C.I.R.M.

Delivery of maritime telemedical assistance via an expert system called Marine Doctor

PRIVACY POLICY

C.I.R.M.

Centro Internazionale Radio Medico ("C.I.R.M.") in collaboration with International Transport Federation (ITF) Trust respect your privacy concerns. References in this document to "C.I.R.M.", "we", "us", and "our" are references to C.I.R.M., the entity responsible for collecting and processing seafarers' personal information.

This Privacy Policy describes the types of personal information we obtain, how we may use that personal information, with whom we may share it and how you may exercise your rights regarding our processing of that information. The Privacy Policy also describes the measures we take to safeguard the personal information we obtain along with our contact details.

This Privacy Policy applies to the personal information we obtain through C.I.R.M. websites, products, services, desktop and mobile apps and other tools offered by C.I.R.M. centre; offline collection including interactions, surveys, questionnaires and evaluations ("Offline Channels"); and third-party sources including related partners involved with service delivery (collectively, the "Offerings").

In connection with providing support, tele-support and other services, C.I.R.M. processes certain data maintained in the environment that it may access to perform teleconsultation, support services and research and analytics ("patient content") on behalf of and at the direction of its customers and partners, as well as log data (e.g., regarding access and authentication requests) that they collect for analysis and security purposes across our services. Our use of Customer Content and Log data is driven by our Customer Agreements and not governed by our Privacy Policy.

The information we collect through our customers and partners' use of our platform called Marine Doctor (such as names, address, employee details etc.) and through our offline interactions with customers and partners is subject to this Privacy Policy.

In our co-branded offerings in which a third party is involved, we will sometimes share or jointly collect customer data related to those transactions with that third party.

The present Privacy Policy is compliant with the European Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data and the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR)

C.I.R.M.

Contents

A. Introduction	4
B. Features of the System	4
C. Technology	5
D. Data protection	5-7
E. Platform summary	8
F. GDPR Privacy Policy	8-9
G. GDPR Compliance Review	10

C.I.R.M.

A. Introduction

C.I.R.M. uses a dedicated application to record, manage and track the medical requests received from vessels. The application is named Marine Doctor (MD). This application integrates with the other applications to provide a seamlessly connected healthcare framework for seafarers.

At the time of a Medical Request, a minimum medical data referral form can be used by Captain to capture the basic information required for the doctor to make an informed medical recommendation. To guarantee the best assistance, it is recommended to use the software MD as guidance in requiring medical advice.

B. Features of the System

1. Automatically sort incoming Medical Request (email) from the Vessel
2. Once the vessel is automatically sorted the Medical List (based on the Flag State and information provided) is visible to the Doctor on duty.
3. The medical request questionnaire form serves as a guideline for Captains to ensure all relevant information is captured in the first instance. This helps quicken the response time.
4. Seafarer requiring medical assistance is easily identified by using the SHIP ID and which is captured in the Medical Request.
5. All correspondence on the medical event is captured in the system. This is extremely helpful if P&I documentation is required and also increases the transparency of the service being provided.
6. All medical events are classified by WHO– ICD 10 codes which provide the basis for analysis and health prevention initiatives later.
7. Secure system with all required Data Protection Protocols and settings to comply with required regulations.
8. This system is fully integrated with a sophisticated telemedicine case from the testing ships. The availability of ships for MD testing allows the transmission of biomedical data guaranteeing the delivery of high quality a distance medical assistance.

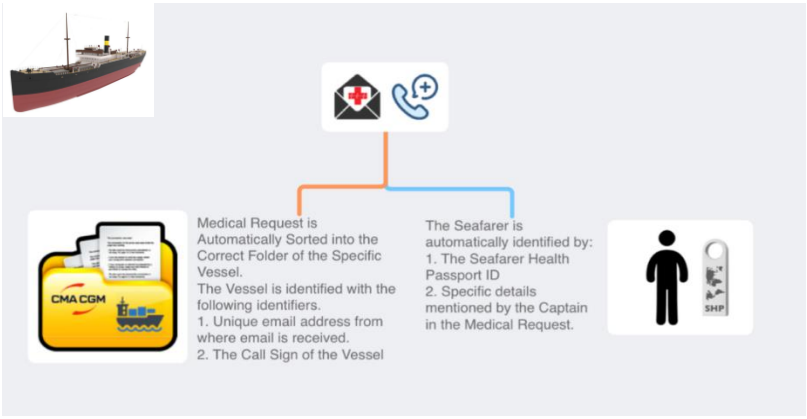
C. Technology

The MD and biomedical data transmitted through the ship computers are accessible only to the C.I.R.M. Doctors that will be replying to the medical requests from the ship. The application is run locally in C.I.R.M. premises in Rome, remote access from doctors is only possible via secured VPN. The Database is housed at C.I.R.M. premises and complies with relevant regulations.

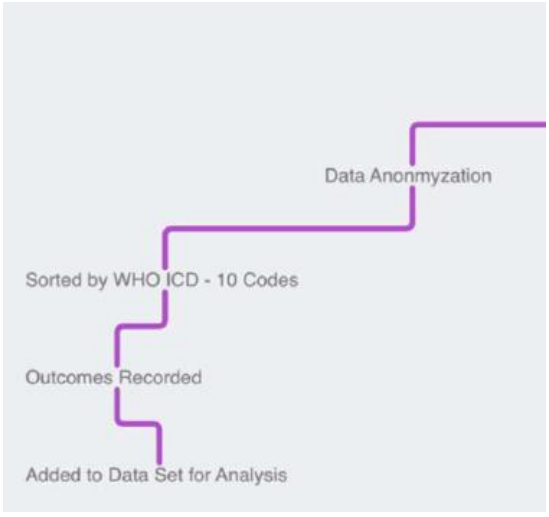
D. Data Protection

How are the data processed?

Most information that enters the system is automatically sorted by the intelligent system.



Journey of the data



How do we protect data?

We maintain administrative, technical and physical safeguards, consistent with legal requirements where the personal information was obtained, designed to protect against unlawful or unauthorized destruction, loss, alteration, use or disclosure of or access to, the personal information provided to us through the channels.

Do we share your information with third parties?

Not at all. The information collected is purely for providing Medical Support services to the seafarers. Data is pseudonymized for research and analytics.

Data can be shared with a specialist for second opinion medical advice if the need arises for medical events involving the individual.

Software Security Checklist

	YES	NO
Are domain names secured	X	
Make sure critical services are secured?	X	
Make sure email is secured	X	
Do you share WiFi		X
Are your non-tech employees connected on the same server as Tech employees?		X
Have a public security policy	X	
Have an internal security policy	X	
Have a security incident response plan	X	
Is everyone trained on best practices for data security?	X	
Is 2 Factor Authentication used in your services?	X	
Does the team lock their machines while away?	X	
Are accounts or computers shared?		X

Use Centralized account management	**X**	
Do you use SSL for your website / online applications	**X**	
Do you review basic website / online security	**X**	
Are Regular back-ups taken?	**X**	
Restrict internal services by IP addresses (ISP, VPN etc.)	**X**	
Keep a list of servers	**X**	
Watch for unusual patterns in your metrics	**X**	
Protocol on how to redeploy infrastructure from scratch	**X**	
Is there are code review checklist	**X**	
Use a static security code analysis tool		**X**
Maintain backlog of security concerns in your issue tracking tool	**X**	
Use a secure development life cycle	**X**	
Application Check		
Run it unprivileged	**Not Applicable**	Desktop-based application *
Monitor your dependencies	**X**	
Use real-time protection service	**X**	
Hire an external penetration testing team		**X**
Enforce a password policy	**X**	
Monitor users suspicious activities	**X**	
* Our platform and code already use advanced security mechanisms including encryption.		

E. Platform Summary

TMV MAP

C.I.R.M.

User: C.I.R.M. ONLY
Access: Closed Platform for C.I.R.M. only.
Security: Username, Password, 2FA, Secure VPN, restricted IP and MAC Address access
Data Location: Physical Server at C.I.R.M. Headquarters

F. GDPR Privacy Policy

Obtaining personal information

We will collect and compile seafarers' details, including name, nationality, Date of Birth, e-mails, telephone calls, health records, treatment and medications, test results, X-rays, etc. and any other relevant information which will enable us to deliver effective medical care.

How we will use patient information

Patient data is collected to provide direct healthcare services. However, if required by law, we can disclose this information, provided you give consent or is justified in the public interest. The public interest includes the safety of the other crew on board. Our effort to provide health statistics and trends will involve using your medical data anonymously. The data may include demographic data, such as date of birth, and information about your health which is recorded in coded form; for example, the clinical code for diabetes or high blood pressure. Processing your information by obtaining your consent ensures that we comply with Articles 6(1)(c), 6(1)(e) and 9(2)(h) of the GDPR.

Maintaining confidentiality and accessing your records

We are committed to maintaining the confidentiality and protecting the information we possess about you. We adhere to the General Data Protection Regulation (GDPR).

Seafarers have a right to access the information we possess about them, and if they wish to access this information, they will need to complete an Applicant Access Request (AAR) form which will give them access to the Health Passport wherein all the information can be found.

Furthermore, should the seafarer identify any inaccuracies, he/she can correct the inaccurate data by contacting us.

Risk stratification

Risk stratification is a mechanism used to identify and subsequently manage those seafarers deemed as being at high risk of requiring urgent or emergency care. Usually, this includes patients with any chronic or long-term conditions. Seafarers' information is collected by some sources, including information shared by the employer, recruiting doctor etc.; this information is processed electronically and given a risk score which is saved along with the information to ensure that you receive the most appropriate care in the Golden Hour.

Retention periods

Following general practices, seafarer healthcare records will be retained for 10 years after his/her's death, or if the seafarer migrates from our service, for 10 years after the date of migration.

In case of questions

Should the seafarer have any questions about our privacy policy or the information we hold about them, they can contact the data controller via email at datacontroller@cirm.it. GP practices are data controllers for the data they hold about their patients.

Complaints

In an unfortunate event that if seafarer does not happy with any element of our data-processing methods, we encourage them to write to the data controller at the same address mentioned above.

Changes to our privacy policy

We review our privacy policy periodically and any updates will be published systematically.

G. GDPR Compliance Review

Review	YES	NO
Is informed consent taken for storing individual information	X	
Do we have a legal basis for storing the information?	X	
Do we have adequate security measures in place for data safety?	X	
Have we appointed a Data Protection Officer and Controllers?	X	
Is the staff trained with the requirements of GDPR?	X	
Do you have a continuous review protocol for security, data stored and handling customer requests?	X	