Welcome to Steward's Website Privacy Notice

The General Data Protection Regulation (**GDPR**) is a European Union (**EU**) law. The GDPR has been implemented in the Malta through the new Data Protection Act (Chapter 586 of the Laws of Malta). These laws are defined in this notice as the **Data Protection Laws**.

The Data Protection Laws applies to 'personal data', which means any information that relates to an identified or identifiable natural person. It does not include data that has been anonymised so that the individual can no longer be identified (anonymous data).

This Privacy Notice applies to the processing of personal data collected through our website, from our patients and suppliers; and in relation to the delivery of healthcare services in Malta.

1. Important Information and who we are

Steward Malta Limited (C 70546) and its subsidiaries including Steward Malta Management Ltd (C 70624), Steward Malta Assets Ltd (C 70625) and Steward Malta Personnel Limited (C 81862) (hereinafter collectively referred to as the "Steward" or "we") are committed to protecting the privacy and security of your personal information. In terms of Data Protection Laws, Steward is the "data controller". This means that we are responsible for deciding what personal data to collect about you, why we collect it and how we use it.

We work closely with other healthcare providers who may also be data controllers of your personal data.

We respect your privacy and are committed to operating the highest standards when it comes to protecting your personal data. We also comply with all applicable medical confidentiality guidelines including those published from time to time by regulators and professional bodies.

We will process your personal data "fairly", "lawfully" and "transparently". This means (i) we will be open and transparent about how personal data is used (ii) we will handle data in line with how we say we are going to handle data and (iii) we will only use or process personal data in accordance with the law. To fulfil these requirements, we set out in this Privacy Notice how Steward collects, uses, retains and discloses personal data.

It is important that you read this Privacy Notice so that you understand how and why we are collecting and/or processing personal data about you. If you have any questions, please contact us at the address provided below.

Data Protection Officer

Steward has appointed a data protection officer (DPO) who is responsible for overseeing questions in relation to this Privacy Notice. If you have any questions about this Privacy Notice, including any requests to exercise your legal rights, please contact the DPO at:

Address: 115A, Floor 5, Msida Valley Road, Birkirkara BKR 9024, Malta
Email: dpo@stewardmalta.org

2. How is Personal Data Collected?

We collect your personal data in a number of ways. These include:

i. *Direct interactions.*
You may give us your identity and contact data by filling in forms or by corresponding with us by post, phone, online or in person.

ii. *Other health care professionals and health care providers*
Steward works in partnership with healthcare professionals and other health care providers who provide healthcare services to you (for example, any other healthcare practitioner or the doctors and nurses of a particular hospital, such as Mater Dei hospital.)

Steward may collect and/or access your patient records as part of this provision of care. For example, where you are under the care of other doctors or clinicians, they may inform us of their consultation records and any observations and/or recommendations they may have for your continued care.

iii. *Your parent or legal guardian.*
Your parent or legal guardian may provide us with your information.

iv. *Cookies and Automated technologies when using our Website*
When you interact with our Website we may automatically collect information using cookies. Please see our section on cookies below.

v. *Through social media sites*

We operate social media sites, including Facebook. We may collect data in relation to any comments or feedback posted on the Steward Facebook page, which may include your personal data. Please be aware that your use of an external application (such as a social media platform) or any informational content found on external applications is subject to and governed by the privacy policies, terms, and conditions of that application.

3. The Data we collect about you

We may collect, use, store and transfer different kinds of personal data about you, which we have grouped together as follows:

i. *Identity*
This may include your name, your parents'/guardian name, age, your Maltese identity card number and your social security number.

ii. *Contact details*
This may include your address, e-mail address and phone number(s).

iii. *Technical Data*
This includes internet protocol (IP) address, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access the Website.

iv. *Usage Data*
This includes information gathered from cookies about how you use and interact with the Website.

We also process the following *special categories of personal data:*

v. *Information about your physical and mental health and patient records:*

This may include your medical records as well as information about your physical and mental functioning, any ailments, diseases or disabilities and health and genetic and biometric data.

vi. *Other sensitive data:*
This may include, race or ethnicity, religious or philosophical beliefs, political opinions, sex life, sexual orientation and, sometimes, information about criminal offences.

These special categories of sensitive personal data require a higher level of protection.

If you fail to provide personal data

Where we need to collect personal data by law, or under the terms of a contract we have with you or those who commission us to provide care, and you fail to provide that data when requested, we may not be able to provide the services to you.

4. How we use personal data and our legal basis for processing

We have set out below, in a table format, a description of the types of personal data we collect, what we use it for and our legal basis for doing so.

We will process the categories of personal data listed below for one or more of the following legal basis:

i. *Consent*
When you give us your consent to process your personal data for one or more purposes listed below
ii. *Legitimate Interests*
Processing of personal data is necessary for our legitimate interests of managing our relationship with you and administering our Website
iii. *Legal Obligations or Legal Claims*
Processing of personal data is necessary for us to comply with laws and regulations that apply to us. We may also process your personal data for the establishment exercise or defence of legal claims.
iv. *Provision of healthcare*
Processing of personal data is necessary for medical diagnosis, the provision of healthcare and management of healthcare systems and services
v. *Vital Interests*
Processing of personal data is necessary to protect your vital interests or those of another person
vi. *Performance of a task carried out in the public interest*
Processing of personal data is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested us
vii. *Public interest in the area of public health*
Processing of personal data is necessary for reasons of public interest in the area of public health

We may process your data:

Use	**Type of Data**	**Legal Basis**
To verify your identity	Identity Contact Details	Provision of healthcare
To register you on our system in order to create a patient record	Identity Contact Details	Provision of healthcare

	Information about your physical and mental health and patient records Other sensitive data	
To store your information on written records and keep our records up to date	Identity Contact Details Information about your physical and mental health and patient records Other sensitive data	Provision of healthcare
To provide care to you	Identity Contact Details Information about your physical and mental health and patient records	Provision of healthcare
To share your information with other professionals or organisations that are involved or responsible for your care	Identity Contact Details Information about your physical and mental health and patient records	Provision of healthcare
To ensure you receive the right care in the right place and at the right time (including booking appointments, referrals and follow ups)	Identity Contact Details Information about your physical and mental health and patient records	Provision of healthcare
To protect you where we have any safeguarding concerns	Identity Contact Details Information about your physical and mental health and patient records	Vital interests
To respond to your request in connection with the exercise of your rights under Data Protection Laws (for more information about your rights please see section 14 below)	Identity Contact Details	Legal obligations
Contacting you and resolving queries about your care	Identity Contact Details Information about your physical and mental health and patient records	Provision of healthcare Legal obligations

To comply with our legal and regulatory requirements and related disclosures	Identity Contact Details Information about your physical and mental health and patient records	Legal obligations
To prevent, detect and investigate crime	Identity Contact Details	Legal obligations
To improve the quality of services we provide and check and report how effective our services are	Identity Contact Details	Performance of a task carried out in the public interest
To make sure services are planned to meet patients' needs now and in the future	Identity Contact Details	Reasons of public interest in the area of public health
To ensure that our services are provided safely and in compliance with our regulatory obligations and to protect the public against dishonesty, regulatory concerns, malpractice or other serious improper behaviour (for example, investigations in response to a safeguarding concern, clinical concerns, complaints or a regulator or governmental body telling us about an issue	Identity Contact Details Information about your physical and mental health and patient records	Reasons of public interest in the area of public health
Investigating and responding to complaints or claims, complying with our legal or regulatory obligations and defending or exercising our legal rights	Contact Details Information about your physical and mental health and patient records	Provision of healthcare Legal obligation Performance of a task carried out in the public interest
To ensure that Steward acts within its contractual terms	Identity Contact Details	Legitimate Interests
To make sure that Steward gives the Maltese government value for money and high quality services	Identity Contact Details	Legitimate Interests
To answer your general queries and comments	Identity Contact Details	Legitimate Interests

To respond to you and take action when you report a problem with our Website	Identity Contact Details	Legitimate Interests
To use data analytics to improve our website, products/services, customer relationships and patient experiences	Technical Usage Data	Legitimate Interests
To review feedback and entries posted on subsections of social media platforms controlled by us	Identity Contact Details	Legitimate Interests
Managing our business: retaining patient records, maintaining accounting records, analysis of financial results, internal audit requirements, receiving professional advice (such as tax, financial, legal or public relations advice)	Contact Details Information about your physical and mental health and patient records	Special category data would not be shared in all these cases but where it is, the basis on which we would be doing so would be: Provision of healthcare Legal claims Legal obligations
Passing your records to a third party to whom we transferred part of our business or a hospital. We may need to transfer the information in order for health assessments, care and/or treatment to be provided to you. The reason we would transfer your records is to minimise the disruption to current or past patients caused by the sale or transfer and to ensure we and a new owner were able to comply with our legal obligations regarding the retention of patients' and other clients' medical records and to ensure continuity of care. Limited information may also be shared, where required, with legal and other professional advisors involved in that transaction.	Contact Details Information about your physical and mental health and patient records	Vital interests Provision of healthcare

We may also process your personal data for the establishment exercise or defence of legal claims.

We may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data. Please contact the DPO if you need details about the specific

legal ground we are relying on to process your personal data where more than one ground has been set out in the table below.

Marketing

We do not process your personal data for any marketing purposes. Should this change we will notify you in accordance with applicable laws.

Automated decision making and profiling

Automated decision-making takes place when an electronic system uses personal data to make a decision without human intervention. We do not carry out any automated decision making including profiling. Should this change we will notify you in accordance with applicable laws.

5. Do I have to consent to the processing of my data?

Health data is data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about that person's health status.

Under the Data Protection Laws, Steward does not have to obtain our patients' consent because processing health data has a lawful basis – namely the provision of healthcare.

The Data Protection Laws has expanded the existing exemption from obtaining consent. Article 6 of the GDPR sets out what is the lawful basis for processing health data. Article 6(1)(e) of the GDPR says that processing health data for providing direct care is necessary in the exercise of the official authority vested in Steward as a data controller. Article 9(2)(h) of the GDPR has put in place an exemption from obtaining a patient's/client's consent in relation to the management of health or social care services and this is why we do not need to obtain your consent to process your health data.

Steward will also comply with all applicable laws in relation to confidentiality and clinical confidentiality guidelines in relation to the sharing of any health records.

6. Confidentiality and patient's records

In addition to the protections under the Data Protection Laws, your health records may also be subject to duties of confidentiality.

7. Change of Purpose

We will only use your personal data for the purposes described in this Privacy Notice. If we need to use your personal data for an unrelated purpose, we will update this Privacy Notice and notify you in accordance with the Data Protection Laws.

8. Cookies

Cookies are small text files that are placed on your computer, smartphone or other device when you visit our website. A cookie file is stored on your device and allows us, or our third party service providers (see below) to recognise you and make your visit easier and more useful to you when you revisit our website.

Cookie	Name	Purpose
Google Analytics	_ga, _gci_au, _gid	These cookies are used to measure traffic to our website. We use the information to compile reports and to help us improve the website. The cookies collect information in an

		anonymous form, including the number of visitors to the website. Read Google's overview of privacy and safeguarding data.

To opt out of being tracked by Google Analytics across all websites, visit http://tools.google.com/dlpage/gaoptout.

Most web browsers allow some control of most cookies through the browser settings. To find out more about cookies, including how to see what cookies have been set, visit www.aboutcookies.org or www.allaboutcookies.org .

9. Data Anonymisation and Aggregation

Your personal data may be anonymised or converted into statistical or aggregated data which cannot be used to identify you, and then used to produce statistical research and reports. This aggregated data may be shared and used in all the ways described above.

10. Children

We understand the importance of taking extra precautions to protect the privacy and safety of children.

If you are a parent or guardian and would like to access, correct, delete or exercise any of your child's data protection rights, please contact us using the contact details provided in section 1 above. We may need to ask you additional information to confirm that you are the child's parent or guardian.

11. Disclosure of Personal Data

Third party recipients

We may have to share your personal data for the purposes set out in in section 4 above with:

i. those involved in your care, such as: doctors, clinicians and other health-care professionals, hospitals, clinics and other health-care providers;

ii. service providers, acting as processors who provide IT and systems administration services;

iii. people or organisations we have to, or are allowed to, share your personal data with by law for example, for fraud-prevention or safeguarding purposes, or for regulatory investigations;

iv. with your medical insurer about your treatment, its clinical necessity and its cost, only if they are paying for all or part of your treatment with us. We provide only the information to which they are entitled. If you raise a complaint or a claim we may be required to share personal data with your medical insurer for the purposes of investigating any complaint/claim;

v. a third party if we restructure or transfer our contracts, business or its assets or have a merger or re-organisation (in which case personal data we hold about our patients or visitors to the Website may be one of the assets the third party takes over);

vi. any member of our group or our affiliate companies (when we refer to company affiliates we mean all the companies in the group, including subsidiaries, holding companies or subsidiaries of such holding companies); or

vii. where necessary to comply with our obligations or as permitted by law and with our legal and other professional advisors including our solicitors and other professional consultants and advisors.

We require all third parties who process data on our behalf to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

We may share your personal data with more parties than the ones listed above. Should this be the case, we will inform you of the change in accordance with applicable laws and regulations

Transfers of personal data outside the European Economic Area (EEA)

Your personal data may be transferred outside Malta and the European Economic Area for the purposes set out above. While some countries have adequate protections for personal data under applicable laws, in other countries steps will be necessary to ensure appropriate safeguards apply to it. These include imposing contractual obligations or other safeguards to provide adequate levels of protection.

For example, we may transfer personal data to our parent company in the US for the purposes of litigation and internal or government investigations.

We take steps to ensure that, when we transfer your personal data outside the EEA, we have adequate safeguards in place in line with applicable data protection laws. For more information about this protection, please contact us at dpo@stewardmalta.org.

12. Data Security

At Steward we take our duty to protect personal data and our confidentiality obligations seriously. We are committed to taking all reasonable measures to ensure the confidentiality and security of personal data for which we are responsible, whether computerised or on paper.

Steward has also appointed a **Data Protection Officer** (DPO) who has professional experience and knowledge of data protection law, specifically in relation to the type of processing that Steward carries out.

All Steward staff handling personal data is required to undertake annual information governance training and is provided with information governance policies that they are required to read, understand and agree to follow. Steward's policies ensure the healthcare professionals who provide our services are aware of their information governance responsibilities and follow best practice guidelines ensuring the necessary safeguards and appropriate use of person-identifiable and confidential information.

[Additionally, everyone working for Steward is subject to a duty of confidentiality according to applicable laws. Information provided in confidence will only be used for the purposes advised and consented to by the service user, unless it is required or permitted by the law.]

We have put in place appropriate security measures, including encryption and using anonymisation tools where necessary, to prevent your personal data from being accidentally lost, used or accessed

in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties on a "need to know" basis. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach in accordance with applicable laws and regulations.

13. Data Retention

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

Details of retention periods for different aspects of your personal data are available in our retention policy which you can request by contacting our DPO.

14. Your Legal Rights

You have the following rights under Data Protection Laws in relation to your personal data.

Request access to your personal data. The Data Protection Laws gives you certain rights to see the information that Steward holds about you and why.

We will confirm whether we are processing your personal data and we will provide you with additional information including what type of data we have, where we collected it from, whether we send it to others, including any transfers outside the EEA, subject to the limitations set out in applicable laws and regulations. We will provide you free of charge with a copy of your personal data, but we may charge you a fee to cover our administrative costs if you request additional copies of the same information.

Request correction of your personal data. You can ask us to correct any incomplete or inaccurate data we hold about you, although we may need to verify the accuracy of the new data you provide to us.

Request erasure of your personal data. You can ask us to delete or remove personal data where there is no good reason for us continuing to process it. However, that we may not always be able to comply with your request of erasure for legal reasons, and we will let you know if this is the case, at the time of your request.

Object to processing of your personal data. You can object to the processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. However, that we may not always be able to comply with your request for legal reasons, and we will let you know if this is the case, at the time of your request.

Request restriction of processing your personal data. You can ask us to restrict the processing of your personal data in certain cases.

Request transfer of your personal data. You can ask us to transfer your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a

structured, commonly used, machine-readable format. Please note this this right only applies in certain cases.

Right to withdraw consent. You can withdraw consent at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to or for you. We will advise you if this is the case at the time you withdraw your consent.

If you wish to exercise any of the rights set out above, please contact the DPO. Contact details are above. We may ask you to provide additional information e.g. your full name, address, date of birth, ID number, etc. so that your identity can be verified.

No fee usually required

You will not have to pay a fee to exercise any of your rights. However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

In so far as it is practicable, we will notify the third parties we shared your personal data with of any correction, deletion, and/or limitation on processing of your personal data.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

Time limit to respond

We try to respond to all requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you of the reasons for the delay and keep you updated.

15. Questions?

If you have any questions about our Privacy Notice, information we hold about you or complaints about how we process your personal information please contact the DPO (contact details above). Complaints can also be made to the Information and Data Protection Commissioner https://idpc.org.mt/en/Pages/Home.aspx .

16. Changes to our Privacy Notice

We keep this processing notice under regular review and we will place our updated Privacy Notice in a visible place. This notice was last updated in August 2019.