PAROMA-MED
Privacy Aware and Privacy Preserving Distributed and Robust Machine Learning

Funded by the European Union

PAROMA-MED Deliverable D3.2

Security and Data Privacy Awareness

Editor, Organisation:	AGE
Deliverable nature:	Report (R)
Dissemination level: (Confidentiality)	PU – Public
Contractual delivery date:	December 31, 2023
Actual delivery date:	December 18, 2023
Suggested readers:	eHealth Application/Service Developers, Platform Operators, PAROMA-MED consortium
Version:	1.0
Total number of pages:	25
Keywords:	Security Awareness, Privacy Awareness,

Abstract

This report collects and presents all the security and privacy awareness concepts and models defined and developed in Task T3.3. This task aims to provide users with situational awareness through visual representation, which enables quick and effective responses to cyber-attacks and continuous monitoring of the current privacy posture. This document reports on the first iteration of the concepts and models defined and developed and a first prototype GUI for situational awareness. The second iteration of the concepts, models and the prototype GUI will be presented in deliverable D3.4.

[End of abstract]

Disclaimer

All PAROMA-MED consortium parties have agreed to full publication of this document.

This project is funded by the European Union under Grant Agreement 101070222. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission (granting authority). Neither the European Union nor the granting authority can be held responsible for them.

Imprint

Full project title	Privacy Aware and Privacy Preserving Distributed and Robust Machine Learning for Medical Applications
Short project title	PAROMA-MED
Number and title of work-package	WP3 Security and Privacy Assurance Services
Number and title of tasks	T3.3 Security and Privacy Awareness
Document title	D3.2 Security and Data Privacy Awareness
Editor: Name, organisation	Benjamin Ertl, AGE
Work-package leader: Name, organisation	Stefan Covaci, AGE
Internal reviewer(s): Name(s), organisation(s)	Orazio Toscano ERI, Stéphane Lorin TSG
Clearance by the Security Advisory Board	Clearance was not required
Estimation of PM spent on the Deliverable	1 PM

Executive summary

In the context of PAROMA-MED, security and data privacy awareness refers to understanding and knowledge of security and data privacy risks, threats, and best practices among the stakeholders involved in developing, deploying, and using the PAROMA-MED platform. This includes developers, IT administrators, end-users, and other parties involved in the project.

Security awareness focuses on protecting the PAROMA-MED platform from cyber threats and attacks. It includes understanding the risks associated with data breaches, phishing attacks, malware infections, and other security threats and the best practices for securing the platform.

Data privacy awareness focuses on protecting the privacy of personal data collected, processed, and stored by the PAROMA-MED platform. This includes understanding the privacy risks associated with data breaches, unauthorised access, and inappropriate data use and sharing, as well as the best practices for protecting personal data, such as obtaining user consent, implementing data encryption and access controls, and complying with relevant privacy regulations.

Adequate security and data privacy awareness methods can help reduce the likelihood and impact of security and privacy incidents and improve the overall safety and privacy posture of the PAROMA-MED platform. These methods can include training, awareness campaigns, regular communication and reminders, and ongoing monitoring and feedback to ensure stakeholders know the latest security and privacy threats and best practices.

The situational awareness GUI developed within this project enables stakeholders to gain comprehensive insights into the security and privacy landscape of the healthcare ecosystem of PAROMA-MED. It facilitates intuitive interaction, enabling users to swiftly comprehend complex data, make informed decisions, and take prompt actions to address potential threats and privacy concerns.

Following core security and data privacy concepts, the PAROMA-MED situational awareness GUI supports stakeholders in conducting security and data privacy training, management of security controls and privacy safeguards, consent and privacy management and privacy impact and risk assessment (PIA).

List of authors

Company	Author	Contribution
AGE	Benjamin Ertl	Editor
AGE	Stefan Covaci	Section 2, 3, 4

History of Versions

Version	Date	Context
0.0	2022/11/04	Draft ToC
0.1	2023/04/19	Initial concepts
0.2	2023/08/14	Updated content Section 3, 4
0.3	2023/08/30	Updated content Section 5, 6
0.4	2023/09/14	Draft version for internal review
0.5	2023/12/04	Version for internal review
1.0	2023/12/18	Final version
Security Advisory Board Review and Comments		
		The document does not contain any personal, private or sensitive information.

Table of Contents

Contents

List of figures and tables

List of figures:

Abbreviations

API	Application Programming Interface
EU	European Union
FHIR	Fast Healthcare Interoperability Resources
GDPR	General Data Protection Regulation
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
JSON	JavaScript Object Notation
NIST	National Institute of Standards and Technology
OPA	Open Policy Agent
PAROMA-MED	Privacy Aware and Privacy Preserving Distributed and Robust Machine Learning for Medical Applications
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
RBAC	Role-based Access Control
SECaaS	Security as a service
UI	User Interface
XML	Extensible Markup Language

1 Introduction

In an era where healthcare innovation meets the digital realm, PAROMA-MED is a pioneering platform-based hybrid-cloud delivery framework that revolutionises how healthcare data is managed and secured. Designed to address the intricate challenges of the modern healthcare landscape, PAROMA-MED empowers healthcare providers, practitioners, and organisations with a comprehensive solution that enables seamless data flows across federated cross-border environments while prioritising utmost privacy and security.

At its core, PAROMA-MED embodies the synergy of cutting-edge technology and patient-centric care. Leveraging its advanced hybrid-cloud architecture, the platform bridges the gap between on-premises infrastructure and cloud resources, offering a harmonious environment for healthcare data management. This unique approach ensures flexibility and scalability, allowing healthcare entities to optimise their operations while adhering to the highest data security standards and regulatory compliance.

The PAROMA-MED security and data privacy awareness concept incorporates innovative features that enable situational awareness and security-conscious decision-making, providing users with real-time insights into threats, vulnerabilities, and potential anomalies detected by sophisticated algorithms. Through intuitive visualisations and models, users immediately understand risk levels associated with identified hazards, enabling rapid and precise responses to cyber-attacks and ensuring continuous monitoring of the current privacy posture. PAROMA-MED allows the definition of custom, pre-defined and on-the-fly remediation actions to safeguard the platform and its users against new and sophisticated attacks.

Privacy and data protection are fundamental to the PAROMA-MED platform. With its federated cross-border capabilities, the platform empowers data flows while safeguarding patient privacy and complying with stringent data protection regulations. Visual representations of privacy and compliance postures provide an intuitive overview, ensuring that data governance remains a constant focus within every facet of healthcare operations.

At its core, the PAROMA-MED security and data privacy awareness pertains to understanding and familiarity with security and data privacy risks, threats, and established protocols within the spectrum of stakeholders involved in developing, deploying, and operating the PAROMA-MED platform. This spectrum encompasses developers, IT administrators, end-users, and other relevant parties associated with the project.

Security awareness emphasises the imperative nature of safeguarding the PAROMA-MED platform against cyber threats and attacks. It encompasses comprehending risks linked to data breaches, phishing schemes, malware infections, and analogous security vulnerabilities. Additionally, it includes the assimilation of best practices in securing the platform from these vulnerabilities.

On the other hand, data privacy awareness aims to recognise the significance of upholding the confidentiality of personal data procured, processed, and retained by the PAROMA-MED platform. This pertains to comprehending potential privacy hazards inherent in data breaches, unauthorised access, and inappropriate data handling and sharing. It underscores the understanding of optimal practices for shielding personal data, including obtaining user consent, deploying data encryption and access controls, and ensuring adherence to pertinent privacy regulations.

Effective implementation of security and data privacy awareness methodologies bears the potential to mitigate the likelihood and impact of security breaches and privacy infringements. These methodologies encompass structured training, awareness initiatives, consistent communication and reminders, and continuous monitoring and feedback mechanisms. This ensures stakeholders are equipped with current insights into the latest security and privacy threats and recommended practices, fostering a resilient security and privacy infrastructure for the PAROMA-MED platform.

1.1 Objective of this document

This document aims to report on all the security and privacy awareness concepts and models defined and developed. These concepts and models provide users with situational awareness through visual representation, which enables quick and effective responses to cyber-attacks and continuous monitoring of the current privacy posture. This document reports on the first iteration of the concepts and models defined and developed and a prototype GUI for consent management as a core functionality of the overall situational awareness GUI.

Some of the presented concepts in this deliverable are realised as-a-Service in work package WP3 and as part of the PAROMA-MED Network and Interconnect Platform (T2.2) as well as the application and data platform (T2.3 and T2.4), and therefore described in more detail in the respective deliverables D2.2, D2.3, D2.4, and D3.1, D3.2.

The second iteration of the concepts, models and the prototype GUI will be presented in deliverable D3.4.

This document is organised in the following structure:

- Common security and data privacy concepts and models (Section 2)
- Security awareness concepts and models (Section 3)
- Data privacy awareness concepts and models (Section 4)
- Prototype GUI for consent management/situational awareness (Section 5)
- Conclusions (Section 6)

Individual concepts are at a different development stage at the moment of this writing. In the first iteration, the focus has been on handling consent management (Section 5). The development and integration of training and workshop material (Section 3.1 and 4.1) as well as mechanisms for threat modelling and risk assessment (Section 3.2 and 4.3) will be reported on in the next iteration of this deliverable.

2 Concepts and Models

Security and data privacy awareness concepts and models are fundamental frameworks that empower individuals and organisations to understand, manage, and mitigate cybersecurity and data protection risks. These frameworks serve as principles for cultivating a proactive stance towards safeguarding sensitive information and ensuring compliance with regulatory standards. In the following, common security and data privacy awareness concepts and models are outlined concerning the Fast Healthcare Interoperability Resources standard (FHIR) [3] and the NIST Security and Privacy Framework [4][5]. The PAROMA-MED platform follows these core concepts and models that are either inherent to the platform's architecture or implemented and offered as a service within the respective work package components (WP2 and WP3) [2]. Additionally, the PAROMA-MED GUI for situational awareness enables stakeholders to understand and manage the platform's security and data privacy posture clearly and intuitively.

2.1 Data Exchange Principles

Data exchange principles are fundamental guidelines and standards governing the secure and efficient information sharing between different entities or systems. These principles outline the core concepts and practices that should be adhered to when transferring data to ensure its accuracy, integrity, confidentiality, and proper utilisation. Data exchange principles help to establish a common framework for data sharing while maintaining privacy, security, and interoperability.

The Fast Healthcare Interoperability Resources standard (FHIR) has inherent fundamental data exchange principles designed to ensure the secure and seamless sharing of healthcare information while upholding data privacy and integrity.

FHIR employs **standardised data formats**, such as JSON and XML, ensuring consistency in data representation. Security awareness entails recognising the importance of using these formats to promote interoperability while implementing measures to prevent data manipulation or tampering. FHIR also supports **secure communication protocols**, like HTTPS, to encrypt data during transmission, safeguarding it from interception by unauthorised parties. In addition, strong **authentication and authorisation** mechanisms are promoted to verify the parties' identities in data exchange and ensure that only authorised entities have access to sensitive information. Moreover, FHIR's **resource access control mechanisms** ensure that only authorised individuals can access and modify specific healthcare data resources. This principle emphasises the need for role-based access controls to prevent unauthorised access. Another core principle is **data minimisation**, where only the minimum necessary patient information is shared to accomplish specific healthcare functions, reducing the potential risk of exposing sensitive data [6].

2.2 Consent and Privacy Management

Consent and Privacy Management, within the context of security and privacy awareness, encompasses practices and mechanisms that ensure the responsible handling of sensitive data during data exchange. It involves adhering to patient preferences, complying with privacy regulations, and maintaining an approach to safeguarding individuals' privacy rights.

Using FHIR consent resources allows patients to control how their data is shared and accessed. FHIR supports granular consent management where patients can specify which data elements

can be shared, enabling them to manage the extent of data disclosure. Stakeholders must be aware of FHIR's consent resources and how they allow patients to express their consent preferences, such as specifying who can access their data and for what purpose. Prioritising the patients' preferences, healthcare providers and organisations should respect these preferences and only share data in line with patient consent.

PAROMA-MED supports consent management with the security and data privacy awareness dashboard developed in WP3 and detailed in Section 5. It allows patients to change their consent preferences at any time, translated into access control policies that systems within the platform must adhere to.

2.3 Risk Management

Privacy risk management plays a critical role in healthcare data exchange, where the convergence of FHIR principles and NIST's security and privacy framework mandates a thorough approach to protect individuals' sensitive information. Privacy risk management involves **identifying**, **assessing**, and **mitigating** potential threats to the confidentiality and integrity of patient data during its life-cycle. PAROMA-MED follows an approach to proactively address vulnerabilities and implement controls to minimise the risk of unauthorised access, data breaches, and improper use of personal information. This approach, guided by a fusion of FHIR's patient-centric consent mechanisms and NIST's rigorous risk assessment methodologies, empowers healthcare entities to uphold privacy rights, adhere to regulatory obligations, and cultivate an environment of trust and ethical data handling within the dynamic realm of healthcare data exchange. Control implementation is mainly detailed in the Access and Privacy Control Architecture and Models deliverable D2.1.

2.4 Security Controls and Privacy Safeguards

In healthcare data exchange, the convergence of FHIR principles and NIST's security and privacy framework underscores the importance of robust security controls and privacy safeguards. These measures are essential to fortify sensitive patient information's integrity, confidentiality, and availability.

By implementing a **comprehensive suite of security controls**, PAROMA-MED can proactively manage risks, enforce access restrictions, and prevent unauthorised data breaches. Concurrently, privacy safeguards ensure that individuals' data is handled responsibly, minimising the potential for data misuse or exposure. These combined efforts, guided by FHIR's patient consent management and NIST's security guidelines, create a resilient ecosystem where data is shared securely, patients' privacy preferences are respected, and healthcare entities fulfil their ethical and regulatory obligations in the data exchange landscape. PAROMA-MED offers its comprehensive suite of security controls and privacy safeguards as a service. This innovative approach reflects a commitment to empowering healthcare entities with an adaptable and dynamic solution. By encapsulating FHIR's **patient-centric consent management** and NIST's **security and privacy principle**s, PAROMA-MED ensures that security controls are seamlessly integrated, and privacy safeguards are rigorously enforced. As-a-service delivery streamlines implementation and provides ongoing **monitoring**, updates, and **adaptability** to evolving threats and regulations.

3 Security Awareness

Security awareness concepts and models play a pivotal role in fortifying the security and privacy posture of the PAROMA-MED platform, especially when considering the interoperability aspects provided by the FHIR standard and the guidance provided by the NIST Security and Privacy Framework. By integrating FHIR-specific security awareness and NIST's Security and Privacy Framework concepts into the PAROMA-MED platform, stakeholders will be equipped with the knowledge and tools needed to navigate the intricate landscape of healthcare data interoperability while upholding robust security and privacy standards.

3.1 Security Training and Workshops

As a security awareness concept, PAROMA-MED offers training sessions and workshops to educate developers, IT administrators, and end-users about FHIR's security considerations and NIST's framework. This covers secure API implementation, data encryption, authentication mechanisms, and incident response. By providing stakeholders with targeted insights into FHIR's data exchange principles and NIST's security framework, security training and workshops fortify participants with a profound understanding of data protection, risk mitigation, and incident response. This educational investment equips developers, administrators, and end-users alike with the skills to navigate the intricate landscape of healthcare data security effectively.

Moreover, offering security-by-design APIs based on a security-policy framework supports application developers by guiding them to implement security best practices from the outset. The situational awareness GUI (Section 5) provides dedicated sections for educational resources, tutorials, and guides on security best practices, offering developers and stakeholders a convenient place to access security training materials.

3.2 Threat Modelling and Risk Assessment

The PAROMA-MED SECaaS solution's security-policy framework encompasses various quality of security levels, reflecting the concept of risk awareness and risk management. This approach ensures that different applications are protected according to their specific risk profiles. This enables stakeholders to perform threat modelling exercises that identify potential security and privacy risks in the context of FHIR data exchange and the NIST framework's risk assessment methodologies to evaluate and prioritise these risks. The continuous risk assessment conducted by the SECaaS solution, leveraging rich contextual and behavioural data, aligns with privacy risk management principles. This ongoing assessment helps identify potential privacy risks associated with data exchange and usage, enabling proactive mitigation. The situational awareness GUI includes visualisations that display the results of the continuous risk assessment, helping stakeholders identify potential privacy risks in real time and enabling proactive risk management.

3.3 Security Controls and Privacy Safeguards

The security controls and privacy safeguards implemented within the PAROMA-MED platform foster a secure and privacy-respecting healthcare data exchange environment. These measures encompass a range of comprehensive solutions, including security-by-design APIs, a novel security-policy framework, and a Security Control Plane featuring a Security Controller and Security Agents as detailed in the Access and Privacy Control Architecture and models

deliverable D2.1. The platform offers encryption, watermarking, and crypto-watermarking services (WP3, D3.1). By seamlessly integrating these components, the platform ensures that data is exchanged with confidentiality and integrity. This holistic approach also encompasses risk assessment, incident detection and mitigation services, continuous monitoring, and compliance assurance, allowing stakeholders to actively safeguard sensitive patient information, adhere to regulatory requirements, and cultivate a culture of security awareness within the dynamic landscape of healthcare data exchange. The situational awareness GUI provides an overview of the security controls and privacy safeguards implemented within the applications. It can display information about encryption, watermarking, and other security mechanisms.

4 Data Privacy Awareness

When coupled with the FHIR standard and the NIST Security and Privacy Framework, data privacy awareness concepts and models establish a robust foundation for safeguarding sensitive healthcare information within the PAROMA-MED platform. These concepts and models ensure that stakeholders are well-versed in the intricacies of data privacy, facilitating compliance with regulations and the ethical handling of patient data.

4.1 Data Privacy Training and Workshops

As a core data privacy awareness concept supported by the PAROMA-MED platform and situational awareness GUI, data privacy training and workshops focus on educating stakeholders about data protection principles, emphasising compliance with regulations like the General Data Protection Regulation (GDPR) [6]. Moreover, PAROMA-MED offers educational resources via the GUI specifically to educate stakeholders about FHIR's principle of data minimisation, stressing the importance of only sharing and collecting the minimum necessary patient information to fulfil healthcare functions and highlighting FHIR's consent resources and capabilities for managing patient consent preferences, enabling stakeholders to understand and implement granular data sharing controls.

The situational awareness GUI also hosts a dedicated section containing educational materials, guides, and interactive tutorials related to data privacy and GDPR compliance. These resources help stakeholders, including developers, administrators, and end-users, grasp the nuances of data protection requirements.

4.2 Consent and Privacy Management

Consent and privacy management, a fundamental data privacy awareness concept fortified by the PAROMA-MED platform and its situational awareness GUI, centres around empowering stakeholders to uphold data privacy while adhering to FHIR principles. The platform's GUI is a hub where individuals' control over their data is respected, aligned with the FHIR standard's emphasis on patient-centric data sharing. Users can seamlessly manage their consent preferences within the GUI, dictating who accesses their data and for what purposes. This robust consent management mechanism harmonises with FHIR's granular data-sharing approach, ensuring that only necessary data is exchanged, adhering to patients' choices. The GUI also facilitates the visualisation of data flows, privacy impact assessments, and anonymiation techniques, offering transparency into how personal data is processed and protected. Overall, consent and privacy management through the PAROMA-MED platform and GUI underscores a commitment to preserving data privacy rights, reinforcing stakeholders' understanding of FHIR's consent resources, and cultivating an ethical and compliant data exchange within the healthcare ecosystem.

4.3 Privacy Impact Assessments (PIAs)

Privacy Impact Assessment (PIA) [7], as a pivotal data privacy awareness concept enriched by the PAROMA-MED platform and its situational awareness GUI, aligns with the NIST security and privacy framework. The platform's GUI serves as a conduit for stakeholders to comprehend and implement PIAs, ensuring that privacy risks are methodically evaluated when exchanging healthcare data. The GUI provides tools to assess the potential impact of data processing activities on individuals' privacy rights, in line with NIST's risk assessment

methodologies. Stakeholders can navigate the GUI to assess, identify privacy vulnerabilities, and develop strategies for appropriate mitigation measures. This integration of PIAs within the platform showcases a dedication to proactive privacy management, where stakeholders systematically consider privacy implications, align data processing activities with regulatory requirements, and uphold individuals' privacy preferences.

5 GUI for Situational Awareness

In the context of the PAROMA-MED hybrid-cloud delivery framework, a Graphical User Interface (GUI) for situational awareness serves as a central hub where stakeholders can gain comprehensive insights into the security and privacy landscape of the healthcare ecosystem. This GUI facilitates intuitive interaction, enabling users to swiftly comprehend complex data, make informed decisions, and take prompt actions to address potential threats and privacy concerns. Following the security and data privacy concepts outlined in Section 3 and Section 4, the PAROMA-MED situational awareness GUI supports stakeholders mainly in conducting **security and data privacy training**, management of **security controls and privacy safeguards**, **consent and privacy management** and **privacy impact and risk assessment**.

5.1 Key Features of the Situational Awareness GUI

Real-time Visualization: The GUI provides dynamic, real-time visualisations that depict the current status of security and privacy elements within the PAROMA-MED platform. These visualisations include graphs, charts, and heatmaps representing data flows, access patterns, and potential threats.

Threat Dashboard: A dedicated section offers an overview of detected threats, vulnerabilities, and anomalies. Users can quickly identify and categorise potential risks, enabling them to prioritise responses effectively.

Risk Assessment and Impact Analysis: Users can access risk assessments and analyses associated with specific threats or vulnerabilities. The GUI presents risk scores, potential consequences, and recommended actions to mitigate risks.

Privacy Posture Indicator: A visual indicator displays the platform's current privacy posture, reflecting compliance with regulatory standards such as GDPR and relevant healthcare privacy regulations. Users can quickly gauge the platform's adherence to privacy requirements.

Interactive Data Flows: Visual representations of data flows across federated cross-border environments offer insights into how patient data is exchanged between different entities. Users can track data movement and identify potential points of concern.

Event Timeline: A chronological display of security events and incidents provides a historical perspective. Users can review past incidents, resolutions, and lessons learned, aiding in improving security measures.

Customisable Alerts: Users can set personalised alerts for specific thresholds, events, or changes in the security and privacy landscape. These alerts ensure timely notifications and responses to critical situations.

Privacy Compliance Monitoring: A dedicated section enables monitoring of privacy compliance activities, including consent management, data access requests, and data retention policies. Users can ensure alignment with data protection regulations.

5.2 User Interaction and Navigation

Intuitive Navigation: The GUI offers an intuitive navigation structure, allowing users to move between different sections, dashboards, and visualisations seamlessly.

Drill-Down Capabilities: Users can drill down into specific visualisations for deeper insights. Clicking on elements reveals additional details and context for more informed decision-making.

Interactive Controls: Interactive controls and filters empower users to customise visualisations according to their preferences, focusing on specific time frames, data categories, or threat types.

Responsive Design: The GUI has a responsive layout, ensuring optimal usability across various devices and screen sizes, including desktops, tablets, and smartphones.

By offering a user-friendly and information-rich GUI for situational awareness, the PAROMA-MED framework empowers stakeholders to proactively monitor, analyse, and respond to security and privacy challenges within the healthcare ecosystem.

5.3 Consent Management

Within the situational awareness GUI of the PAROMA-MED platform, consent management emerges as a pivotal feature, facilitating the thorough handling of healthcare data-sharing preferences. This feature is a central hub for stakeholders, allowing them to exercise granular control over their consent settings. Whether individuals are patients or platform users, they can effortlessly configure their consent preferences, ensuring that data access aligns with their intentions. Changes in consent preferences are instantly updated, enabling swift adjustments to data-sharing permissions.

The system maintains a comprehensive log that diligently records consent-related activities, serving as an audit trail to confirm compliance with regulatory standards. Furthermore, integrating consent management with privacy impact assessments (PIAs) encourages users to conduct checks when altering their consent preferences. This empowers them to evaluate the potential privacy implications of their choices.

Stakeholders can set up alerts and notifications to stay informed about alterations in consent settings and data access requests. Visual representations illustrate data flows in line with consent preferences, giving users a visual understanding of how their choices impact data exchange. Moreover, consent management is coupled with security controls via security and privacy policies expressed in the Open Policy Agent (OPA) policy language to ensure that data access adheres to configured consent preferences. Access requests undergo validation against consent settings before being granted, enhancing security.

The GUI's data minimisation efforts promote an understanding of the necessity of data for specific purposes, in harmony with GDPR and privacy-by-design principles. It also supports compliance tracking, offering insights into aligning data-sharing practices with regulatory requirements, such as GDPR.

In addition to these features, stakeholders can create consent templates for common scenarios, simplifying the consent configuration process and promoting consistency in data-sharing preferences. In essence, consent management within the situational awareness GUI empowers stakeholders to assert control over their personal data during healthcare data exchange, fostering a culture of transparency, privacy, and compliance within the PAROMA-MED platform.

6 Conclusions

In the landscape of healthcare data exchange, the convergence of FHIR and NIST security and data privacy concepts harmonises seamlessly with the innovation brought forth by the PAROMA-MED platform's situational awareness GUI and SECaaS solution. This dynamic synergy fosters a comprehensive approach to security and data privacy awareness, equipping stakeholders with the tools and knowledge they need to navigate the complexities of the digital healthcare domain.

The FHIR standard's emphasis on patient-centric data sharing finds resonance in the platform's GUI, where intuitive interfaces and granular controls empower consent and privacy management. Stakeholders, including patients, developers, and administrators, can actively manage data-sharing preferences and ensure adherence to regulatory obligations. This concept extends to privacy impact assessment, where the GUI guides stakeholders through evaluating potential privacy risks, allowing them to align data processing activities with ethical standards.

Simultaneously, the principles set forth by the NIST security and privacy framework are implemented within the platform. Security controls and privacy safeguards are seamlessly integrated, ensuring sensitive patient information's confidentiality, integrity, and availability. Stakeholders benefit from the GUI's visualisations and real-time monitoring, providing insights into applications' security posture and compliance status.

At its core, the situational awareness GUI is a beacon of empowerment. It supports stakeholders in conducting security and data privacy training, enabling them to navigate a landscape enriched by educational resources and interactive tutorials. The GUI also empowers stakeholders to proactively manage security controls and privacy safeguards, shaping an environment where the highest data protection standards are upheld.

Towards a secure and privacy-respecting healthcare data exchange ecosystem, the PAROMA-MED platform's situational awareness GUI allows harmonising innovative technology with comprehensive security and data privacy awareness concepts. It bridges knowledge, practice, and innovation, ensuring stakeholders can navigate the complexity of healthcare data exchange with confidence, ethics, and a profound respect for patient privacy.

References

[1] https://paroma-med.eu/ PAROMA-MED Website, 2023

[2] https://paroma-med.eu/dissemination/deliverables/ PAROMA-MED Deliverables, 2023

[3] https://hl7.org/fhir/ HL7 FHIR Release 5, 2023

[4] https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf NIST Privacy Framework Version 1.0, 2020

[5] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.ipd.pdf NIST Cybersecurity Framework 2.0, 2023

[6] https://gdpr-info.eu/ General Data Protection Regulation (GDPR), 2018

[7] https://iapp.org/media/presentations/12DPC/DPC12_PIA_PPT.pdf The state of the art in privacy impact assessment, David Wright, 2012

Annex A Consent Management Views

The following shows the first prototype implementation views of the consent management feature within the situational awareness GUI.

A.1 Dashboard View

The main dashboard view provides a summary of the user's consent settings, such as the number of services that require consent, the types of data being collected, and the purpose for which it is being used.

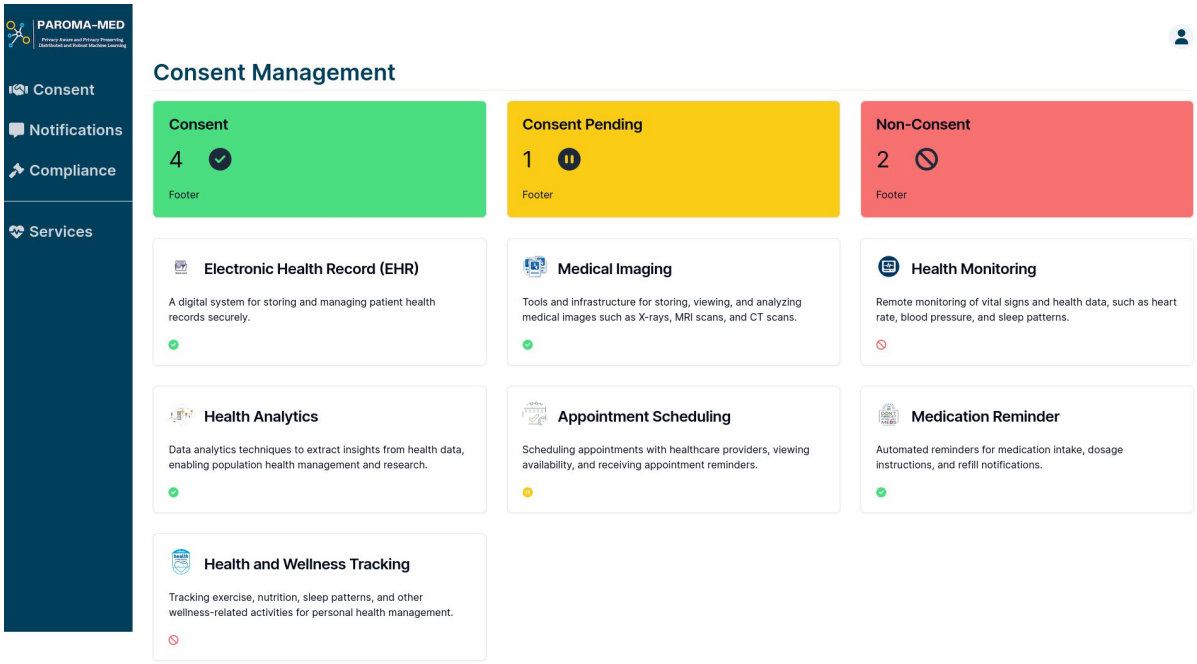

Figure 1: Situational Awareness GUI – Consent Management Dashboard

A.2 Services View

The service list view displays a list of all the services that require user consent. Users can modify the user's consent settings for each service.

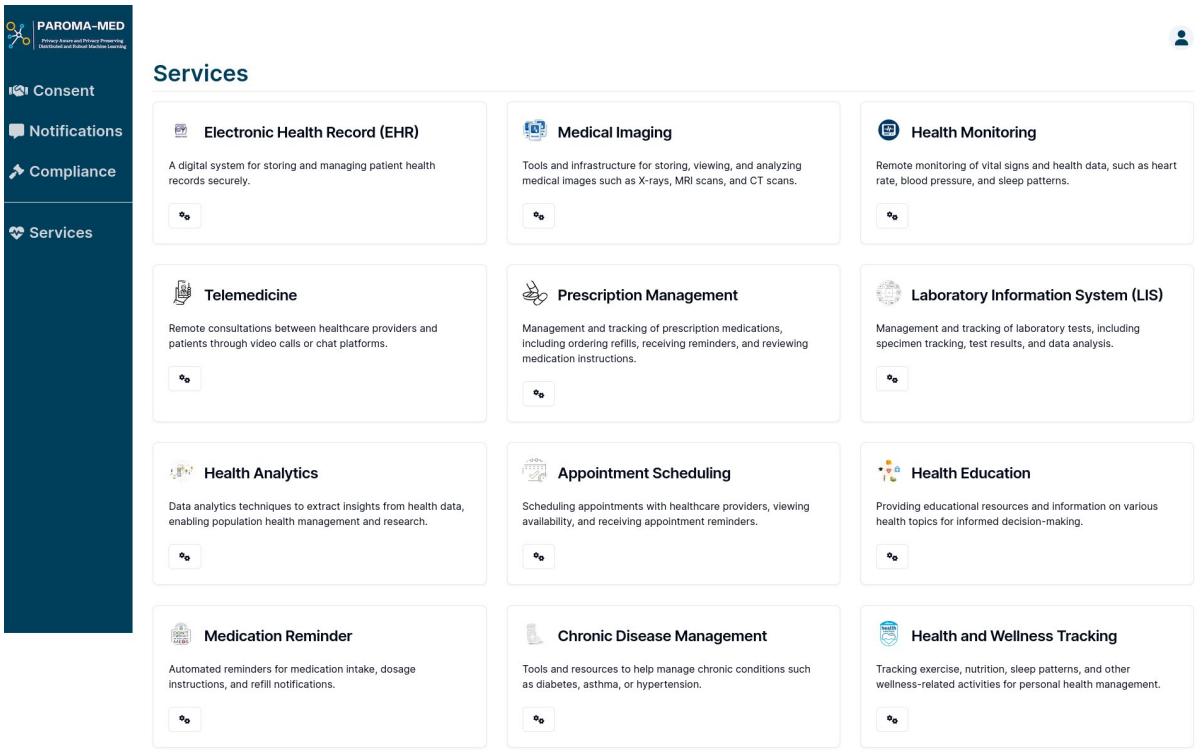

Figure 2: Situational Awareness GUI – Consent Management Service Overview

A.3 Notification View

The notification view allows users to receive notifications and modify their consent. Users can also revoke their consent or modify their settings at any time.

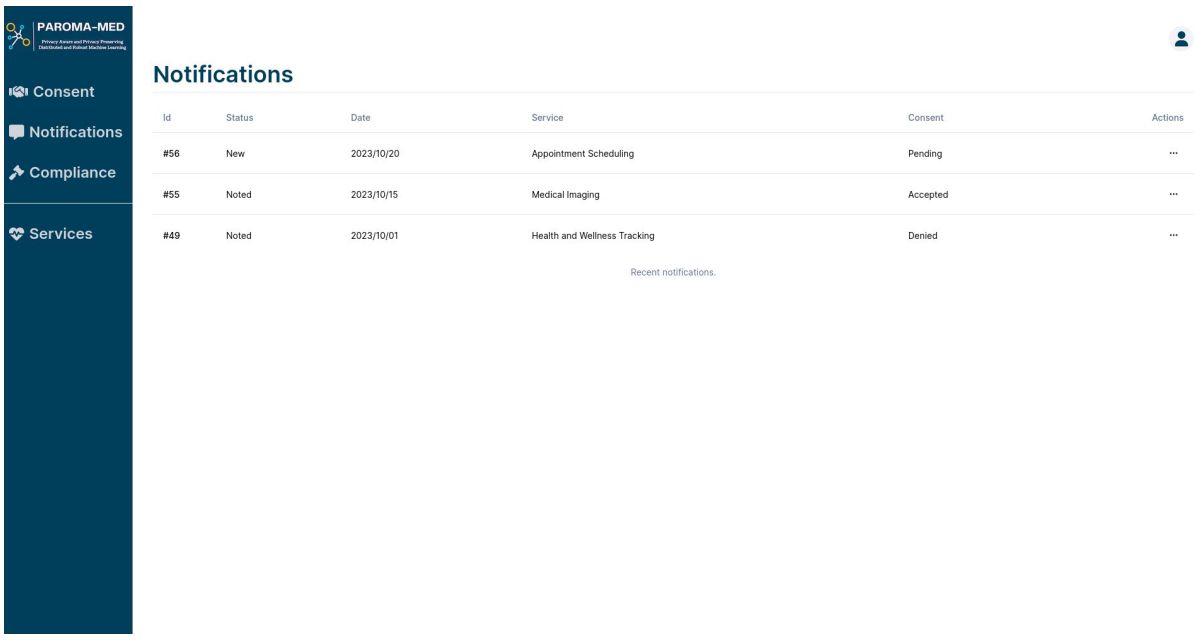

Figure 3: Situational Awareness GUI – Consent Management Notification View

A.4 Compliance View

The compliance view shows the metrics/privacy posture of PII related to a user, e.g. the compliance of a request to consent with regards to the GDPR.

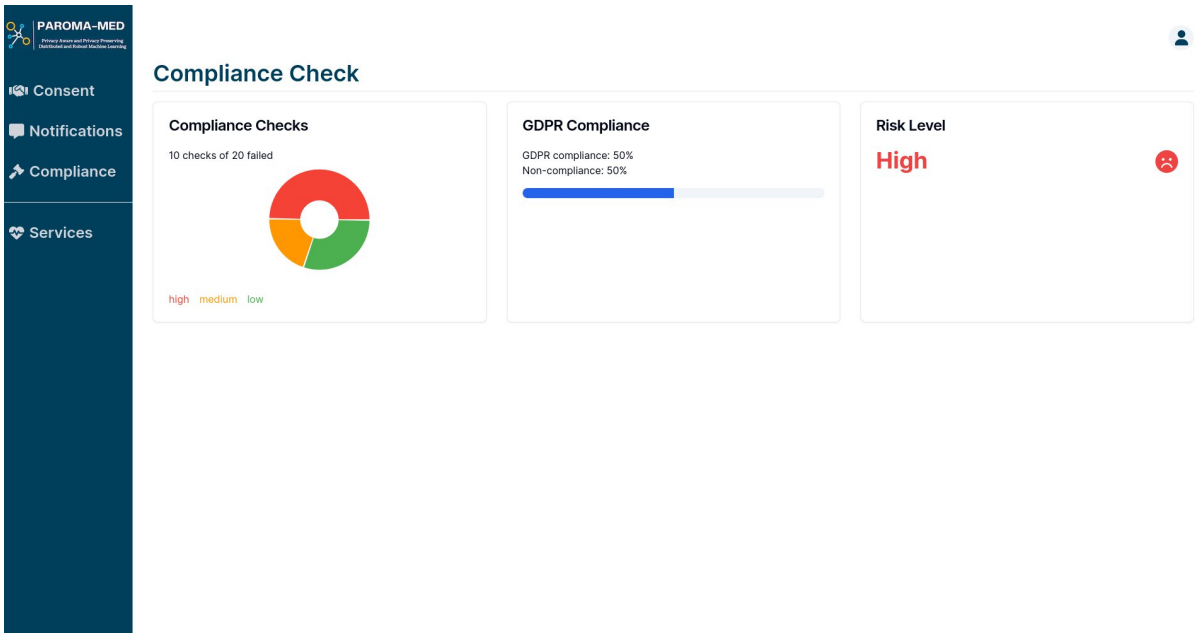

Figure 4: Situational Awareness GUI – Compliance View

A.5 Consent Management per Service View

The consent management per service view allows user to associate patients with a consent form (written or electronic) and a specific service/for a specific purpose.

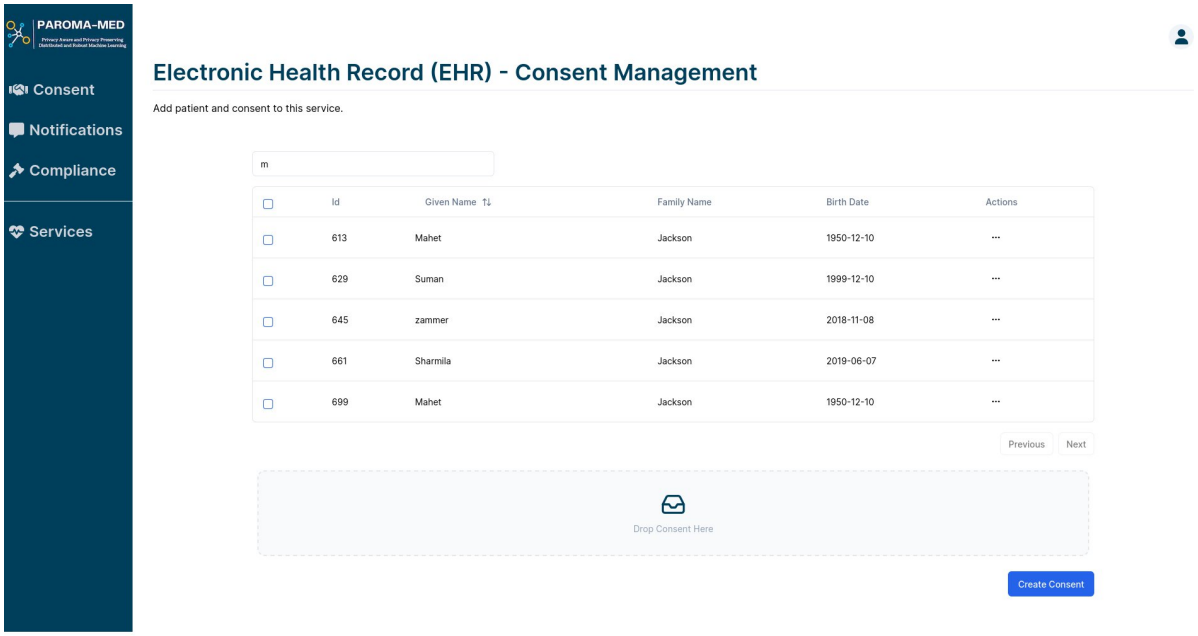

Figure 5: Situational Awareness GUI – Consent Management per Service View

[end of document]

