D4.1

The HEIR 2nd layer of services package for the MVP

Project number	883275
Project acronym	HEIR
Project title	A secure Healthcare Environment for Informatics Resilience
Start date of the project	September 1st, 2020
Duration	36 months
Programme	H2020-SU-DS-2019

Deliverable type	Demonstrator
Deliverable reference no.	D4.1
Workpackage	WP4
Due date	08-2021-M12
Actual submission date	01/09/2021

Deliverable lead	AEGIS
Editors	Leonidas Kallipolitis, Michalis Vakalellis
Contributors	Michalis Smyrlis (STS), Matthias Pocs (STELAR)
Reviewers	George Tsakirakis (ITML), Matthias Pocs (STELAR)
Dissemination level	PU
Revision	Final / 1.0
Keywords	Observatory, Benchmarks, Cyber-Security

Abstract

This deliverable serves as an accompanying report which refers to the release of the 2nd layer of services package for the HEIR MVP. The described work presents the functionalities and design of the components that compose this demonstrator, namely the HEIR Observatory, the global benchmark and the 2nd layer of visualisations.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883275

Executive Summary

The deliverable 4.1 'The HEIR 2nd layer of services package for the MVP' describes and shows screenshots of the first prototype of the HEIR Platform. At this stage, only the minimum required components are containerized to act as a proof of concept of the effective integration of the 2nd layer components into an integrated prototype. The demonstrated minimum functionality showcases the potential of the proposed solution. For the needs of the first MVP, HEIR components were deployed at PAGNI infrastructure.

The 2nd layer of services package for the MVP includes the components: i) the HEIR Observatory, ii) the HEIR global benchmark against which the RAMA scores of medical infrastructures will be compared, and iii) the 2nd layer of Visualizations. It also includes the guidelines and description of the legal and security requirements that are incorporated in the current version of the platform.

Next Actions have been identified to enrich the functionalities of each component to serve the security needs of medical devices for the 1st complete version of the HEIR 2nd layer of services package in M18.

Table of Contents

List of Figures

List of Tables

AUCUNE ENTREE DE TABLE D'ILLUSTRATION N'A ETE TROUVEE.

1. Introduction

1.1 Scope and objectives

This document presents the current status of the HEIR platform regarding the developed components that realize the HEIR Observatory and the 2nd layer of services package for the MVP. The HEIR Observatory is a web-based platform that collects, analyses and correlates the results of all tests run by the HEIR Client in any device or system, facilitating the work of IT professionals in medical environments as it can display their current security status in terms of adaptation of good practices.

In the context of MVP, the Observatory is based on data being fetched by the HEIR Client deployed in PAGNI premises. Therefore, the infrastructure is provided by PAGNI and serves as a demonstrator for minimum viable product of HEIR offerings.

This deliverable and the current development efforts support the fulfilment of the following specific project objectives:

- S.O.1: Develop and support a threat identification and cybersecurity knowledge base system
- S.O.2: Provide scientific and technological advances in Risk Assessment and Security
- S.O.3: Provide novel tools and services for enabling secure data storage and sharing in healthcare operations

1.2 Document structure

The deliverable is organized into five sections whose purpose is briefly described next.

- Section 1 introduces the deliverable.
- Section 2 presents the MVP definition, the MVP development, and the subsequent steps towards the establishment of fully functional prototypes.
- Section 3 describes the HEIR MVP architecture, its legal aspects and provides deployment details of the Observatory components.
- Section 4 presents the use case scenarios.
- Section 5 highlights the overall conclusions and plans.

1.3 Relationship with other documents

This deliverable is related to all the Tasks and deliverables of WP4. Moreover, there is a close interrelation between this deliverable and the WP2 and WP3 deliverables, and especially D2.1 (The HEIR facilitators package: MVP) & D3.1 (The HEIR 1st layer of services package for the MVP), as well as with WP7 concerning the legal framework monitoring.

In addition, this deliverable is strongly connected to D5.2 “HEIR Minimum Viable Product” as HEIR 2nd layer of services packaging will be part of the overall HEIR MVP.

2. MVP definition

2.1 Methodology

A minimum viable product (MVP) is a concept that stresses the impact of learning in new product development. The MVP is an early version of a new product which allows a team to collect the maximum amount of validated learning about end-users with the least effort. A key premise behind the idea of MVP is that you produce an actual product that you can offer to customers and observe their actual behavior with the product or service.

The primary benefit of an MVP is not to deliver the smallest amount of functionality of the platform but to develop and provide the criteria of being sufficient to learn about the business viability of the product.

For the definition of MVP for the 2nd layer of services package we followed the following iterative process:

- Identification of most important business goal: Need to validate technology readiness to meet security expectations of medical institutions
- From business goals to feature scope: Choosing what is absolutely necessary to achieve business goal
- Creating MVP scope draft: Identification of MVP scenario that can serve our goal
- Iteratively reduce the scope: Walk through each use-case and identify of the absolutely necessary functionality
- Translating scope into technology: The actual development and integration of the components in scope.
- Execute, Evaluate, Learn: Understanding of end-user feedback in order to improve / refine the original scope.

2.2 HEIR 2nd layer of services MVP

Following the above methodology and taking into account the advancements of work done in the HEIR Facilitators (WP2-D2.1) and the HEIR Clients (WP3-D3.1), the MVP for the 2nd layer of services package includes (i) the HEIR Observatory (ii) the HEIR global benchmark against which the RAMA scores of medical infrastructures will be compared; and (iii) the sub-system for the 2nd global layer of visualization. The demonstrator will be presented in a short report, including screenshots and explonatory comments of the functional description of each involved component and its description.

The MVP implementation provides the foundation for integrating the 'HEIR Analytics Engine' component as described in the HEIR architecture, reported in D1.3. In specific, the HEIR Analytics Engine is expected to handle the data from multiple clients, stored in the Observatory Database. The Engine intents to provide functionalities such as statistical analysis, outlier detection and more according to the incoming data processed by HEIR clients. Given the fact that only one client is included in the MVP, the scope of the Analytics Engine will be met in the subsequent implementation of the fully integrated prototype.

For the HEIR 2nd layer of services MVP, data stored in Observatory database consists mainly of standalone security assessment data, as collected and processed by HEIR Client. The local

RAMA Score is fed to ‘HEIR Global Benchmarks’ module, through the ‘HEIR Aggregator’ component in order to calculate the Global RAMA score. All data collected and analysed by HEIR Observatory, are then visualized and presented to end users by the 2nd layer Visualization component.

3. 2nd layer of services MVP architecture

3.1 HEIR Global Benchmarks

3.1.1 Functional Description

As described in "D3.1- The HEIR 1st layer of services package for the MVP", the MVP version of the HEIR Global benchmarks will be based on the RAMA score of a single department. More specifically, the local RAMA Score calculator integrated within PAGNI's local environment will provide the local RAMA score along with a set of metadata (e.g., number of identified vulnerabilities, number of identified misconfigurations, etc.) to the HEIR Aggregator. Next, the aggregator will provide this information to the HEIR observatory to make them available to the interested parties as personalized services. That being said, MVP's Global RAMA Score will contain information from a single pilot excluding the personalised information.

3.1.2 Component Design

As presented in Figure 1, the local instantiation of the RAMA Score calculator will communicate with the HEIR aggregator to provide the local RAMA score as well as the above-mentioned metadata. These will constitute the main part of the HEIR's MVP Global Benchmark and will be made available to the interested parties through the HEIR Observatory module.

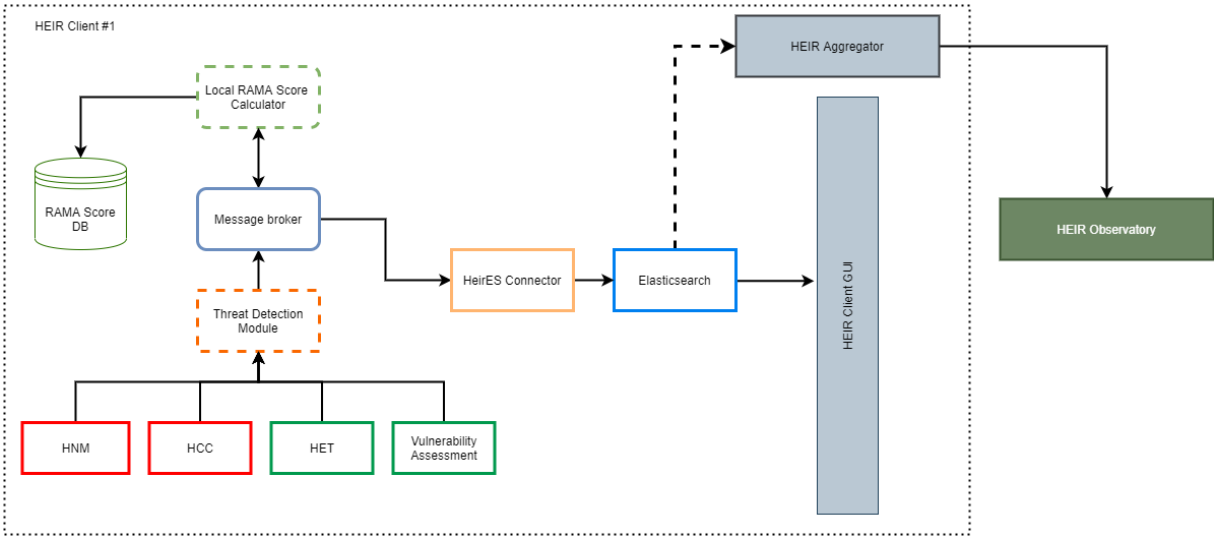

Figure 1 Global benchmarking high-level architecture

3.2 HEIR Observatory

3.2.1 Functional Description

The HEIR Observatory is responsible to collect, analyse and present the results of all the deployed HEIR Clients in order to provide global insights on the level of security in healthcare environments. The Observatory database will store all this information which will be analysed by the HEIR Analytics Engine in order to produce statistics, historical analysis and trends as well as recommendations and best practices. In the MVP context, data will be collected from the HEIR Client deployed in PAGNI's infrastructure. Basic statistics will be available for the second layer of Visualisations since the Analytics Engine will be engaged at the second phase of development in order to have greater amount of data to work with.

3.2.2 Component Design

The following figure depicts the high-level architecture of the HEIR Observatory for the MVP. The HEIR Client of PAGNI will send RAMA score and relevant metadata as analysed in D3.1, without any hospital identifying indicator. This de-association of events sent to the repository will be applied to all clients so as to preserve anonymity and make any aggregated information and statistical information on cybersecurity events displayed in the observatory impossible to be connected with any particular hospital.

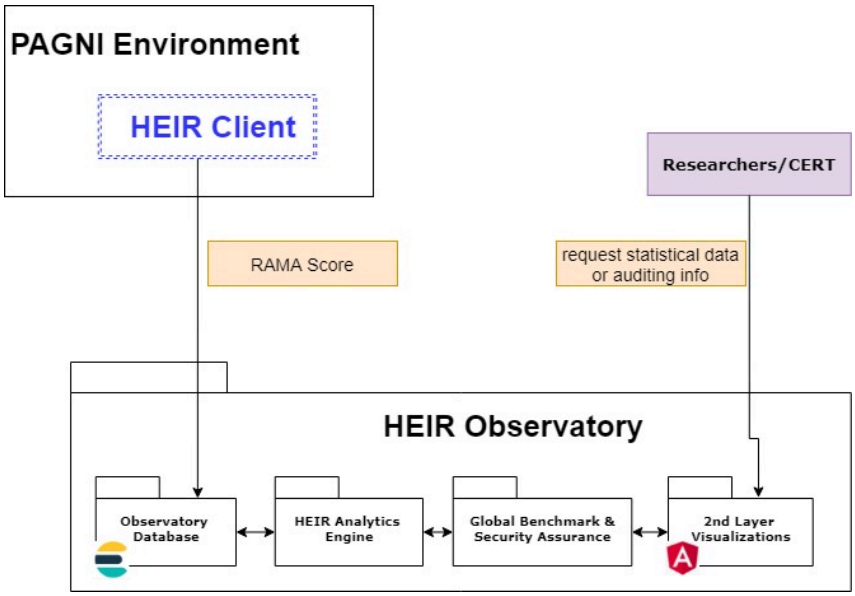

Figure 2 HEIR Observatory architecture

The technology used for the HEIR database is Elastic Search[1] which can accommodate storage, fast searching and analysis of huge numbers of data items. It provides a RESTful API for advanced searching and aggregation queries that support statistical analysis and also has built-in support for scaling operations such as automatic management of cluster-based deployments.

The 2nd layer of Visualisations will be developed as a web application as described in the next section.

3.3 2nd layer of Visualizations

3.3.1 Functional Description

The 2nd layer of Visualisations includes all the elements and methods to present information gathered by the HEIR Observatory. For the MVP, the Global RAMA Score will be derived by the single HEIR Client deployed in PAGNI but once more Clients get deployed in the next development phase, data will be presented at this layer as well.

Users accessing the HEIR Observatory will have a read-only access to data collected from the HEIR Clients. The main functionalities offered in the MVP are the presentation of the Global RAMA Score, the RAMA Scores per hospital in an anonymized manner (i.e. no hospital will be given by name since this information will not be available as described in previous section) and some global statistics about the collected cybersecurity-related events.

[1] https://www.elastic.co/elasticsearch/

3.3.2 Component Design

The 2nd layer of Visualisations is a web application presenting the aforementioned information. Figure 3 below shows how the Global RAMA Score is presented and how RAMA score information about various hospitals is given to end-users. (Note that only one hospital is actually connected during the MVP).

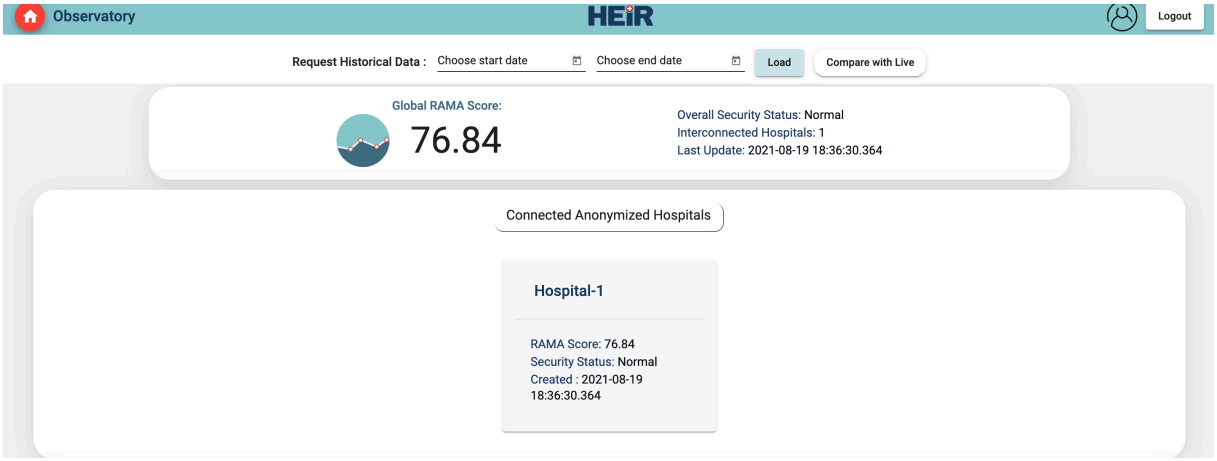

Figure 3 2nd layer Visualisations: Global RAMA Score

Moreover, the global statistics section of the screen will present the initial statistical information derived by data captured or generated within the MVP context. So, the top 10 identified vulnerabilities with the appropriate links to MITRE's CVE knowledgebase[2] for each vulnerability are presented. Moreover, the daily average of critical events identified in connected clients together with the corresponding RAMA Score are presented for the latest time period. Finally, RAMA Score per hospital (anonymised) is also displayed in a separate chart to illustrate how hospitals compare with the global RAMA core. Figure 4 below depicts how the information will be displayed.

[2] https://cve.mitre.org/

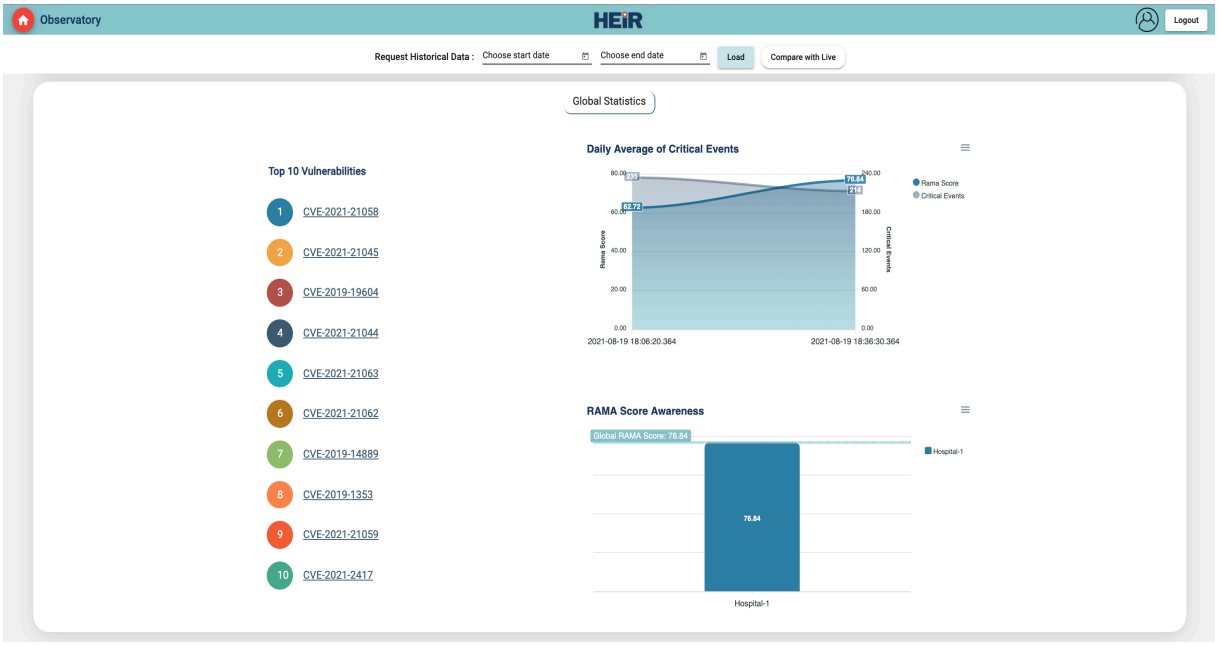

Figure 4 2nd layer Visualisations: Global Statistics

All this information will be displayed in order to give an overview of the cybersecurity status within the HEIR ecosystem. Authorised researchers and relevant audience will have the opportunity to explore knowledge gathered from HEIR Clients and identify common vulnerabilities and exposures that threaten healthcare infrastructures. The complete picture of HEIR's 2nd layer visualisation is illustrated in Figure 5 that follows.

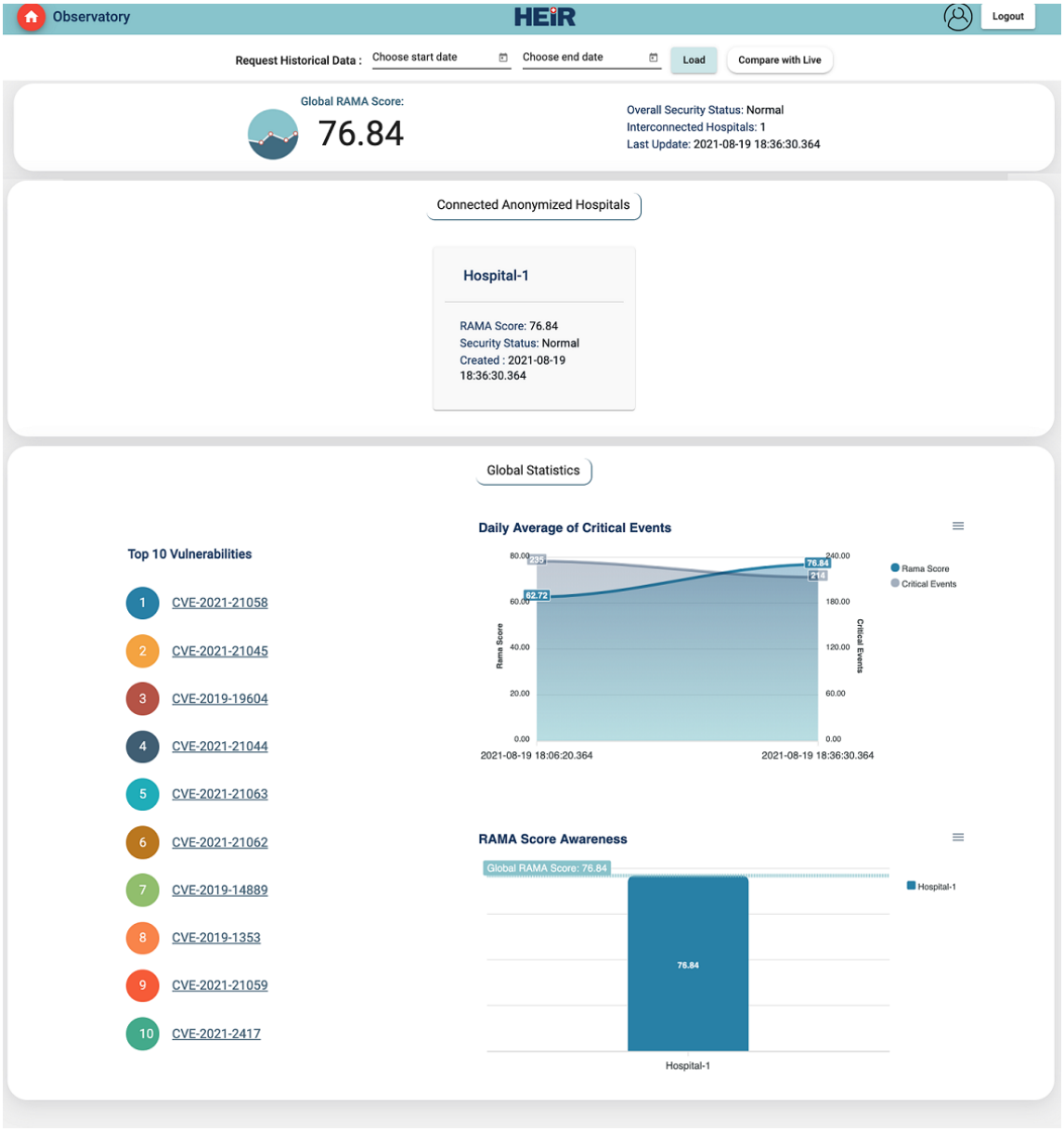

Figure 5 2nd layer Visualisations: Full Page

3.4 Legal Issues on health environment security

In healthcare organisations, health data security and privacy are two of the most crucial concerns. In particular, the healthcare systems may involve access to anonymised data provided by participants to advance research. Medical datasets are intended to be kept confidential. This means that control should be provided over the ability to share health information without compromising patients' privacy. Data security is a central aspect of the HEIR project. For this reason, compliance with legislation such as the General Data Protection Regulation (GDPR), ePrivacy Directive and other laws concerning data protection and privacy of any specific partner's home country will be ensured concerning personal data and protection of privacy in the electronic communication and networks.

The HEIR platform will rely on different security and privacy technologies and techniques. One part of this are Privacy-Enhancing Technologies (PET), a category of technologies (i.e., Software, Hardware,) designed at protecting the privacy of users by reducing personal data,

usually without losing the functionalities of the systems to which the Privacy Enhancing Technologies are applied. These technologies are a very board category and measures covering anything from a broadly speaking sensor to advanced cryptographic techniques [15]. However, Privacy Enhancing Technologies includes techniques that allow for personal data to be tagged with instructions about how this data can and should be used, for example, for anonymising networks, prevent tracking online and secure messaging [16].

From a legislative perspective cybersecurity is governed by the Directive 2016/1148 of the European Parliament and of the Council on measures to ensure an integrated high level of security of network and information systems throughout the Union (NIS Directive) [6]. To support the legislation, the NIS Cooperation Group (national ministries and cybersecurity agencies) work towards the EU-wide consistent transposition of the Directive and guides the EU CSIRT network. The draft NIS 2 Directive [7] further develops the cybersecurity requirements and explicitly includes healthcare as a group of services subject to the legislation as well as services of Electronic Identification and Trust Services for Electronic Transactions (eIDAS). Another novelty would comprise the setup of an EU Cyber Crisis Liaison Network (EU-CyCLONe) to facilitate cross-border communication about security incidents.

The General Data Protection Regulation (GDPR) is the legislative framework for the processing of data about people in the EU. It aims to protect the rights of citizens but also to promote free data flow across borders of the EU Member States (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2]). The GDPR principles (Article 5) include lawfulness (e.g. consent; see Articles 6 to 9), data quality, proportionality, data security, fairness, accountability, and transparency (see e.g. Articles 12 to 14). In contrast to the NIS Directive(s) which need(s) to be transposed into national law, the GDPR is directly applicable in the EU Member States. Other pieces of legislation include the Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [4] and the ePrivacy Directive [5] (to be repealed by a Regulation). In order to be able to trust information received by individuals and organisations using signatures, seals, time stamps, documents, delivery, certificates, etc., the eIDAS Regulation sets the EU level of electronic identification, trust and authentication services (Regulation (EU) 2014/910 [3]).

The application of the GDPR is only required the data are “personal”, that is, the information concerns an “identifieed or identifiable” natural person [2]. However, this is not a trivial assessment and there are techniques to achieve anonymisation and pseudonymisation (see e.g. [13]). It is to be highlighted that pseudonymous data are still considered “personal”. For the concept of personal data [21], it is central to consider the latest state of the art in technology and business practice because the GDPR defines data as non-anonymous if any means are “reasonably likely to be used” to identify the individuals ([2] Recital 26). But even if data are considered anonymous, the safeguards for achieving and maintaining the state of anonymity is precisely what can be considered as a legal requirement to be able to rely on the inapplicability of the GDPR. Anyway, the stakeholders (developer, controller, processor, patient, researcher) need to be taken into account. In order to comply with the legal obligations, the state of the art needs to be considered, for example, according to Article 25(1) GDPR. European and international privacy standards specify the state of the art (see analysis in [18]) such as:

- ISO/IEC 27701 [8], ISO 27799 [9] on security management
- CEN Standard on the implementation of the International Patient Summary [10]
- prEN 17529 (public consultation draft) [11] on data protection by design
- ISO/IEC 29134 [12] on privacy impact assessment
- ISO 25237, ISO/IEC 20889 [13] on pseudonymisation and de-identification techniques

- ISO/IEC 62304 [14] on secure health software development lifecycle

Specifically for healthcare, Member State law is still applicable. Article 9(4) GDPR stipulates that "Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health." Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 (Patient's Rights Directive) regulates the application of patients' rights in cross-border healthcare and is the main political and strategic Governance Body for eHealth in Europe, connecting the National Authorities responsible for National Contact Points for eHealth (NCPeH) [1]. It sets up the eHealth Network (eHN) under Article 14 to develop interoperability for cross-border eHealth services. The Patient's Rights Directive is supported by the Agreement between EU Member States governing the data exchange among National eHealth Contact Points (NCPeH) [13]. An analysis of data protection in healthcare can be found in [17]. In order to address security in HEIR, the legal aspects mentioned above will be taken into account to prevent unauthorised access, modification, replication, or destruction of data. This is true for data transport but also storage in online repositories, the sensitivity level of the data in question, the on-premise data use (for research and development) and communication (e.g. email) and the software used.

4. 2nd layer of Services MVP scenario

The MVP Scenario for the HEIR Observatory is as follows:

- The HEIR Client in PAGNI generates events and RAMA Score.
- Events are anonymized and sent to the HEIR Database.
- RAMA Score is sent to the HEIR Database.
- Global benchmark is calculated.
- 2nd layer visualisations fetch data from the HEIR Database and present them in the UI.
- Anonymous users can access statistical data and view aggregated, global information about RAMA Scores and cybersecurity events.

5. Conclusion

This document is the first outcome of WP4 and sets the basis for upcoming output of WP4 Tasks and strongly links to the work that is - in parallel - conducted in other technical WPs, including WP2 and WP3. It describes the functional components that are part of the 2nd layer of services package for the MVP, their design specifications and their integration elements that enable the delivery of first version of HEIR Observatory. The technical approach for the MVP is based on a service-oriented communication between the components, i.e. the HEIR Global Benchmark and the Observatory. Data will be stored in a document-based database, namely ElasticSearch, which will also provide the basis upon which further analytics will be extracted on the next development phase.

The implementation of the Observatory will continue through an iterative-incremental process to produce two more releases of the proposed solution - the first complete version in M18 and the final version of 2nd layer of services package in M26 of the project.

REFERENCES

[1] Directive 2011/24/EU of The European Parliament and of The Council of 9 March 2011 on the application of patients' rights in cross-border healthcare.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj

[3] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

[4] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). COM/2017/010 final - 2017/03 (COD), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010

[5] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058

[6] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148

[7] Shaping Europe's digital future. 16 December 2020. Proposal for directive on measures for high common level of cybersecurity across the Union https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union

[8] ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines, https://www.iso.org/standard/71670.html

[9] ISO 27799:2016 Health informatics — Information security management in health using ISO/IEC 27002, https://www.iso.org/standard/62777.html

[10] CEN standard TS 17288 'The International Patient Summary: Guideline for European Implementation', https://www.cen.eu/news/brief-news/Pages/NEWS-2021-009.aspx

[11] EN 17529 Data protection and privacy by design and by default, https://standardsdevelopment.bsigroup.com/projects/2020-00802#/section

[12] ISO/IEC 29134:2017 Information technology — Security techniques — Guidelines for privacy impact assessment, https://www.iso.org/standard/62289.html

[13] ISO/IEC 20889:2018 Privacy enhancing data de-identification terminology and classification of techniques https://www.iso.org/standard/69373.html

[14] IEC 62304:2006 Medical device software — Software life cycle processes, https://www.iso.org/standard/38421.html

[15] The Royal Society, protecting privacy in practice: The current use, development, and limits of Privacy Enhancing Technologies in data analysis. ISBN 978-1-78252-390-1, https://royalsociety.org/topics-policy/projects/privacy-enhancing-technologies/

[16] ENISA PETs Controls Matrix report, 12/2016, https://www.enisa.europa.eu/publications/pets-controls-matrix/pets-controls-matrix-a-systematic-approach-for-assessing-online-and-mobile-privacy-tools

[17] Conley, E.C. and Pocs, M., "GDPR Compliance Challenges for Interoperable Health Information Exchanges (HIEs) and Trustworthy Research Environments (TREs)", European Journal for Biomedical Informatics, Volume 14 (2018), Issue 3, pages 48-61. Available online at https://www.ejbi.org/abstract/gdpr-compliance-challenges-for-interoperable-health-information-exchanges-hies-and-trustworthy-research-environments-tre-4619.html.

[18] Quemard et al., Report of the European Cybersecurity Agency ENISA: Guidance and gaps analysis for European standardisation, 2019. Available online at https://www.enisa.europa.eu/publications/guidance-and-gaps-analysis-for-european-standardisation.

[19] Guidelines 05/2020 on consent under Regulation 2016/679, point 1(2), also 2(9), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

[20] Working Party Opinion 1/2010 on the concepts of "controller" and "processor, 2010, page 13, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf.

[21] WP29. Opinion 4/2007 on the concept of personal data, 2007. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf, page 5