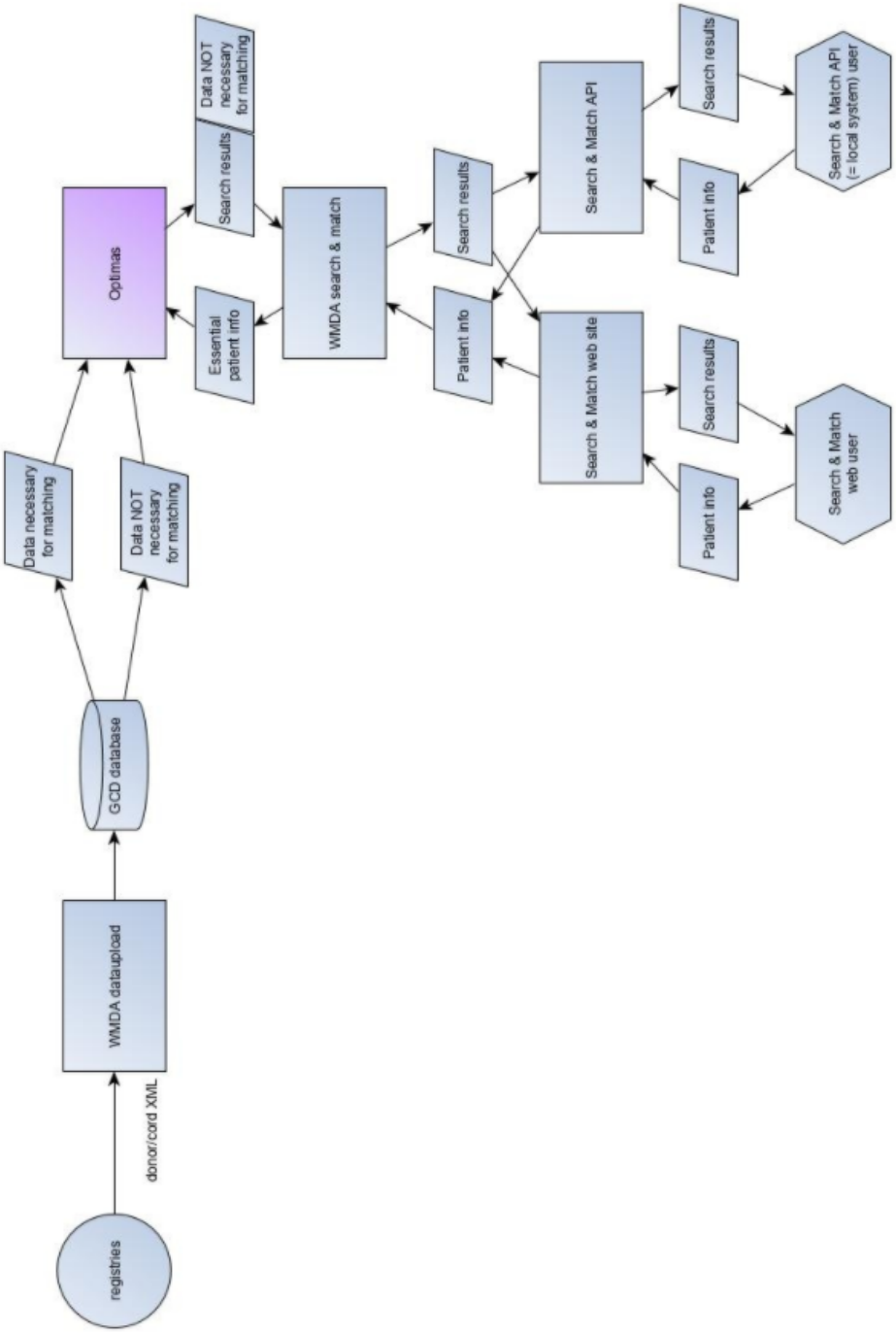


Figure 1: Flow and presentation of donor and CBU data in the absence of sideloading

With sideloading:

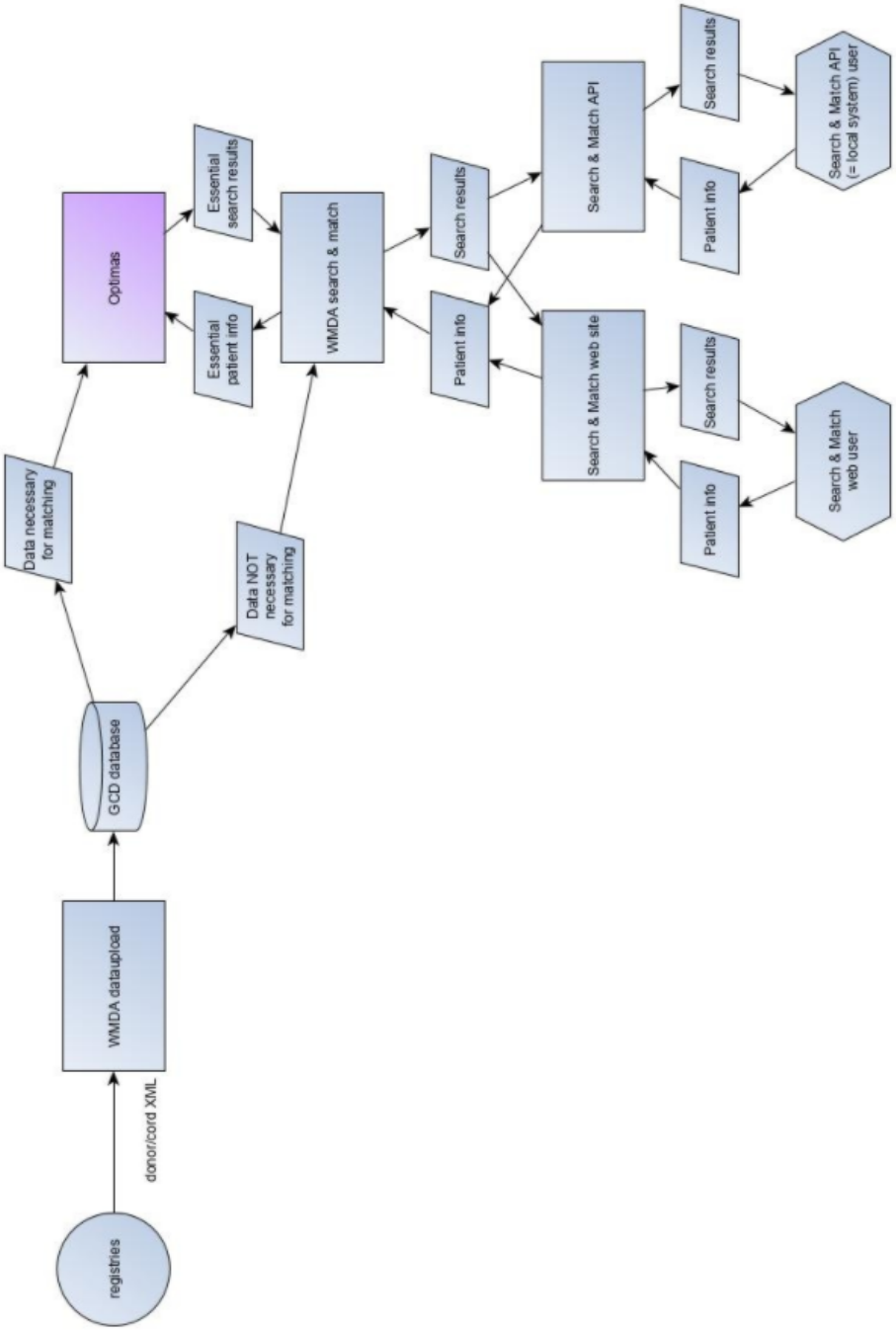


Figure 2: Flow and presentation of donor and CBU data following the addition of sideloading

With sideloading and additional matching engine:
Note: Future version of the WMDA Search & Match website will be a single page application (SPA) and work through the API instead of directly to Search & Match.

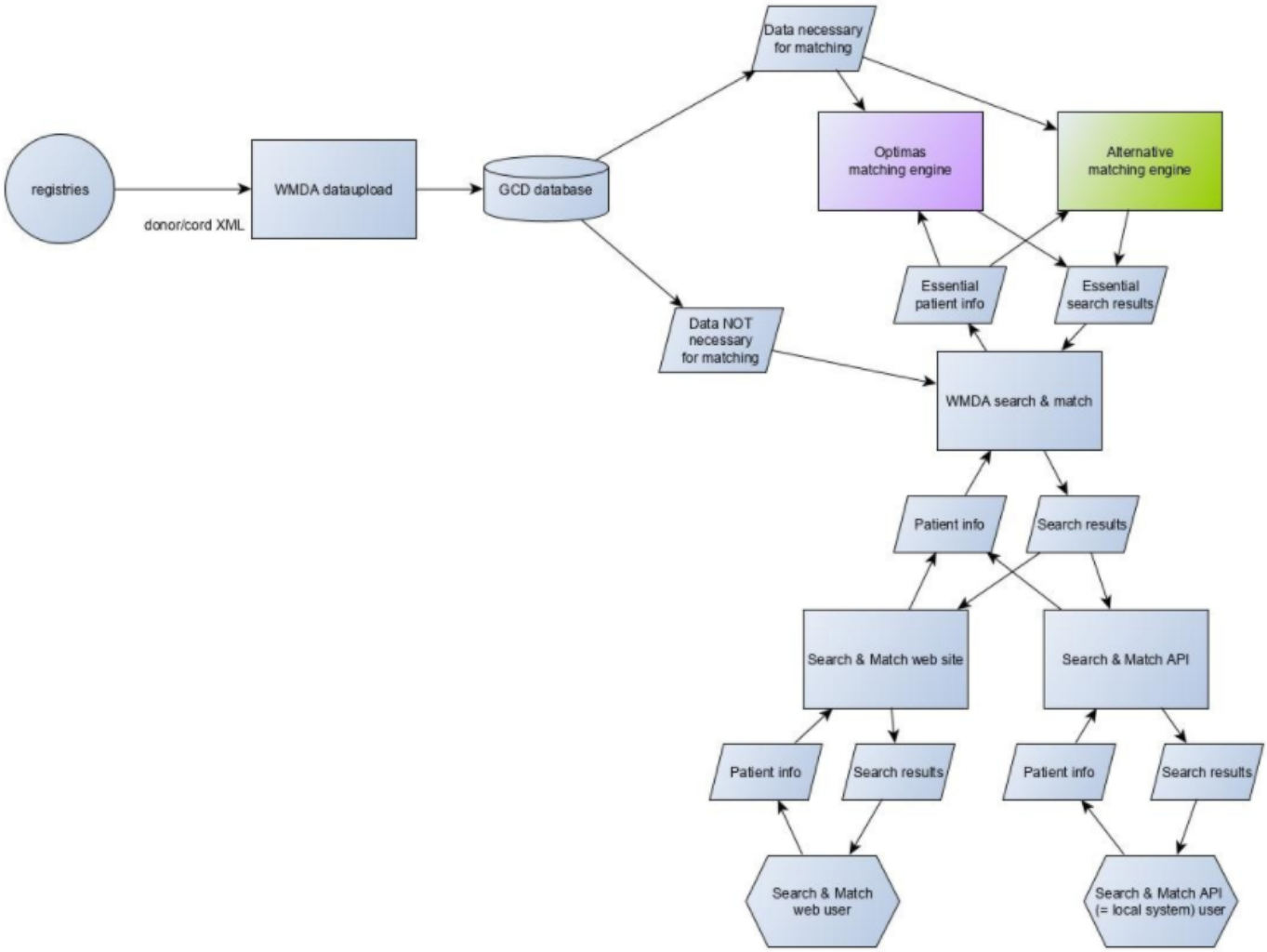


Figure 3: Flow and presentation of donor and CBU data following the addition of sideloading and an additional matching engine

Please see Appendix 2 for a breakdown of the loading requirements as they pertain to the WMDA Search & Match Service.

2.3 Connect API

The Connects API is a messaging system that connects registries to one another and aims to improve patient outcomes by reducing the time, complexity and risk involved in finding the best available stem cell source. This will be achieved by creating an integration between systems that allow donor health and availability requests, extended HLA and HLA verification typing requests, donor infectious disease marker requests, donor workup requests and CBU shipment requests in a secure way.

2.3.1 Approach to deliver the goal – EMDIS Proxy

WMDA will develop a single Search, Match & Connect data exchange hub (Proxy). This data hub will only validate the data exchange between registries. To serve all organisations the data exchange hub will accommodate various data formats, including EMDIS. The Proxy will enable organisations to use their internal system as their single 'front end' with all messages and communications between parties being handled securely by the data exchange hub. Storage will be handled in a GDPR compliant way.

A key aspect of our delivery will be sourcing from relevant partners (or building anew) to create the capability to convert traditional EMDIS messages to stand-alone message packets, which can be routed to non-EMDIS and EMDIS registries. The EMDIS registries can work through the EMDIS protocol or move to an API. The non-EMDIS organisations can choose to work through an API or through a secure webpage. The API allows that registries to define their own business rules and the freedom to choose which other WMDA member organisations they want to connect with.

With the implementation of one single connection, communication to any registry is possible regardless if it is an EMDIS registry or not. The connection will translate the message into the right format for the receiver. This way registries do not have to setup and maintain multiple point-to-point connections, thus reducing complexity. It will reduce the workload of a Search Coordinator as only one way of working is needed to retrieve information. By using API's, the registry systems directly receive the results from Connect. In case of error situation, the registry system will be the controlling part and receives an error notice. The WMDA only provides a (stateless) translation mechanism which can be used by the registry who will remain responsible. The API's will run in the widely used available cloud infrastructure (Microsoft Azure) which has high availability and has built-in redundancy, reducing the risk of unavailability to almost zero.

Core requirements:

- Setup EMDIS Communication System (ECS) and WMDA mailbox
  - Public keys for all registries
  - Sequence number initialization
- Setup a proxy service
  - Infrastructure and deployment
  - Matrix of compatibility
  - Logic to receive and parse messages
  - Logic to decide if a message can be sent and sending them on
- Documentation
  - Devise a clear plan to allow registries to migrate to the proxy
  - Ensure the technical feasibility of seamless migration
  - Create a comprehensive, user-friendly migration guide
- Performance
  - Evaluate our anticipated load
  - Plan for cost-effective future scalability

Added value features:

- Message integrity checks
  - Additional validation of received messages (e.g., Does the sending hub match the sending email?)
- User interface

- Make adding new registries easier and quicker
- User-driven configuration of “matrix of compatibility”
- Allow configuration by business users

- Auditing
  - Non-ECS auditing of sequence numbers to aid debugging and tracing of messages
- Statistics & reporting
  - Management information reporting on the use of the system

Architecture:

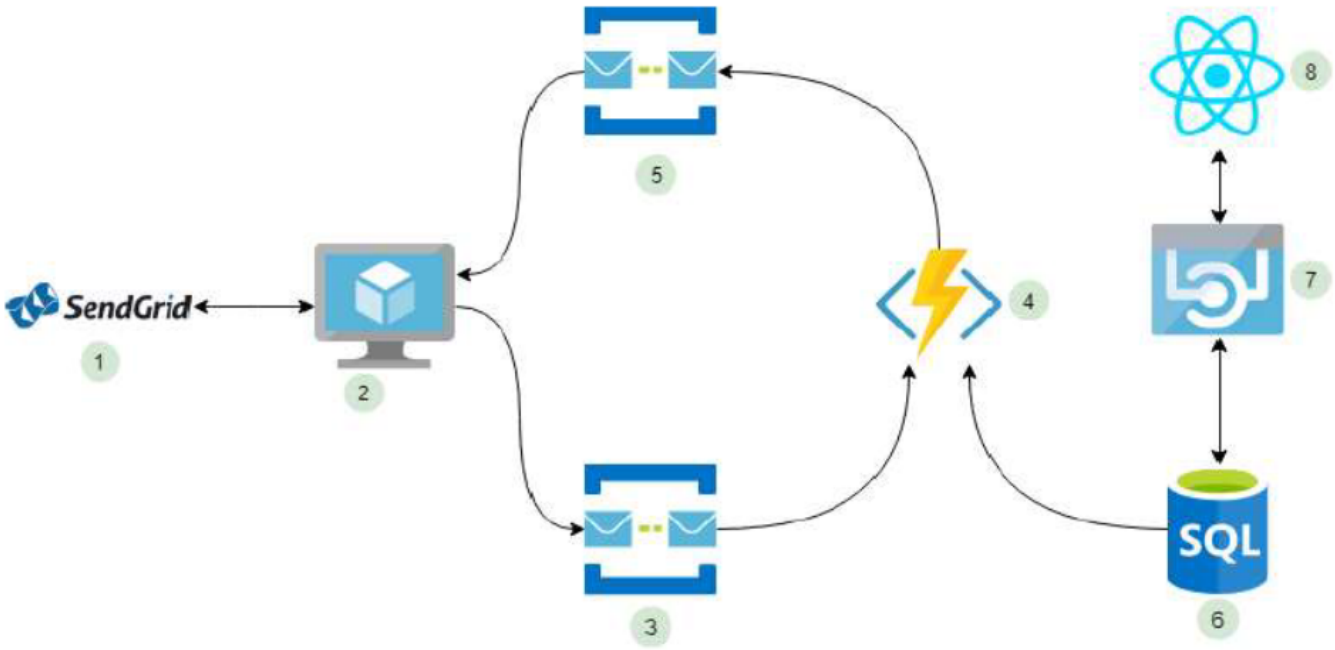


Figure 4: Technical architecture of the EMDIS Proxy

1. Transactional email provider to act as the “EMDIS mailbox” for the proxy
2. Virtual machine running an existing version of ECS. Handles encryption/decryption and sequencing of messages
3. Azure service bus – incoming messages waiting to be processed
4. Azure Function to parse the messages and decide whether they can be sent on
5. Azure service bus – outgoing messages waiting to be processed
6. Azure SQL database stores configuration information for the proxy (e.g., Communication rules between registries)
7. (added value) API to allow configuration to be altered
8. (added value) UI to allow configuration to be altered

2.3.2 User Engagement – Work-up requests

While the existing EMDIS communication platform does not facilitate the transmission of donor work-up requests from one registry to another, the vision of Connect was to include this feature. It is generally understood that the donor work-up process is so complex and varied amongst registries that establishing a single workflow that could be communicated electronically would not be feasible. To determine whether this is

truly the case, two face-to-face workshops were planned. One in Madrid, Spain with Transplant Centre Coordinators during the annual EBMT conference (March 2020) and another in Quebec City, Canada with registry Harvest Coordinators during the WMDA/IDRC conference (June 2020). Unfortunately, both conferences were cancelled due to the pandemic and an alternative strategy had to be devised to gather the information needed. The following plan was set in motion:

User engagement plan in lieu of EBMT/WMDA/IDRC working group sessions

1. Prepare set of discussion-guiding questions
    a. Donor work-up
    b. CBU request
2. Identify shortlist of registries to approach
3. Setup "one-on-one" Zoom meetings with relevant stakeholders
4. Collate data from discussions
5. Present initial findings to wider community for discussion
6. Implement consensus into Connect API

Interviews Performed:

1. 08 Apr 2020: South African Bone Marrow Registry (SABMR)
2. 08 Apr 2020: The Finnish Stem Cell Registry - Finland
3. 29 Apr 2020: National Marrow Donor Program (NMDP) – United States of America
4. 22 May 2020: Matchis – The Netherlands
5. 29 May 2020: Deutsche Knochenmark Spenderdatei (DKMS) – India & Chile
6. 03 Jul 2020: Bone marrow Donor Programme (BMDP) - Singapore
7. 20 Jul 2020: Australian Bone Marrow Donor Registry (ABMDR)
8. 05 Aug 2020: REDOME - Brazil
9. 14 Aug 2020: Canadian Blood Service
10. 14 Sep 2020: Anthony Nolan – United Kingdom

From the interviews the following pain points were identified:

- Registry to transplant centre (TC) communication plays a critical role and, in most cases, this is still a manual process of document exchange.
- Based on national regulations in the respective countries, a wet signature (as opposed to a digital signature) from the requesting transplant physician is required on the forms.
- Due to the varying prevalence of infectious diseases around the world, not all registries perform the same Infectious Disease Marker (IDM) testing on requested donors during the medical examination and workup process.
- Multiple organizations, service providers and individuals are involved in the process of collecting stem cells from a donor: Transplant Centre, Collection Centre, requesting Registry, donor Registry, donor, patient, processing laboratories, courier services. All coordinating a single, time sensitive event by communicating via various platforms while maintaining both patient and donor confidentiality.
- Registries in non-EU countries may not be GDPR compliant.

While the interviews were conducted with a wide variety of registries spanning over many continents and ranging in size from thousands of donors to millions of donors, the possibility remains that some information is lacking from the investigations done. However, based on the information gathered it seems plausible that a standardized workflow could be developed based on existing WMDA forms and accreditation standards that

meet the required timeframe and confidentially safeguards to ensure safe collection, processing, transport and infusion of stem cell products. Ideally an open discussion needs to take place with key stakeholders to iron out any remaining issues.

Please see Appendix 3 for the discussion-guiding questions that were asked during the scheduled meetings.

2.3.3 Integration of EMDIS into WMDA

The WMDA's 2018 Strategy established a 'Search, Match and Connect' (SMC) pillar that aims to facilitate the best possible match between donors and patients by optimising the global search platform. Its ambition is to provide faster access to donors, to make the best quality donor related data available to members, and to enable all members to efficiently search and connect. Since 2018, new capabilities have been introduced through the implementation of APIs that provide users with secure and controlled transactions between their own and other systems, as well as the EMDIS Proxy. The aim of this approach is to provide seamless communication between EMDIS and non-EMDIS registries, with less overhead on setup and maintenance, and to provide a 'translation' layer between different versions of the EMDIS specification.
In 2019, the EMDIS 4.0 Whitepaper - informed by feedback from EMDIS users - signalled an intention to revamp the EMDIS infrastructure, setting the goals to provide modern, commonly accepted technology and greater functionality, that will enable faster communication between EMDIS registries. Acknowledging the shared ambition, complementary goals and opportunities for synergy the EMDIS Steering Group proposed the 'integration' of EMDIS into the WMDA. This proposition builds upon a long-standing shared objective to harmonise and align the two initiatives, demonstrated by efforts in recent months to ensure reciprocal representation on oversight/steering committees and user and technical groups. Integration would also mitigate the risk that the initiatives are perceived to be in competition or have divergent aspirations and would formalise the collaboration and commonality that characterise the EMDIS and WMDA communities.

On 27 October 2020 the EMDIS community met virtually and by democratic vote approved, in principal, the integration of EMDIS into WMDA on the condition that the EMDIS Chairs provide a clear integration delivery plan by April 2021 that includes the technical blueprint of the combined EMDIS 4.0 and WMDA Connect projects.

It was agreed to commission the development of a document that will serve as a framework for the proposed 'integration.' This was a collaborative exercise to appraise the rationale and business case for the potential change, with the output reviewed and approved by the EMDIS community ahead of its endorsement by the WMDA Board.

- **Development approach**

A 'Writing Group' was convened comprising representatives of WMDA and EMDIS:

  - Lydia Foeken, Executive Director WMDA
  - Hans-Peter Eberhard, SMC Bioinformatics Committee Chair (ZKRD)
  - David Steiner, EMDIS Technical Group Chair (Steiner Ltd.)
  - Simona Pollichieni, EMDIS User Group Vice Chair (IBMDR)
  - Matti Korhonen, EMDIS 4.0 Steering Committee Chair, SMC board committee member (Finnish Stem Cell Registry and Blood Service)
  - Felix Bussman, EMDIS 4.0 Steering Committee (Swiss Blood Service)
  - Matt Prestegaard (NMDP - Be The Match; CIBMTR)
  - Hugh Allen (Anthony Nolan; SMC)

- Alice Cheatle (Anthony Nolan - providing secretariat support, e.g. coordination, planning, notes and actions etc.)

The Group led the development of the framework document. Technical support and guidance were provided by Danny Attias (Anthony Nolan) and Mark Melchers (WMDA).

- **Engagement and consultation**

The WMDA and EMDIS communities have a strong tradition of democratic accountability and inclusive decision-making. The development of the framework document reflects this ethos, ensuring diverse members and users have opportunities to contribute to the development of options, to feedback on proposals and to decide whether the integration is viable and desirable. The composition of the core Writing Group reflects this intent, with members drawn from both the WMDA and EMDIS communities and representing the technical and user perspectives. Wherever possible, options and recommendations were developed on the basis of consensus, and any areas of divergence were disseminated for negotiation and decision-making by the broader WMDA and EMDIS communities and committees.

- **Content**

The framework provides an exposition of the case for integration, along with options and proposals for how this may be achieved in practice. It includes as an annex an overview of the technical blueprint, setting out options for technical integration, which will act as a foundation for future joint decision-making and planning.

The framework addresses the following topics and questions:

- A shared vision
  - What is the overarching ambition?
  - What will be different and better in the future?
- Benefits
  - What are the problems to be solved and the opportunities to be harnessed?
  - What outcomes will be achieved?
  - How will these benefit EMDIS users and WMDA members, and ultimately how will they benefit patients and donors?
  - What can be achieved by 'coming together' that can't be achieved in the status quo?
- Principles and values
  - What are the principles and values that will underpin the integrated activity?
- Approach
  - What are the options and recommendations for how 'integration' will manifest in practice?
  - What are the cultural and behavioural aspects of integration and how can these be addressed?
- Governance
  - What are structures, roles and responsibilities for setting strategic direction, decision-making, prioritisation and resource deployment?
  - What 'oversight' structures and mechanisms need to be adjusted or established, e.g., steering groups and committees?
  - What structures and mechanisms need to be adjusted or established to ensure robust user/member involvement and the provision of technical expertise?
  - Who is accountable for delivery, and how will delivery - and the realization of benefits - be monitored and evaluated?

- What is the legal basis / framework for this integration, e.g., contracts and ownership?
- Finances
  - What financial resources will be pooled/shared and what will be retained?
  - What are the options for user/member fees?
  - What is the budget for the integrated initiative?
  - How will development work be funded, i.e., what are the sources of funds?
- Risks
  - What are the risks of the status quo?
  - What might prevent or hinder the proposed integration?
  - What are the headline risks to the achievement of desired benefits and outcomes?
  - How can risks be mitigated and what contingencies should be put in place?
- Issues
  - What are the remaining areas of divergence and disagreement?
  - What options are there to converge and agree, and what are the pros and cons of these?
  - What decisions need to be made and by whom?
- Outline integrated delivery plan and technical blueprint
  - What is the 'integration' timeline and activity?
  - What needs to change in the EMDIS 4.0 and SMC delivery plans?
  - What is the appropriate prioritisation and correct sequencing of planned activity?
  - Who is leading and contributing to delivery?

Please see Appendix 4 for the indicative governance, financial arrangements and draft technical blueprint of this proposed integration.

2.4 Security and Privacy

The WMDA's Security Privacy Committee encourages and enables the WMDA and its members in managing information security and privacy matters as a global business risk. With proper risk management, WMDA can ensure the long-term sustainability of global data sharing that is necessary to achieve its mission.

The WMDA Security and Privacy Committee (WMDA SPC) achieves this by:

- Establishing minimum security and privacy standards that are required for WMDA membership.
- Supporting the WMDA Accreditation process to ensure these standards are enforced.
- Providing regular education and training to members at semi-annual meetings and with publications.
- Informing members on emerging risks and regulations that may threaten the WMDA mission.
- Providing practical guidance specifically crafted for small- and mid-sized stem cell registries with an international supply chain and data profile.

2.4.1 Current projects

- **Incident Ledger on WMDA Share.**
  WMDA SPC created, maintained and populated a ledger of data privacy and security incidents encountered by WMDA members. These incidents are published on WMDA Share. All aspects of any incident are anonymized, including WMDA member identifying information. These real incidents are used as educational materials (lessons learned) to improve the overall security of the WMDA network.

  No incidents have been reported since the launch of this facility.
- **Peer Security Assessment / Accreditation.**

WMDA SPC established a simple, scalable and repeatable assessment process to perform registry-to-registry peer risk assessments of registry applications. One security, privacy, or IT representative from WMDA performs a security and privacy assessment on behalf of the entire WMDA network. Basic information on the results, and any material corrective actions, are published on WMDA Share. Members may rely on these results to comply with their own internal and external risk assessment requirements. Large registries and the WMDA are the early adopters of this new process.

This process was piloted between NMDP and ZKRD. The WMDA's systems were also subjected to the Security and Privacy Committee's assessment and was found to be acceptable.

Please see Appendix 5 for a list of registry application security essentials and the assessment questionnaire.

In Chapter 3. Project plan for 2021, a clear roadmap on the future developments and improvements to guide efforts in 2021 is presented.

3. Project plan for 2021

3.1 Search API

In order to launch the Search API into production and make the source code available to registries to implement into their internal systems, the alternative matching algorithms (HAP-E & ATLAS) need to be integrated and tested in the newly established cloud environment (Microsoft Azure). Automated notifications (electronic messages) to relay information about the delivery and receipt of registry-to-registry communication will also be developed and implemented to assist with troubleshooting and provide a reliable audit trail of interactions between organisations.

Upcoming – 2021

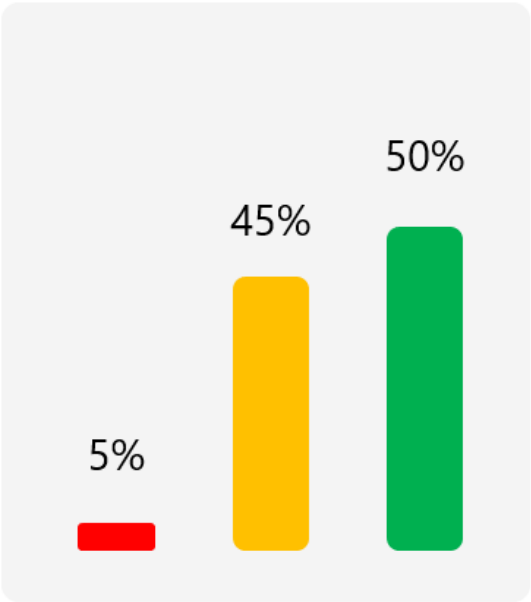
Notifications
Testing of alternative algorithms
Monitoring cloud environment
Launch Search API

Complete – 2020

Alternative matching algorithms
Cloud migration

Complete – 2019/20

Start/update a patient search
Retrieve patient search summary
Retrieve search results
Retrieve full detailed report for donor & CBU searches



3.2 EMDIS-Connect

In 2021 the APIs and EMDIS 4.0 will be extended to support each other, provide additional processes, status updates and auto-complete forms. WMDA will endeavour to implement a secure registry-to-registry communication solution based on the original scope of the Connect API in collaboration with the EMDIS Technical User Group and their vision of EMDIS 4.0. The integrated solution (EMDIS-Connect) will be delivered step-by-step ('agile' delivery) and will enable registries to connect their internal system to the global community allowing Search Coordinators to:

- Send and receive messages between non-EMDIS and EMDIS users based on EMDIS protocols.
- Perform donor availability checks, subject to data quality dependencies.
- Conduct donor health and availability requests, extended HLA and HLA verification typing requests, donor infectious disease marker requests, donor workup requests and CBU shipment requests.
- Receive automated acknowledgement, receipt and status notifications.

From an IT management point-of-view the following core principles are safeguarded:

- Low disruption to existing systems and processes and avoidance of 'forced systems migration'.
- Ease of implementation to establish connections to all registries.
- Low maintenance and overhead for registries.

- Security and data protection 'built in' to user authentication and message handling solutions.
- Single data model based on EMDIS semantics and used by all registries.
- Data quality and governance steered by WMDA and supported by the Data Dictionary Working Group.
- Improved transparency and reporting of data flows.
- Centralised notification and support for process and business rule related issues (e.g., invoicing problems)

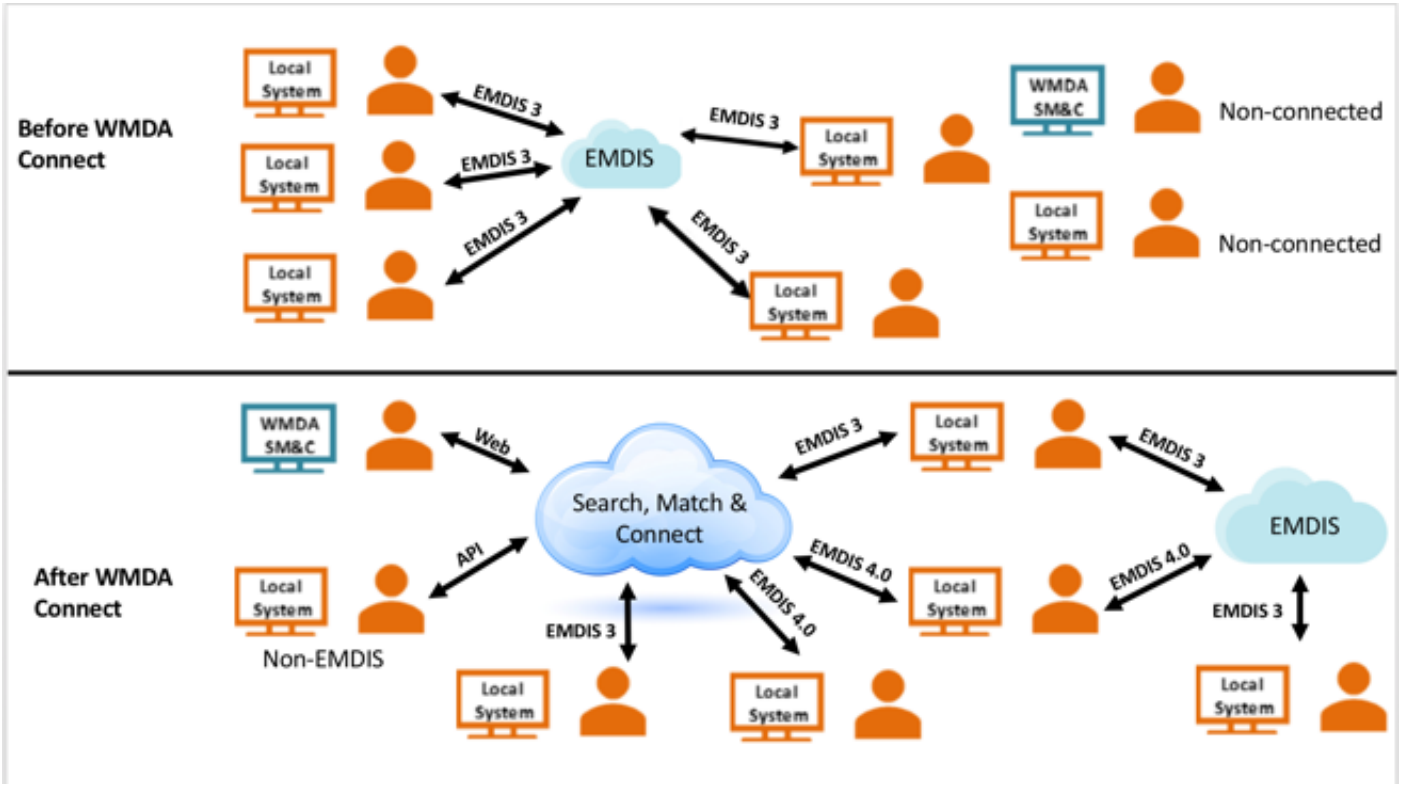


Figure 5: Impact on registry-to-registry communication following implementation of an integrated communication solution

The WMDA's vision will be achieved by realising the following goals:

- One single Search, Match & Connect data exchange hub (described as WMDA Connect in figure 1)
  - Facilitate effective and efficient communication between registries.
  - Facilitating registries by offering one single connection point to connect to, for communication to all registries.
  - Translation of messages in different data formats including EMDIS.
  - Based on EMDIS data semantics; and keep an eye on development in HL7/FHIR.

- Implementation of APIs to Search, Match & Connect for real-time data uploading downloading (described as API in figure 1)
  - Search coordinators can obtain the same information in their local system through an API as they can obtain when they register a search online through the web application.
  - Development of a secure, robust, simple and scalable API.
  - Non-disruptive, backward compatible connector, that allows registries to continue to use their current operational registry software application.
  - Compliance with European data regulations (GDPR), reducing the need to create a data hub or to have a

downloaded copy of the dataset.

- Extended functionality connectors with respect to EMDIS (described as API in figure 1)
  - The connector provides the possibility to exchange more data including documents.
  - The connector supports more processes (e.g., verification and extended typing, infectious disease marker
    testing, work-up requests)
  - The connector provides status updates, e.g., request received, request read, etc.
  - The connector provides automatically filled-in forms.

- Maintaining master data on behalf of registries (described as API in figure 1)
  - The connector will allow registries to define their preferences to decide how to collaborate with their international partners.

- Improved functionality (described as API in figure 1)
  - Storing/re-use of search criteria (profiles).
  - Define user/transplant centre preferences.
  - Quality monitoring.

- Use of modern technology
  - Low maintenance, non-specialized ICT team available once implemented.
  - Widely used technologies in-line with standard industry practice, preferably open source.
  - Implemented via an agile framework, step-by-step delivery to the WMDA member registries.
  - Cloud native approach allowing for distributed processing, improved resilience and optimized performance.
  - Open, allowing for inclusion of community developments (added functionality).
  - Based on “secure by design” and “privacy by default” with full traceability of performed actions.
  - Use of automatic quality checks to reduce test effort and improve quality of delivery.

- Improved availability of Search, Match & Connect
  - Improved hosting environment: Connect requires high availability across the world and a scalable
    environment which is maintained 24x7; business requirements will be developed in collaboration with
    the Search, Match & Connect Steering Committee.
  - Continuous delivery approach for functional enhancements.

By combining the existing EMDIS proxy with the EMDIS-Connect communication solution, secure registry-to-registry communication will be available to all WMDA member registries and will pave the way for complete integration of EMDIS into the WMDA.

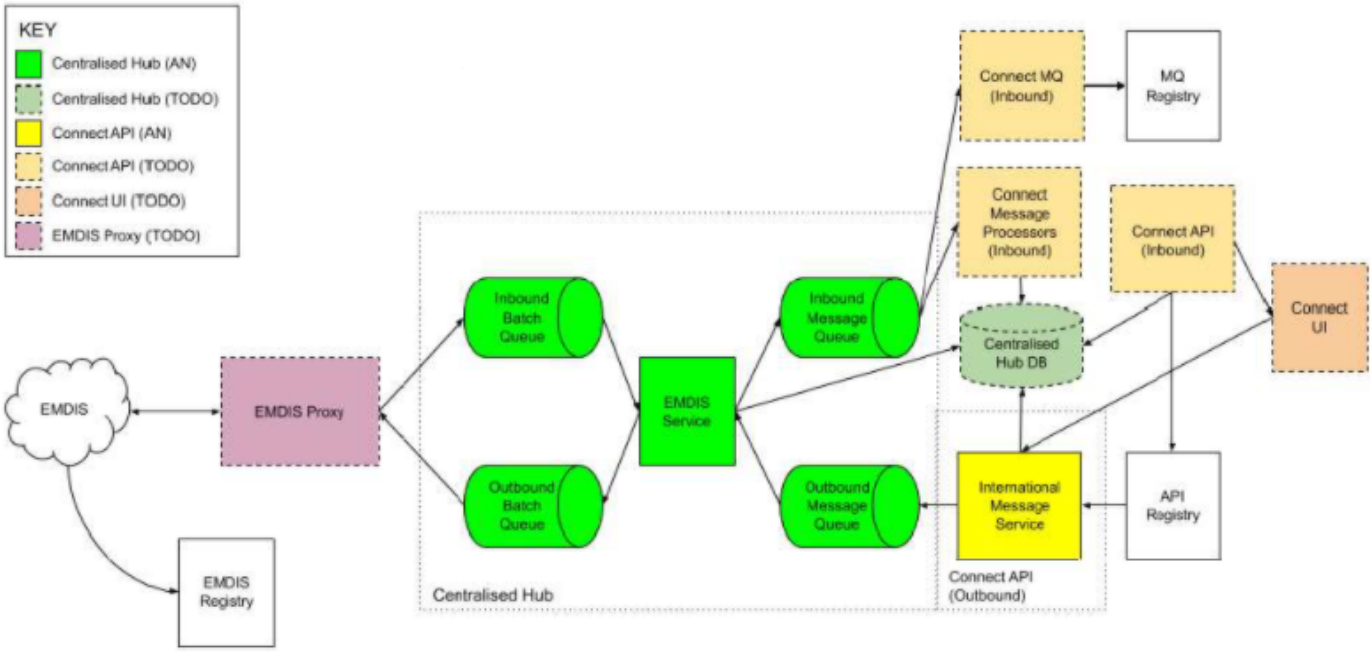


Figure 6: Proposed technical overview of communication flow between EMDIS & non-EMDIS registries

3.3 Security & Privacy

EMDIS Security and Privacy / Global Erasure Request.

WMDA Security and Privacy Committee reviewed, defined and documented technical security and privacy specifications for the future enhancement of EMDIS. The updates would formally incorporate privacy-by-design principles in addition to modern security specifications (encryption, authentication, etc). The current EMDIS specifications share unnecessary privacy data (e.g., date of birth) that make it difficult for members to meet global privacy obligations.

Appendix 1 – HAP-E and ATLAS Algorithm Requirements

	Category	Subcategory	Type	Title	Description	Mandatory?
1	Data Management	Data Import	Task	Transfer record_Ids to permanent ones	If all data was imported again, the new records should all be able to find a representative donor within the old records, so calculation time is low. Afterwards, the old records could be removed.	
2	Data management	Donor Import	Feature	Import consistency check	When a ddupdate file with updateMode "full" is imported, it should be checked against the existing donors in the database. Only deleted / missing / changed records should be updated.	Y
3	Databases	Database	Task	Dev / Staging database	Create new instance(s) for staging / DEV	Y
4	Search	6/6 Search	Task	Enable 6/6 search	To enable the 6/6 search, ABDR genotypes must be calculated for all donors.	N1
5	Search	Cord Blood	Feature	CB AB low DR high search	CB AB low DR high search -> exact requirements needed	N2
6	Search	Cord Blood	Feature	CB ABCDR high search	CB ABCDR high search is only a minor adaption to the donor 8/8 search	N1
7	Search	Cord Blood	Feature	CB down to 4/8	Search for more mismatches in CB searches (frequency calculation only down to n-2/n)	N2
8	Search	Delta Search	Feature	Use dd update id in delta searches	Adjust delta search to use ddupdate_id instead of timestamp	Y
9	Search	HLA data	Feature	Deprecated routine for WMDA data	Adopt the routine for new deprecated alleles to WMDA data -> replace donor typing in lager_hla_wmda and alle_spender if the old typing becomes deprecated	Y
10	Search	Match Probabilities	Feature	Adapt locus match probabilities	Adapt locus match probabilities - convert DKMS mm probabilities to match probabilities	Y
11	Search	Match Probabilities	Feature	No calculation for unknown haplotypes	Switch off the match probability calculation for donors / patients with unknown haplotypes and ambiguous typing	N1

12	Search	Match Probabilities	Feature	n-2/n probability also for n/n donors	n-2/n probability also for n/n donors	N2
13	Search	Search Results JSON	Feature	Include DPB1 TCE	Calculate DPB1 TCE match grade based on allele frequencies	Y
14	Search	Search Results JSON	Feature	Include MM Locus string	Determine position and kind (allele vs. antigen) of mismatches between donor and patient for all HLA loci with available typing results	Y
15	Search	Search Results JSON	Feature	Include NMDP match string	Include NMDP match string	Y
16	Test	Donors	Task	Match donors Testing	Compare Hap-E Search match donors to Optimatch (should be the same)	Y
17	Test	Match Probabilities	Task	Match probabilities Testing	Compare Hap-E Search match probabilities to Optimatch (should be comparable - explainable deviations)	Y
18	Test	Performance	Task	Performance Testing	Further performance tests under load comparable to Optimatch	Y
19	Test	Delta Search	Task	Delta search testing	Test that all changed donors are found in delta search	Y
20	Search	Match Probabilities	Feature	Homozygous mismatch counting	Include homozygous mismatch counting for adopted patient genotype calculation	N3
21	Data Management	Data Import	Task	Check correct import of files	Run import consistency check	Y
22	Test	HLA data	Task	Check correct HLA import		Y
23	Data Management	Data Import	Task	Run import & genotype calculation for all prod donors	Start with a "fresh" lager_hla_wmda and alle_spender table and calculate once the genotypes for all final productive donors	Y
25	Stability	Donor Import	Feature	Check import file	Make sure the input file is correct - no double entries etc. Skip records that have some kind of error	Y
26	Stability	Search	Feature	Check search request	Check that search_Request JSON is correct. Error when not supported options are selected	Y
27	Stability	Jobs	Feature	Robustness against Maintenance shutdowns	Realize when jobs were interrupted by a maintenance shutdown. Repeat / resume the stopped job automatically	Y

28	Data Management	Donor Import	Feature	Translate MACs to G-Code wert_ids when importing	If the imported MAC is identical to a G-Code, use wert_id of the G-Code instead of the MAC	N
29	Data Management	Haplotypes	Feature	Update haplotype frequencies	Enable the update of haplotype sets with recalculation of genotype information in the background	N
30	WMDA	Integration	Feature	Side loading		Y
31	Data Management	Integration	Feature	Client for Hap-E Search	Start Searches, Delta search handling, etc.	Y
32	Data Management	Donor Import	Feature	Automated Donor data uploads	Automated recognition of changed donors	Y
33	WMDA	Integration	Feature	GUI adaptions	Chose search engine, adopt to different output	Y
34	WMDA	Integration	Feature	Search API changes		N1
35	Test	Donors	Task	Mirror searches from Optimatch production in Hap-E Search		Y
36	Test	Donors	Task	Synchronize Hap-E Search Test system with Optimatch Staging	Import donors from staging to Hap-E Search and compare results	Y
37	Communication	Instruction	Task	Prepare How-To for User group		Y
38	Communication	Instruction	Task	Changes		Y
39	Test	Match Validation	Task	Perform WMDA Match Validation	Perform matching validation on database clone	Y
40	Test	User Acceptance	Task	User acceptance testing	Approval by members of the user group	Y
41	Documentation	Code	Task	Code documentation	Technical and user versions	N2
42	Legal	Contract	Task	Create long-term contract		Y

Appendix 2 – Sideloading Requirements for WMDA's Search & Match Service

Epic	User story	MoSCoW	Description
As a Search Coordinator I want to always see the latest non-HLA/Ethnicity data for a donor, cord or other stem cell product in the search results for a patient	As a search coordinator I want to always see the latest non-HLA/Ethnicity information in Donor Search results.	Must (matching engine 2)	Information should come directly from the WMDA "source of truth": GCD2 or an up-to-date cache.
			Should be performing same or better compared to current setup (time from start search to availability to end-user)
			Should also be up-to-date information when search results were retrieved from matching engine up to 24 hours ago. Nightly refresh should take care of nightly update, but during rest of day results should ALWAYS be up to date at time of showing to end-user.
	As a search coordinator I want to always see the latest non-HLA/Ethnicity information in CBU Search results.	Must (matching engine 2)	Assumed the above task for donor will include building reusable code that will be implemented also for CBU retrieval making this task easier to complete.
	As a search coordinator I want to always see the latest non-HLA/Ethnicity information in Donor full report.	Must (matching engine 2)	This will provide the basic Azure function API feature and SMC client interface that can be reused and extended
	As a search coordinator I want to always see the latest non-HLA/Ethnicity information in CBU full report.	Must (matching engine 2)	Assumed the above task for donor will include building reusable code that will be implemented also for CBU retrieval making this task easier to complete.
As a Product Owner I need new functionalities to be	As a Product Owner I need the sideloading to be performed in a cloud-	Should	This should ensure a high performance and low-cost solution.

created in a reliable and future-proof way	native way (e.g., using functions)		
	Scope for Azure Devops CI/CD	Should	This should ensure continuous deployment automation for the new features
	As a product owner I need unit tests to be created to test this functionality	Should	Preferably by having a parameter during retrieval. .env parameter could also work.
	As a product owner I need to be able to compare search results output between sideloaded and not sideloaded.		

Appendix 3 – Conversation Guiding Questions investigating Donor Workup Requests

1a

- "Talk me through the process of submitting a WU request for a donor from another registry":
  - When does a workup procedure start? How does it start?
  - Average period between VT & WU
  - Which forms are used?
  - Are forms completed by registry, requesting Dr or both?
  - How many donors in parallel?
  - Do you accept electronic signatures?
  - Preference: submit to known case manager/contact person or default recipient?
  - Generally, fax or email? Other method?
  - How long do you wait before first reminder?
  - Do you request any additional testing on donors during medical exam?
  - How often do you ask for simultaneous VT/WU?
  - How & when do you expect to receive the WU schedule?
  - How & when do you expect to receive donor clearance?
  - Do you have a preferred courier?
  - How & when do you expect to receive the final cell count?
  - Do you routinely provide post-TX patient follow-up? How do you communicate this?

- "How does the process of submitting a request for a subsequent donation differ from the above?"

- "Talk me through the process of receiving a WU request from another registry for one of your donors":
  - Which forms do you require?
  - Do you require the requesting Dr's signature?
  - Do you accept digital signatures?
  - Do you accept multiple donors in WU at the same time for a single patient?
  - Do you have a single point of contact for the requesting registry or do you communicate with them from a default/generic email account?
  - How do you communicate with the requesting registry? Fax, email, other?
  - How do you communicate donor availability with the requesting registry?
  - Which tests do you perform during the medical exam?
  - How & when do you report donor clearance?
  - Do you offer simultaneous VT/WU? How often do you perform these?
  - How do you communicate the WU schedule?
  - What courier recommendations do you provide?
  - What courier information do you require?
  - When do you require the courier information?
  - How and when do you communicate final cell counts?
  - Do you provide post-TX patient follow-up? How do you communicate this?

- "How does the process of receiving a request for a subsequent donation differ from the above?"

- "Did COVID-19 have a severe impact on the way you approach donor VT & WU?"
  - Were all the changes made to the process temporary or will some be made permanent?
  - What permanent changes have you made?

- How do they change the way you communicate with registries?

1b

- "Talk me through the process of requesting a CBU from another registry":
  - Do you give preference to accredited CBBs?
  - Initial contact with CBB
  - Which forms are used?
  - Are forms completed by registry, requesting Dr or both?
  - How many CBUs in paralleled?
  - Do you accept electronic signatures?
  - Preference: submit to known case manager/contact person or default recipient?
  - Generally, fax or email? Other method?
  - How long do you wait before first reminder?
  - Apart from VT, do you request any additional testing prior to shipment?
  - How do you expect to receive the CBU report and VT results?
  - What timeline from initial contact to shipment do you expect?
  - How & when do you expect to receive the transport information?
  - Do you have a preferred courier?
  - How do you return the shipper? What forms/communication is involved?
  - Do you routinely provide post-TX patient follow-up? How do you communicate this?

- "Talk me through the process of receiving a CBU request from another registry":
  - Which forms do you require?
  - Do you require the requesting Dr's signature?
  - Do you accept digital signatures?
  - How do you manage multiple CBU requests for a single patient?
  - Do you have a single point of contact for the requesting registry or do you communicate with them from a default/generic email account?
  - How do you communicate with the requesting registry? Fax, email, other?
  - How do you communicate CBU issues with the requesting registry?
  - Apart from VT, do you perform any additional testing prior to shipment?
  - How do you communicate the CBU report and VT results?
  - What timeline from initial request to shipment do you strive for?
  - How & when do you communicate the transport information?
  - Do you have a preferred courier?
  - How do you return the shipper? What forms/communication is involved?
  - Do you provide post-TX patient follow-up? How do you communicate this?

- "Did COVID-19 have a severe impact on the way you approach CBU requests and/or shipping?"
  - Were all the changes made to the process temporary or will some be made permanent?
  - What permanent changes have you made?
  - How do they change the way you communicate with registries?

Appendix 4 – Proposed Governance, Financials and Technical blueprint of EMDIS integration

Indicative governance, financial arrangements and draft technical blueprint of the proposed integration of EMDIS into the WMDA

Governance refers to the *way* we get things done. It sets out agreed mechanisms and structures for:

- Setting strategic direction, decision-making, prioritisation and the deployment of resources.
- Monitoring and oversight, so we can track whether we are doing and achieving what we set out to and can act quickly in response to changing circumstances and to get back on track when necessary.
- Involving, engaging and communicating with stakeholders - including users and members - so that their views, skills and knowledge determine, inform and contribute to design and delivery.
- Defining accountability, with clear roles and responsibilities.

Good governance helps to ensure accountability, transparency, responsiveness, stability, equity and inclusiveness, empowerment, and broad-based participation. Over time, the EMDIS and WMDA communities have developed their own governance principles, processes and structures that reflect their overarching principles and values and inform their ways-of-working. The effective integration of these is a vital but complex component of the proposal to integrate the EMDIS community into the WMDA.

This Framework provides an overview of how this could be achieved, including options for consideration by each community. However, it is important to recognise that good governance needs to adapt and continuously improve, considering the insight generated from real-life experience. The governance arrangements established at the outset of integration will inevitably evolve over time, informed and determined by members of each community.

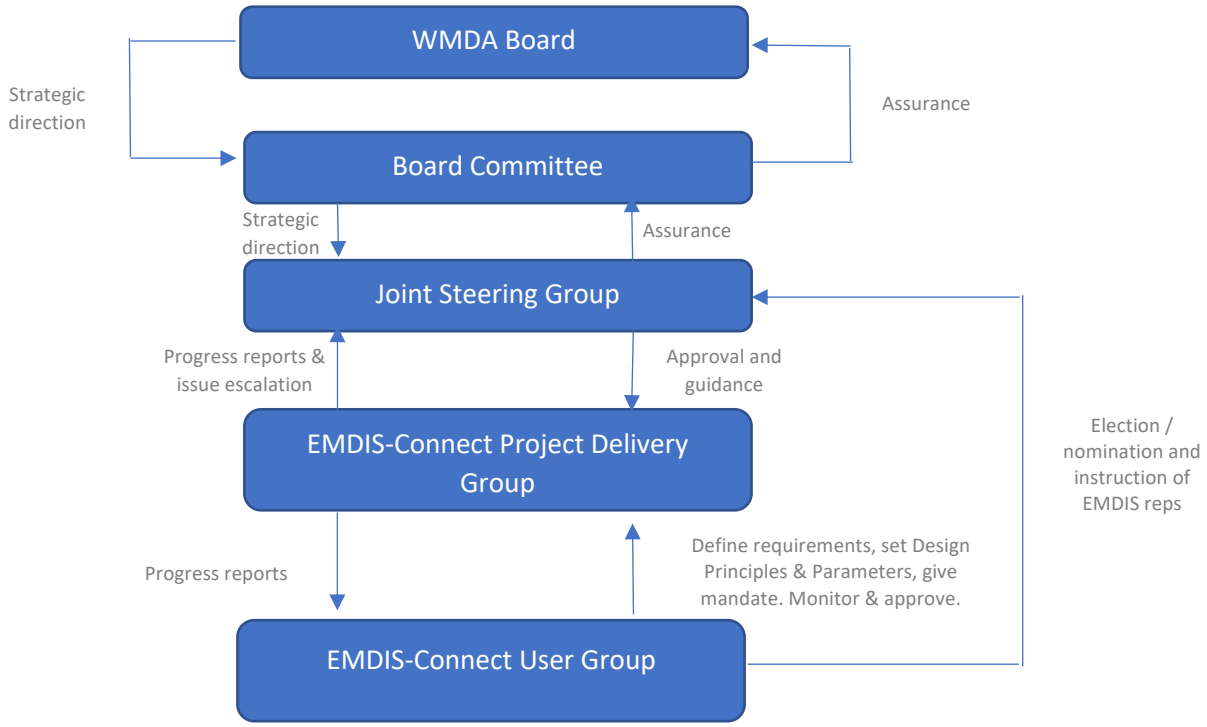
It is also important to acknowledge the varying arrangements that are required to effectively govern the 'design, development and implementation' of [a] new technical solution[s], and those required in 'steady state' / BAU. The former requires programme/project management-style governance to ensure the successful delivery of a change initiative. The latter requires governance that ensures the effective maintenance and continuous improvement of systems and associated processes, including the management and approval of 'Requests for Change'. This Framework focusses primarily on the governance arrangements to be established for the 'design, development and implementation' phase. Steady state / BAU governance arrangements will be developed in partnership with Users to ensure they reflect their needs and serve to safeguard their interests.

Indicative governance arrangements

<u>Principles</u>

- The principle of democratic and inclusive decision-making will be enshrined in the governance arrangements, with users and members having responsibility for defining their requirements; setting Design Principles and Parameters and mandating the Project Delivery Group. Users / members will monitor design and development to ensure adherence to Design Principles and Parameters and will test and approve products to ensure they reflect their agreed requirements.
- The Project Delivery Group shall have autonomy to design and develop products with agility, within the Design Principles and Parameters agreed by users and members.

Structure



Indicative financial arrangements

Other than the costs covered by the grant awarded by the European Union, the costs associated with the development and ongoing maintenance of SMC and EMDIS will be met through the payment of fees by users of each system/protocol. As a core principle, users and members will – where feasible and practical - only be responsible for the payment of fees for the systems, components and functionality they actually deploy and use.

Should SMC and EMDIS be retained as two distinct but aligned initiatives and systems/protocols (*Option 1*), there will be distinct fees for use of the two systems. Reflecting the principle of 'ever closer union', the viability of integrating the initiatives into a single solution with a shared infrastructure will – in time - be explored and, if/when agreed by users, pursued. This may, in time, lead to the harmonisation of fees.

Should fuller integration be pursued (*Option 2*), and a single solution with shared infrastructure be developed in the short-to-medium term, further exploration will be made – in consultation with users – to determine an appropriate harmonised fee structure. No changes to the fee structure will be implemented without the explicit consent of users, and the fee model will adhere to the overarching principle that users and members – where feasible and practical - will only be responsible for the payment of fees for the systems, components and functionality they actually deploy and use.

The following assumptions have been made about the costs and fees associated with each system / protocol. These assumptions will need to be revisited and validated as the two Options are appraised in detail.

Search and Match

According to WMDA, the fee for using Search and Match functionality will not change in the next few years. The pace of development will be determined by the resources available within the limitations of income generated

by existing fees. Income from fees and from the European Union grant will cover infrastructure development, implementation and new developments / on-going maintenance.

Connect
The European Union grant, and existing fees are expected to cover the costs associated with the design and implementation of 'Connect' functionality. Ongoing development and maintenance costs will be reflected in fees payable by members who utilise this functionality.

EMDIS 4.0:
Estimates of the cost of EMDIS 4.0 infrastructure and maintenance are around EUR 25,000 per year. It has not yet been decided how these costs will be distributed amongst the community. With the current 44 EMDIS users and a uniform distribution, the cost would be around EUR 550/year for each EMDIS registry. This new fee will be collected by the WMDA office. On-going development and maintenance costs will be covered by each individual EMDIS member, in line with current arrangements.

Detailed analysis of the costs of pursuing the development of a single solution has not yet been performed, as this is largely dependent on the technical blueprint. Once options for the technical blueprint have been developed, the consequences for costs and fees will be set out ahead of any decision by users.

Draft technical blueprint

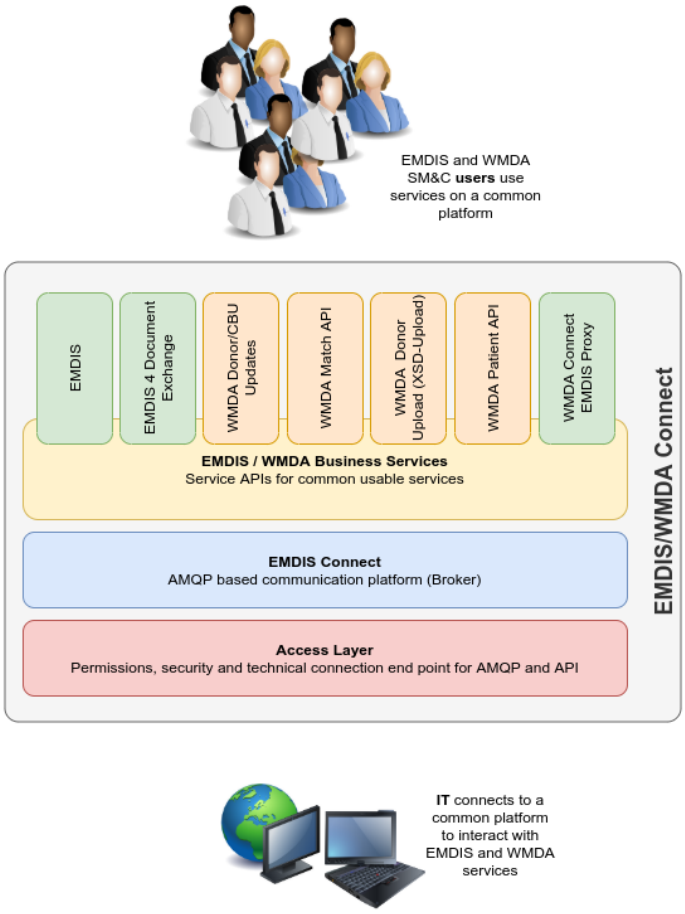


Figure 7: Draft technical blueprint of EMDIS-Connect

Appendix 5 – Security Essentials and Assessment Questionnaire

List of Registry Application Security Essentials:

1. RBAC - The registry system must be designed with role-based access whereby a user's authorization is limited to the duties of their role.
2. Authorization – The user entity (i.e., member) must have a process whereby access must be approved by company management before access is granted. An audit trail of the request, approval, and access enablement must exist. User access should be revoked in alignment with a role change or employment status.
3. Authentication – The registry system must authenticate users with multifactor authentication.
4. Auditing – The registry system must record significant security events (e.g., login, logout, password changes, etc).
5. Entitlement Review – The user entity (i.e., member) must perform quarterly entitlement reviews. Evidence of these reviews must be maintained for inspection.
6. Inactivity Timeout – The registry system must terminate idle user sessions after <= 30 minutes of idle time.
7. System Accreditation – The registry system manufacturer is responsible to ensure the registry system undergoes a formal security audit. Software releases are inspected for security impact as part of the software development lifecycle.
8. Penetration Testing – The registry system, when Internet accessible, must undergo a penetration test every N years (NMDP is 2 years), or upon architecturally significant change.
9. Transport Encryption – The registry system must encrypt all sensitive data (including personal data, user credentials, etc) in transit.
10. Encryption Keys – The registry system must employ a key management system to ensure the proper protection and scheduled rotation of keys. Only safe cryptographic algorithms can be used.
11. System Maintenance – The registry system's technologies must be hardened to the manufacture's hardening recommendations and patched within 30 days as the manufacturer releases security updates.
12. Anti-Malware – The registry system must be running anti-malware technology with continuous updates.
13. Physical Protection – The registry system must reside in a physically secured data centre or data processing room. This room must enforce named user credentials and retain an audit trail of access.
14. External Segmentation – The registry system, when accessible from the Internet, must employ a bastion host in an isolated network segment (i.e., DMZ).
15. Internal Segmentation – The registry system must reside on a segmented internal network with other production-class hosts, segmented from the internet workstation network(s).
16. Terms of Use – The registry system must display proper Terms of Use and Privacy Notice at the initial login screen.

Peer-to-Peer Security Assessment Questionnaire:

#	Subject	Check if compliant	GDPR	AU Privacy Act	US DPR
1	**Subject Consent**		**II**		
1.1.	Does the registry have adequate procedures in place to ask, store and retrieve consent from donors from who it collects personal information	O	II.7		§164.502

1.2.	In case the registry acts as a co-controller for the collection of patient data: does it have adequate procedures in place to ask, store and retrieve consent from patients or the assurance	O	II.7	APP 11	§164.502
1.3.	Does the donor's consent encompass portability to other registries and WMDA to allow matching with patients?	O	III.20	APP 8	§164.502
1.4.	Is all collected information sufficiently specified and explained in the registry's consent forms?	O	II.9	APP 1	§164.502
1.5.	Does the registry's state law allow exemption for medical and/or other sensitive data collected?	O	II.9.2a	APP 8	§164.502
2	**Information and access to personal data**		**III.S2**		
2.1.	Does the registry have procedures in place to confirm the collection of personal data at the time when personal data are obtained and does such confirmation include:	O	III.13.1	APP 10	
2.2.	Does the registry have procedures in place to provide access to personal data to donors within one month after receipt of a request thereto?	O	III.15	APP 12	45 CFR 164.524
3	**Rectification and erasure of personal data**		**III.S3**		
3.1.	Does the registry have procedures in place for donors to rectify personal information, either by direct access or a request?	O	III.16	APP 13	NA
3.2.	Does the registry have procedures in place to erase personal data or anonymize donor records in such way that the donor can no longer be identified at the donor's request?	O	III.17	APP 1	NA
3.3.	Does the registry have procedures in place to erase personal data or anonymize donor records in such way that the donor can no longer be identified when the donor no longer fulfils the criteria for being registered?	O	III.18	APP 1	NA
3.4.	In case of the action described under 3.3.: does the donor receive notification of the erasure?	O	III.19	APP 10	NA
4	**Data processing responsibilities**		**IV.S1**		

4.1.	Does the registry have data processing agreements or co-controlling arrangements in place with and of the following third parties to whom personal or pseudonymized data is provided: • WMDA • Donor centres whose donors are requested on behalf of local transplant centres • Transplant centres	O	IV.24 IV.26 IV.28	APP 8	§164.502(e)(1)(ii)
4.2.	Does the registry comply with requirements for controllers or processors outside the European Union?	O	IV.27	APP 8	
5	**Data security and data breach provisions**		**IV.S2**		
5.1.	Does the registry have a written information security policy in place?	O			
5.2.	Does the registry have adequate security measures in place to protect personal data, to include but not limited to: • Regular penetration testing and a record of remedial action based on the findings of such testing	O	IV.32	APP 11	§164.308 §164.310 §164.312
5.3.	Is a procedure in place to notify the supervisory authority or the data controller in case of a personal data breach within the limits as the regulations or the data processing agreements	O	IV.33	APP 11	§ 164.410(a)(1)
5.4.	Is a procedure in place to notify the donor in case of a personal data breach within the limits as the regulations or the data processing agreements require?	O	IV.34	APP 11	§ 164.410 - 414
5.5.	• Does the registry have examples of such notifications and can it demonstrate compliance with the regulations in these cases?	O	IV.33 IV.34	APP 11	?
6	**Data protection impact assessment**		**IV.S3**		

6.1.	Does the registry have procedures in place to assess and classify security risks, including but not limited to: • Environmental incidents, acts of God • Hardware failure • Physical access to data	O	IV.35	APP 11	§164.308(a)(1)(ii)(A)
6.2.	Does the registry have adequate backup procedures, to include: • data mirroring to prevent interruption of operations in case of hardware failure • complete recovery of the systems environment for a limited period • procedures to restore data and testing thereof • interval backup's	O	IV.35	APP 11	§164.308(a)(7)(ii)(A)
7	**Data Protection Officer**		**IV.S4**		
7.1.	Did the registry appoint a Data Protection Officer in compliance with local regulations?	O	IV.37	APP 1	45 CFR 164.308