Disclaimer:
"The content of this Deliverable D3.1 represents the views of the author only and is his/her sole responsibility; it cannot be considered to reflect the views of the European Commission and/or the Consumers, Health, Agriculture and Food Executive Agency or any other body of the European Union. The European Commission and the Agency do not accept any responsibility for use that may be made of the information it contains."

D3.1 Progress report on the WMDA online tool for reporting Serious Adverse Events and Reactions (S(P)EARs)

Grant Agreement number: 101015514
Project acronym: SAVDON
Work Package number: WP3

Periodic report: 1st □ 2nd □ 3rd □ 4th X

Period covered: from 01st January to 31st December 2021

Organisation: **World Marrow Donor Association (WMDA)**
LEAR: Lydia Foeken
Project coördinator: 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 D3.1 of an activity received funding under an operating grant from the European Union's Health Programme (2014-2020)."

Table of contents

Abbreviations

- S(P)EAR = Serious (Product) Events and Adverse Reactions
- WMDA = World Marrow Donor Association

Introduction

The WMDA believes that donor health and safety are of critical importance to ensure the continued viability of the global infrastructure of volunteer donors and therefore requires its members to report and investigate Serious (Product) Events and Adverse Reactions (S(P)EARs). Since mid-2019, the current WMDA online central global reporting system allows for members and non-members to submit S(P)EAR reports to the WMDA. This allows for the WMDA and its members to gain insight in the occurrence of serious events and adverse effects in relation to cell donation, collection and processing. This online reporting system has been previously described in the publication on EU deliverable report D4.1 '*Launch an online reporting system to report Serious(Product) Events and Adverse Reactions -S(P)EARs-(unrelated donors)*' in 2019 and D3.1 '*Online educational materials for transplant centre physicians on SEAR reporting*' in 2020.

Throughout 2020 and 2021, the continued use of the online reporting tool S(P)EAR has allowed for the WMDA to gather vital information on the occurrence of adverse events and to notify the transplantation and donation community of possible trends and areas of concern. Over the years, the numbers of received S(P)EAR reports as well as the number of reporting organisations have increased (2019: 210 reports, 27 reporting organisations; 2020: 474 reports, 32 reporting organisations). To allow for more flexibility to add on new requirements and solve existing barriers to reporting, a project was started in the late fall of 2020 to rebuild the S(P)EAR system. Details on this rebuild version are described in chapter 1.

This deliverable D3.1 publication focuses on the progress of the S(P)EAR online reporting tool since its initial release and reports on the process and achievements the WMDA has made towards implementation of a improved S(P)EAR online reporting tool in 2021. It also details which steps have been taken to ensure the awareness to the entire transplantation and donation community on the existence of the S(P)EAR reporting tool and to encourage adverse event reporting to the WMDA. This publication is part of the 2021 work programme of the World Marrow Donor Association for the EU Third Health Programme (2014-2020) and it will be used as a resource to support the development of the S(P)EAR online reporting tool and to ensure best reporting practices that serve to protect the rights and safety of donors.

2021 highlights

- Identified barriers on reporting to competent authorities by sending out a survey to reporters and ask about areas of improvement (Chapter 1).
- Rebuild of S(P)EAR online reporting tool commenced (Chapter 1)
- Published a report on SEAR/SPEAR 2020 incidents to WMDA on a public website and ask the Dutch Competent Authorities to share with their international colleagues (Chapter 2).
- Organised a webinar and consultation hour to explain SEAR/SPEAR to reporters and encourage organisations to start reporting (Chapter 2).
- WMDA members, transplant centres and healthcare authorities are aware of the WMDA reporting system and have the possibility to report serious adverse events and reactions to WMDA

1. The S(P)EAR online reporting tool

1.1. Background

The WMDA has been collecting data on serious events and reactions for almost 20 years (since 2003). In the early years data was submitted on paper to the WMDA, later on this evolved to a simple online survey form. Both methods left little opportunity for thorough data analysis. Some of the main issues identified on a macrolevel are listed below in Figure 1.

Main issues regarding the workflow prior to the implementation of S(P)EAR global online reporting tool (2019 release):

- Reporting organisations have to fill out the questionnaire in 1 go, users cannot save in between.
- Reporting organisations have no insight into history of previously reported S(P)EARs by their organisation.
- If additional information is required by the S(P)EAR committee it is time consuming and not added to the data available in the submitted form.
- Data export files take many hours to prepare
- No statistics analysis can be done on data.

Figure 1: Main issues regarding the workflow prior to the implementation of S(P)EAR global online reporting tool (2019 release)

To provide the WMDA and its member organisations more control over the submitted data, to increase user-friendliness and to guarantee safe handling of sensitive information, it was necessary to move towards a modernized version of reporting. Therefore, a new tool was introduced in 2019: the S(P)EAR global online reporting tool. Its design was based on the use of a framework for creating and maintaining form data called Knack; a hosted system designed to capture input from users and store the results in a database. More on the 2019 S(P)EAR online reporting tool below.

1.2 Current working version of S(P)EAR (2019 release)

The main objective of the 2019 S(P)EAR online reporting tool was to build a system that would address the issues listed above in Figure 1. The online reporting tool was developed in collaboration with an external party as described in the 2019 publication on EU deliverable report D4.1 '*Launch an online reporting system to report Serious(Product) Events and Adverse Reactions -S(P)EARs-(unrelated donors)*'. This publication highlights key points of action (see Table 1).

The S(P)EAR online reporting tool provided a big improvement from collecting data on paper or via the online questionnaire. The WMDA saw an increase in the numbers of received S(P)EAR reports as well as the number of registered reporting organisations (2019: 210 reports, 27 reporting organisations[1]; 2020:

[1] This only includes reporting organisations that *have* submitted a report during year listed. The total number of registered reporting organisations is larger, but since not all have submitted a report that year they are not counted.

474 reports, 32 reporting organisations[1]). The new reporting tool also allowed for customizable exports of data and this could then be used for data analysis.

Continuous monitoring of user satisfaction demonstrated that although it was a major step up from the old system, new challenges and concerns arose that needed to be addressed. The WMDA office and S(P)EAR committee also identified additional requirements to the system in place. It became apparent when reflecting upon the key points of the S(P)EAR reporting tool (as described in Table 1), and taking into account the annually growing number of reporters, reporting organisations and S(P)EAR reports received, that it was time to re-evaluate if the current tool still fit with the new needs and requirements from the WMDA office as well as the S(P)EAR reporters. It turned out that partially the existing reporting tool could be adapted to accommodate these changes, but for some changes an alternative solution would be required.

TABLE 1: KEY POINTS OF S(P)EAR REPORTING TOOL 2019	ACHIEVED	NEED TO ADDRESS/ROOM FOR IMPROVEMENT
User-friendly[1]	Partially	Yes
Enables reporters to keep track of all of their own reports in a dashboard	Yes	Yes
Enables reporters to do their own statistics	No	Yes
Provides the users the possibility of database queries[2]	Yes	Yes
Can be used by different organisations working on the same reports	No	Yes
Reports can be disseminated to organisations that operate outside the WMDA[3]	Partially	Yes
Adheres to the current privacy rules and regulations (EU GDPR)[4]	Yes	Yes

1. Although the system is much more user-friendly than what was used before, areas for improvement have been identified.
2. Only users that belong to the WMDA office can use database queries.
3. Currently only by saving the document locally as a PDF and then sharing it with the third party.
4. The system adheres to the EU GDPR, but reporters still upload sensitive information themselves. An improvement would be to identify areas for concern with the reporters regarding the GDPR more clearly and to make it more difficult for them to upload privacy-sensitive information.

1.3 Rebuild version of S(P)EAR (release due Q1 2022)

To ensure that the needs and requirements of the users were reflected in the new rebuild of the S(P)EAR online reporting tool, a survey was sent out to the S(P)EAR reporters. This, together with areas for improvement identified by key members of the S(P)EAR committee and WMDA office, formed a list of requirements that guides the development of the rebuild release (see Appendix I).

The new S(P)EAR reporting tool will allow for more elaborate data analysis by combining data from different sources available to the WDMA, more control over validated forms to implement updates when necessary, additional functionalities, such as: notifications of report status changes, joint reporting between reporting registries, the export of an organisation's own data, as well as improved security and privacy measures.

This rebuild of the is currently in development and will be released in 2022, please see Figure 2 for a timeline of the development.

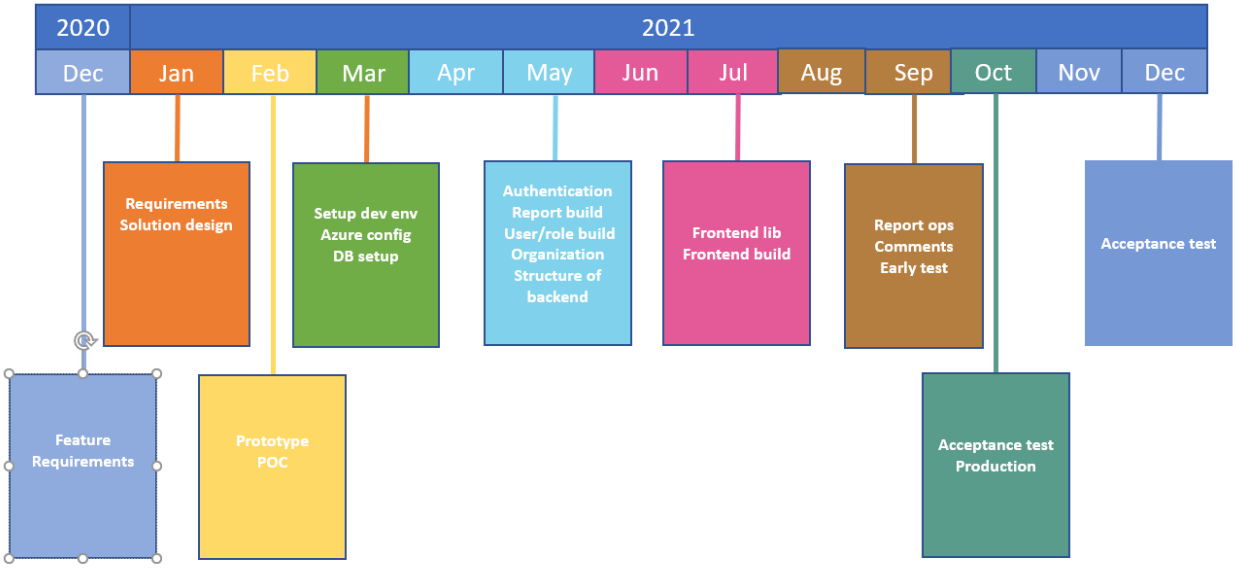


Figure 2: S(P)EAR rebuild timeline

2. Opportunities for promotion and publicity

Each year the WMDA uses their platform to provide exposure to the S(P)EAR reporting tool by informing the membership of analysed S(P)EAR data and providing opportunities for new and current S(P)EAR reporters to learn about the online reporting tool.

2.1 Published a report on SEAR/SPEAR 2020 incidents to WMDA on a public website and ask the Dutch Competent Authorities to share with their international colleagues

WMDA has sent the report to the Dutch Competent Authorities to be shared with their colleagues.

2.2 Webinars

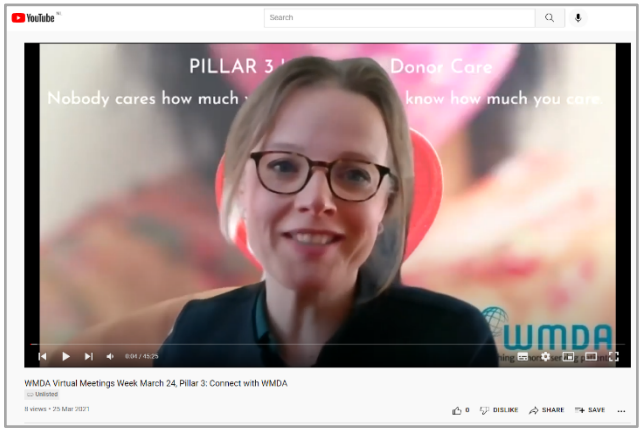
In 2020 two webinars were given to inform the blood stem cell community on S(P)EAR-related topics.

2.2.1 WMDA Virtual Week: S(P)EAR Annual Report by Thilo Mengling and Mirjam Fechter

During the WMDA Virtual Week held in March 2021, Thilo Mengling (Chair of the WMDA S(P)EAR Committee) and Mirjam Fechter (WMDA medical consultant/member of the S(P)EAR committee) hosted a webinar to elaborate upon the data analysed for the 2020 S(P)EAR annual report. In this webinar, the most important data of the 2020 report were presented and notable cases were discussed. The webinar can be viewed here: https://youtu.be/Zn3lajZHj5U

2.2.2 WMDA Virtual Week: Consultation Hour (Connect with WMDA) by Mirjam Fechter and Thilo Mengling

A novel way of connecting to new and existing S(P)EAR reporters was via the consultation hour webinar held by Mirjam Fechter (WMDA medical consultant/member of the S(P)EAR committee) and Thilo Mengling (Chair of the WMDA S(P)EAR Committee). During this hour attendees were invited to ask questions regarding S(P)EAR reporting. The casual set-up allowed for a direct dialogue with S(P)EAR committee members that might otherwise be perceived as difficult for (prospective) reporters to obtain. The webinar can be viewed here: https://youtu.be/5mETUmA5kUo



4. Future directions – lessons learnt

The focus of WMDA for 2021 in regard to S(P)EAR reporting was to ensure the S(P)EAR reporting tool meets the needs of the users and to encourage reporting amongst all users, including transplant centres. With the rebuild of the S(P)EAR online reporting tool and the webinars the WMDA has made significant and fruitful efforts in working towards these goals.

In 2022, the WMDA aims to roll-out the rebuild of the S(P)EAR reporting tool and monitor its performance and usage to ensure it has incorporated all the necessary requirements. In addition to the standard educational materials, such as webinars, the WMDA plans to fortify the S(P)EAR documentation base and to deploy an educational course for S(P)EAR reporters after the release of the rebuild. The documentation base surrounding S(P)EAR needs to be reviewed and revised where necessary to make sure it is complete, accessible, up to date and easy to use. By providing more and accurate documentation, the S(P)EAR set-up and process will become more transparent to the reporting centres. This will aid reporters in becoming more knowledgeable on S(P)EAR and hopefully will facilitate the registration of more reporting members and non-member organizations.

An important step forward in this era of a growing demand on family donors will be to continue to include transplant centres to submit their S(P)EARs regarding cell donations of family members throughout 2022. The WMDA would like to focus its attention in 2022 on reaching out to these transplant centres specifically to make them aware of our reporting structure and to actively recruit them to report their adverse events to the WMDA. The WMDA will send a letter to the Competent Authorities and will provide access to the application for interested Competent Authorities.

5. Appendices

5.1 Requirements S(P)EAR rebuild

1. Functional requirements

Most of these requirements are based off the current S(P)EAR application made in Knack. When any requirement is unclear it should follow the current application as closely as possible.

1. Must haves

1. The system should have users with 6 roles: Reporter, Committee member, Committee chair, Moderator (WMDA), Application Admin (Eefke) and System Admin (Bert & Leo).
    1. The system should distinguish between reporters from member and affiliate organisations.
        1. Reporters from affiliate organisations should only be able to submit incident reports to their super organisation, who need to approve them before they can be submitted to the moderator.
        2. Reporters from member organisations should be able to submit incident reports directly to the moderator.
        3. An incident report should be able to have up to two reporters. One from the affiliate organisation that created it and one from the member organisation that finally submitted it.
    2. For each user, the system should store their name, email address, password hash, user status, organisation(s) and roles.
2. Users should be able to have multiple roles.
    1. Users should be able to switch their active role to any of their assigned roles.
    2. Users should only be able to have one role active at any time.
    3. Users should be able to use the application correctly with any of their selected roles.
3. Users, organisations, and their roles should be imported from the CRM hourly through XML/JSON format.
    1. Any users/organisations that are no longer in the CRM should have their status changed to inactive.
4. The system should store organisations with their name, membership, parent organisations, ION number and status.
5. The system distinguishes between incident reports and overview reports.
    1. Incident reports are reports submitted by reporters concerning an incident.
    2. Overview reports provide an overview of the submitted incident reports visible to the user and can be exported by the user.
6. The system should store incident reports made by reporters.
    1. For each incident report the system should store among other things a reference number, author, status, organisation, creation date, date of most recent update, comments and filenames of uploaded files.
    2. There should be three types of incident reports: Harm to Donor, Harm to Recipient and Risk of Harm.
    3. The incident report should include a section Description of Harm.
    4. The incident report should include a section Product Specification.
    5. The incident report should include a section Donation Details.
    6. The incident report should include a section Donor Details.
    7. The incident report should include a section Recipient Details.
    8. The incident report should include a section Transplantation Details.
    9. The incident report should include a section Investigation of Problem or Incident.
    10. The incident report should include a section Investigation of Transport Problems.
    11. The incident report should include a section Finalization.
    12. Incident reports that have not been submitted should be available to a reporter as a draft with all filled in information saved.
7. Reporters should be able to
    1. create new incident reports.
    2. edit their own incident reports when it has not been submitted (draft) or when it has been unlocked to edit.
    3. delete their own incident reports before submitting.
    4. submit an incident report
        1. Reporters should only be able to submit an incident report when all File Response fields are completed.
        2. Reporter should only be able to submit an incident report when there are no validation errors on given data.
    5. view incident reports by their organisation.

6. view the committee's assessment of their incident reports.
7. view the status of their incident report.
8. comment on their own incident report when it has not been submitted for review or reviewed by the committee.
9. attach files to an incident report.
    1. The system should be able to handle files up to 10 MB.
    2. The system should be able to store up to 5 files related to a report.
    3. The system should only accept files with the following extensions: [.xlsx, .xls, .docx, .doc .pdf, .jpeg, .png, .gif, .tiff, .bmp, .txt].
    4. When attaching a file, the user should be required to tick a box stating that the file does not contain personal information, and if it does, they are responsible for violating GDPR, not WMDA.

8. All user actions should be logged.
    1. Log files should be kept for at least 6 months.
    2. Log files should not contain privacy information.
    3. Log files should be used for alerting in ELK suite and Kibana and defined such that they can be used in either.
9. The system should make regular backups of the database.
    1. A full backup of the database should be created daily.
    2. The system should keep logs off all changes to the database since the last full backup.
10. Committee members should be assigned to review groups by the Application Admin.
11. A review group will be automatically assigned to review certain types of incident reports.
    1. Members of the group that are related to the incident report's submitting organisations should be excluded from reviewing.
12. Moderators/Committee members should be able to write comments on incident reports.
    1. For each comment, the system should store the creation date, comment text, status, author and the reference number of the incident report it comments on.
    2. Comments should be visible to the committee, moderator and reporter of the report.
13. Comments/review notes should be editable as long as they are not submitted.
    1. It should be possible for comments/review notes which are not submitted to be deleted.
14. Moderators/Committee members should be able to write review notes on incident reports.
    1. For each review note, the system should store the creation date, note text, status, author and the reference number of the incident report in comments on.
    2. Review notes can only be seen by the creator.
    3. The committee chair should be able to release all review notes to be visible for the committee.
    4. For S(P)EAR, review notes should always be visible to all committee members of the review group.
15. Moderators/Committee members should be able to request additional information.
16. Committee members should be able to
    1. see the incident reports submitted to the committee.
    2. review submitted incident reports.
    3. see previously reviewed incident reports.
17. Moderators should be able to
    1. view all incident reports.
    2. approve incident reports and send them to committee members.
    3. Unlock incident reports for editing
18. Users should be able to export the incident reports they have access to as overview reports.
    1. Users should be able to create export templates.
    2. Overview reports should include comments and review notes on the incident reports in the overview report if the user can view them.
    3. The user should be able to export an incident as a pdf.
    4. The user should be able to export overview reports as json or csv.
19. The application admin should have backend access.
    1. The application administrator should be able to change an incident report's status.
    2. The application administrator should be able to add/remove questions.
    3. The application administrator should be able to add validation to questions or remove validation from questions.
20. Users should be able to log in using email, password and two factor authentication.
    1. Users should be able to change their password.
    2. Users should be able to recover a forgotten password by password reset request.

3. Users should only be able to change their password into a strong password.
4. A user's password should expire after 3 months after which they will be forced to change it using a password reset request.
5. Error messages at login should clearly state that username or password is incorrect.
6. Users should be able to log out
7. Users should be automatically logged out of the system after some period of inactivity.
    1. The application admin should be able to edit the maximum length of the inactivity period.
8. Before logout all changes should be saved.

21. The system should be able to display help texts with questions when editing an incident report.
    1. Users should be able to hover a help icon to access additional info on a question.
22. Users should see an overview of the incident report before submitting.
23. The system should create backups of the database periodically.
    1. It should be possible to recreate the current database at any time using the last database backup and the log files.
24. The system should show a validation error when invalid data is filled in.
25. Date fields should have a calendar in which you can select the date.
26. Reporters should be informed by email about changes to the status of one of their reports.
27. When a user switches to a different section, the incident report should be saved automatically.
28. When the incident report is submitted, the whole report is saved to the database.

2. Should haves

1. When editing an incident report, reporters should be able to switch between sections using shortcuts.
2. Users should be able to search their incident reports.
3. User should be able to create templates that they can use to create similar incident reports quickly.
4. Moderators, Application admins and System admins should be able to display general notifications to all users.
5. The system should have an endpoint to communicate with the WMDA dashboard.
6. The system should log new data in json format in addition to the text log.

3. Could haves

1. Users should be able to
    1. view statistics on their incident reports.
    2. view statistics on incident reports from their organisation.
2. The system should be able to show statistics on submitted incident reports.
3. While writing a comment or review note, the user should be able to browse the relevant incident report.

4. Would/won't haves

None

2. Non-functional requirements

1. The system should be programmed using Python 3.8.
2. The underlying database should be made using PostgreSQL 11.
3. The system should be build using Django 3.1 framework.
4. The Frontend of the system will be made using ReactJS, VueJS or Angular.
5. The system should comply with GDPR.
6. The system should follow the ISO 27001:2017 standard.
7. The rebuild app should be delivered for User Acceptance Testing (UAT) latest Q2-2021.
8. The system should be documented.
    1. Any changes with respect to the current application should be documented.
    2. All design decisions should be documented.
    3. Any potential improvements to the system for after go-live should be documented.
9. The code should have built-in unit tests. This does not apply to the GUI.
10. The system should be quality checked using SonarCube.
11. The system should use Progressive Web App technology to work on any device.
    1. Progressive Web App technology should be tested on multiple devices and all tests should be documented.
    2. The system should notify users when their system is not supported by Progressive Web App technology.
12. All code should be stored on the WMDA Github source code repository
13. All code should have inline documentation to a high standard.
14. The system should be tested and test testimonials should be documented.
15. Test cases should be designed at user level.

16. The system should be able to support 20 concurrent users.
17. The system should be structured using the SOLID principles.
18. The system response time should be lower than 2 seconds for regular operations.
19. The system should be easily adaptable for new functionality