Information Governance Policy

Updated July 2020 –

- **Subject Access Requests Policy / Procedure (Appendix A)**
- **Social and Digital Media Privacy Policy & Procedure**
- **Breach Notification Policy / Procedure (Appendix B)**
- **Fair Processing Notice (Appendix C)**
- **The Rights of the Data subject**

Contents

1. Introduction

This policy documents provides an outline as to how personal, sensitive and confidential information is managed across Lifestar Medical Ltd. The information presented supports the business in maintaining legislative and regulatory compliance.

2. Purpose

The purpose of this policy is to outline the key responsibilities regarding the management of personal, sensitive and confidential within Lifestar Medical Ltd.

3. Scope

This policy document is overarching across the whole of Lifestar Medical Ltd.

The following staff may be affected by this policy document;

- Directors
- Operational Mangers
- Paramedics, Technicians and Medical Responders
- Administrative Staff

The following stakeholders may be affected by this policy document;

- Client organisations
- NHS, including Ambulance and First Responder organisations
- Patients and their families/representatives

4. Legislation

The document is developed to support Lifestar Medical Ltd in meeting for the following:

- The Data Protection Act (2018)
- The General Data Protection Regulation (2016) [EU 2016/679]

In order to ensure full exposure is considered, a range of government issued publications have been considered in the creation of this document. Further information in relation to specific elements of GDPR can be found in the appendix of this document.

5. GDPR Background

GDPR came into force on the 25 May 2018 and replaced the Data Protection Act 1998. The GDPR provides greater protection to individuals and places greater obligations on organisations but can be dealt with in small pre-defined sections which enables the organisation to ensure that any impact on the provision of care and services is minimised.

6. Approach to GDPR Compliance

Lifestar Medical Ltd is required to take a proportionate and appropriate approach to GDPR compliance.

Lifestar Medical Ltd understands that not all organisations will need to take the same steps – it will depend on the volume and types of personal data processed by a particular organisation, as well as the processes already in place to protect personal data.

We understand that if we process significant volumes of personal data, including **special categories of data**, or have unusual or complicated processes in place in terms of the way we handle personal data, we will consider obtaining legal advice specific to the processing we conduct and the steps we may need to take.

GDPR does not apply to any personal data held about someone who has died. Both the Access to Medical Reports Act 1988 and the Access to Health Records 1990 will continue to apply.

7. Promoting Compliance

To ensure Lifestar Medical LTD is compliant with GDPR, a suite of documents are available and should be read in conjunction with this overarching policy to provide a framework:

- **Subject Access Requests Policy / Procedure (Appendix A)**
- **Social and Digital Media Privacy Policy & Procedure**
- **Breach Notification Policy / Procedure (Appendix B)**
- **Fair Processing Notice (Appendix C)**

8. Initial Audit & Privacy Impact Assessment

Lifestar Medical Ltd understands that it must regularly audit the personal data it holds and processes. This can be carried out internally by Lifestar Medical Ltd with the assistance of key staff members.

Regular auditing will reveal whether the ways in which Lifestar Medical Ltd processes personal data meet the requirements of GDPR and will also indicate whether Lifestar Medical Ltd should delete some of the personal data it currently holds.

A Privacy Impact Assessment will be completed to finalise this document.

9. Key Terms

GDPR places obligations on all organisations that process personal data about a Data Subject. A brief description of those three key terms and are expanded below:

Data Subject
An individual about whom Lifestar Medical Ltd has collected personal information.

Data Protection Act
The Data Protection Act 2018 is an Act of Parliament that further develops and updates the data protection laws in the United Kingdom. It sits alongside the European Unions law 'The General Data Protection Regulations (GDPR)

General Data Protection Regulation (GDPR)
A regulation enshrined into EU Law that ensures privacy for all persons within the EU. Created in 2016 it became enforceable in May 2018.

Data Controller or Data Processor
The requirements that Lifestar Medical Ltd need to meet vary depending on whether Lifestar Medical Ltd is a Data Controller or a Data Processor. We recognise that in most scenarios, Lifestar Medical Ltd will be a Data Controller.

Special Categories
Special categories of data attract a greater level of protection, and the consequences for breaching GDPR in relation to special categories of data may be more severe than breaches relating to other types of personal data. Further information can be found in the full GDPR regulations here: https://gdpr-info.eu/

10. Key Principles

There are 6 key principles of GDPR which Lifestar Medical Ltd must comply with. These 6 principles are very similar to the key principles that were set out in the Data Protection Act 1998. They are:

- Lawful, fair and transparent use of personal data
- Using personal data for the purpose for which it was collected
- Ensuring the personal data is adequate and relevant
- Ensuring the personal data is accurate
- Ensuring the personal data is only retained for as long as it is needed
- Ensuring the personal data is kept safe and secure

Lifestar Medical Ltd must be able to provide documentation to the Information Commissioner's Office (ICO) on request, as evidence of compliance.

We understand that we must also adopt 'privacy by design'. This means that data protection issues should be considered at the very start of each new project.

11. Data Protection Officer

Whether or not Lifestar Medical Ltd needs to appoint a formal Data Protection Officer remains a decision to be undertaken by the directors of the company. Regardless of the outcome, Lifestar Medical Ltd will appoint a single person to have overall responsibility for the management of personal data and compliance with GDPR. The person appointed to this role is the Managing Director.

12. Processing Personal Data

The position has been improved under GDPR in terms of the ability of care sector organisations to process special categories of data. The provision of health or social care or treatment or the management of health or social care systems and services is now expressly referred to as a reason for which an organisation is entitled to process special categories

- The Data Subject has given his or her consent to the organisation using and processing their personal data
- The organisation is required to process the personal data to perform a contract; and
- The processing is carried out in the legitimate interests of the organisation processing the data

The other grounds which may apply are:

- The processing is necessary to comply with a legal obligation
- The processing is necessary to protect the vital interests of the Data Subject or another living person
- The processing is necessary to perform a task carried out in the public interest

13. Company Specific Examples of Personal Data

- Patient Care Records
    - Patient Report Forms
    - Audit Information
    - Complaints, Compliments and Concerns Information
    - Statutory Notifications (CQC, RIDDOR, PHE,)

- Employee information
    - HR Information
    - Training Records
    - Payroll & Banking details

- Customer information
    - Account details including contact information
    - Business sensitive information such as quotations & pricing plans

    - Payment information

- Supplier information
    - Account details including contact information
    - Business sensitive information such as quotations & pricing plans
    - Payment information

- CCTV Video & Still images

14. Data Security & Retention

GDPR places an increased responsibility onto the Lifestar Medical Ltd to ensure that any data it holds is;

a) Kept secure and that access is restricted to only persons who require access and
b) Only retained for as long as is necessary to ensure a safe service is provided. In accordance with The Records Managements Code of Practice for Health and Social care 2016 (appendix 3).

15. Subject Access Request

A data subject has the right to request copies of information held by Lifestar Medical Ltd, about them.

Where a subject access request is received, in writing by a data subject, this must be passed, without delay to the Managing Director who will, after seeking advice, make available the necessary information.

16. The rights of the Data Subject

In addition to being able to request data held about them, Data subjects have several additional rights, including;

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

17. Breach Notifications

It is acknowledged that it is possible, even with safeguards, that a Information Governance breach may occur. In these circumstances the Managing Director must be informed immediately. Upon confirmation an investigation must be commenced to understand the nature and the depth of the breach. Upon conclusion of the investigation and certainly within 72 hours a notification must be made to the Information Commissioner and to the Data Subject concerned.

18. Fair Processing Notice

Lifestar Medical Ltd, like all other organisations, are required to make available to Data Subjects information in relation to how their personal data is processed. The easiest and most appropriate way to do this is by publishing a 'Fair Processing Notice'

A copy of the Lifestar Medical Ltd fair processing notices is attached to this document.

19. Transfer of Data

Lifestar Medical Ltd will not transfer data to any third party with the exception of a copy PCR being provided to a NHS service for the purpose of transferring care in an emergency.

20. Key facts for Data Subjects

- Your personal data will be protected, always
- You have the right to see what information we hold about you.
- In addition to this Information Governance & GDPR policy your care will remain confidential
- Consent will be obtained, wherever possible, prior to the storage of personal data

21. Training and Development

To maintain information handling standards throughout our organization, Lifestar will ensure that all staff are provided with clear guidelines on their own obligations for confidentiality, data protection and information security.

Lifestar Medical must comply with all aspects of the law that concern the processing of personal data. This includes legislation (Acts of Parliament) regulations, common law duties and professional codes of practice.

It is vitally important that new staff are made aware of the relevant requirements and in particular given clear guidelines about their own individual responsibilities for maintenance of Information Governance, and that existing staff complete refresher training periodically. Emphasis will be placed on how the requirements affect their day to day practices.

As a minimum the induction training includes:

- The duty of confidentiality
- Sanctions for breach of the duty of confidentiality
- Keeping personal information private, e.g. Avoiding gossip and inappropriate venues for discussion of patient care.
- The use of security measures to ensure information is not inappropriately disclosed e.g. Closed doors, locked cupboards, password management etc.
- The frameworks in place to allow appropriate disclosure
- Dealing with subject access requests
- Freedom of information Act responsibilities
- The importance of accurate information capture
- Pointers to where the company policies, procedures and further information are located.
- On an annual basis all staff must complete an online E-learning module on Information Governance.

22. Monitoring & Review

Lifestar Medical Management are responsible for leading on the implementation of this policy and other Information Governance related policies and procedures. They will ensure that clear formal guidelines have been provided to staff on all aspects of Information Governance.

This policy will be continually monitored and will be subject to regular review. An early review may be warranted if one or more of the following occurs:

- As a result of regulatory/ statutory changes or developments
- As a result of commissioner policy changes or developments
- For any other relevant or compelling reason.

Data Subject Requests Policy – Appendix A

1. ABOUT THIS POLICY

1.1 Data subjects have certain rights in respect of their personal data. When we process data subjects' personal data, we shall respect those rights. This Policy provides a framework for responding to requests to exercise those rights. It is our policy to ensure that requests by data subjects covered by these procedures to exercise their rights in respect of their personal data are handled in accordance with applicable law.

1.2 For the purposes of this Policy, "personal data" means any information relating to an identified or identifiable data subject. An identifiable data subject is anyone who can be identified, directly or indirectly, by reference to an identifier, such as a name, identification number or online identifier. "Processing" means any operation or set of operations that is performed on personal data, such as collection, use, storage, dissemination and destruction.

1.3 This Policy only apply to data subjects whose personal data we process.

2. RESPONDING TO REQUESTS TO ACCESS PERSONAL DATA

2.1 Data subjects have the right to request access to their personal data processed by us. Such requests are called subject access requests (SARs). When a data subject makes an SAR we shall take the following steps: -

(a) log the date on which the request was received (to ensure that the relevant timeframe of one month for responding to the request is met);

(b) confirm the identity of the data subject who is the subject of the personal data. For example, we may request additional information from the data subject to confirm their identity;

(c) search databases, systems, applications and other places where the personal data which are the subject of the request may be held; and

(d) confirm to the data subject whether or not personal data of the data subject making the SAR are being processed.

2.2 If personal data of the data subject are being processed, we shall provide the data subject with the following information in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in writing or by other (including electronic) means: -

(a) the purposes of the processing;

(b) the categories of personal data concerned (for example, contact details, bank account information and details of sales activity);

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients overseas (for example, US-based service providers);

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data or to object to such processing;

(f) the right to lodge a complaint with the Information Commissioner's Office (ICO);

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; and

(i) where personal data are transferred outside the EU, details of the appropriate safeguards to protect the personal data.

2.3 We shall also, unless there is an exemption (see *Paragraph 9* below), provide the data subject with a copy of the personal data processed by us in a commonly used electronic form (unless the data subject either did not make the request by electronic means or has specifically requested not to be provided with the copy in electronic form) within one month of receipt of the request. If the request is complex, or there are a number of requests, we may extend the period for responding by a further two months. If we extend the period for responding we shall inform the data subject within one month of receipt of the request and explain the reason(s) for the delay.

2.4 Before providing the personal data to the data subject making the SAR, we shall review the personal data requested to see if they contain the personal data of other data subjects. If they do, we may redact the personal data of those other data subjects prior to providing the data subject with their personal data, unless those other data subjects have consented to the disclosure of their personal data.

2.5 If the SAR is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of providing the personal data, or refuse to act on the request.

2.6 If we are not going to respond to the SAR we shall inform the data subject of the reason(s) for not taking action and of the possibility of lodging a complaint with the Information Commissioner's Office (ICO).

3. RESPONDING TO REQUESTS TO RECTIFY PERSONAL DATA

3.1 Data subjects have the right to have their inaccurate personal data rectified. Rectification can include having incomplete personal data completed, for example, by a data subject providing a supplementary statement regarding the data. Where such a request is made, we shall, unless there is an exemption (see *Paragraph 9* below), rectify the personal data without undue delay.

3.2 We shall also communicate the rectification of the personal data to each recipient to whom the personal data have been disclosed (for example, our third party service providers who process the data on our behalf), unless this is impossible or involves disproportionate effort. We shall also inform the data subject about those recipients if the data subject requests it.

4. RESPONDING TO REQUESTS FOR THE ERASURE OF PERSONAL DATA

4.1 Data subjects have the right, in certain circumstances, to request that we erase their personal data. Where such a request is made, we shall, unless there is an exemption (see *Paragraph 9*

below), erase the personal data without undue delay if: -

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws their consent to the processing of their personal data and consent was the basis on which the personal data were processed and there is no other legal basis for the processing;

(c) the data subject objects to the processing of their personal data on the basis of our performance of a task carried out in the public interest or in the exercise of official authority vested in us, or on the basis of our legitimate interests which override the data subject's interests or fundamental rights and freedoms, unless we either can show compelling legitimate grounds for the processing which override those interests, rights and freedoms, or we are processing the data for the establishment, exercise or defence of legal claims;

(d) the data subject objects to the processing of their personal data for direct marketing purposes;

(e) the personal data have been unlawfully processed;

(f) the personal data have to be erased for compliance with a legal obligation to which we are subject; or

(g) the personal data have been collected in relation to the offer of e-commerce or other online services.

4.2 When a data subject makes a request for erasure in the circumstances set out above, we shall, unless there is an exemption (see *Paragraph 4.5* and *Paragraph 9* below), take the following steps: -

(a) log the date on which the request was received (to ensure that the relevant timeframe of one month for responding to the request is met);

(b) confirm the identity of the data subject who is the subject of the personal data. We may request additional information from the data subject to do this;

(c) search databases, systems, applications and other places where the personal data which are the subject of the request may be held and erase such data within one month of receipt of the request. If the request is complex, or there are a number of requests, we may extend the period for responding by a further two months. If we extend the period for responding we shall inform the data subject within one month of receipt of the request and explain the reason(s) for the delay;

(d) where we have made the personal data public, we must, taking reasonable steps, including technical measures, inform those who are processing the personal data that the data subject has requested the erasure by them of any links to, or copies or replications of, those personal data; and

(e) communicate the erasure of the personal data to each recipient to whom the personal data have been disclosed unless this is impossible or involves disproportionate effort.

We shall also inform the data subject about those recipients if the data subject requests it.

4.3 If the request is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of erasure, or refuse to act on the request.

4.4 If we are not going to respond to the request we shall inform the data subject of the reasons for not taking action and of the possibility of lodging a complaint with the ICO.

4.5 In addition to the exemptions in *Paragraph 9* below, we can also refuse to erase the personal data to the extent processing is necessary: -

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by law and to which we are subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in us;

(c) for reasons of public interest in the area of public health;

(d) for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims.

5. RESPONDING TO REQUESTS TO RESTRICT THE PROCESSING OF PERSONAL DATA

5.1 Data subjects have the right, unless there is an exemption (see *Paragraph 9* below), to restrict the processing of their personal data if: -

(a) the data subject contests the accuracy of the personal data, for a period to allow us to verify the accuracy of the personal data;

(b) the processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(c) we no longer need the personal data for the purposes we collected them, but they are required by the data subject for the establishment, exercise or defence of legal claims; and

(d) the data subject has objected to the processing, pending verification of whether we have legitimate grounds to override the data subject's objection.

5.2 Where processing has been restricted, we shall only process the personal data (excluding storing them):

(a) with the data subject's consent;

(b) for the establishment, exercise or defence of legal claims;

(c) for the protection of the rights of another person; or

(d) for reasons of important public interest.

5.3 Prior to lifting the restriction, we shall inform the data subject of the lifting of the restriction.

5.4 We shall communicate the restriction of processing of the personal data to each recipient to whom the personal data have been disclosed, unless this is impossible or involves disproportionate effort. We shall also inform the data subject about those recipients if the data subject requests it.

6. RESPONDING TO REQUESTS FOR THE PORTABILITY OF PERSONAL DATA

6.1 Data subjects have the right, in certain circumstances, to receive their personal data that they have provided to us in a structured, commonly used and machine-readable format that they can then transmit to another company. Where such a request is made, we shall, unless there is an exemption (see *Paragraph 9* below), provide the personal data without undue delay if:-

(a) the legal basis for the processing of the personal data is consent or pursuant to a contract; and

(b) our processing of those data is automated.

6.2 When a data subject makes a request for portability in the circumstances set out above, we shall take the following steps: -

(a) log the date on which the request was received (to ensure that the relevant timeframe of one month for responding to the request is met);

(b) confirm the identity of the data subject who is the subject of the personal data. We may request additional information from the data subject to confirm their identity; and

(c) search databases, systems, applications and other places where the personal data which are the subject of the request may be held and provide the data subject with such data (or, at the data subject's request, transmit the personal data directly to another company, where technically feasible) within one month of receipt of the request. If the request is complex, or there are a number of requests, we may extend the period for responding by a further two months. If we extend the period for responding we shall inform the data subject within one month of receipt of the request and explain the reason(s) for the delay.

6.3 If the request is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of providing or transmitting the personal data, or refuse to act on the request.

6.4 If we are not going to respond to the request we shall inform the data subject of the reasons for not taking action and of the possibility of lodging a complaint with the ICO.

7. RESPONDING TO OBJECTIONS TO THE PROCESSING OF PERSONAL DATA

7.1 Data subjects have the right to object to the processing of their personal data where such processing is on the basis of our performance of a task carried out in the public interest or in the

exercise of official authority vested in us, or on the basis of our legitimate interests which override the data subject's interests or fundamental rights and freedoms, unless we either:-

(a) can show compelling legitimate grounds for the processing which override those interests, rights and freedoms; or

(b) are processing the personal data for the establishment, exercise or defence of legal claims.

7.2 Data subjects also have the right to object to the processing of their personal data for scientific or historical research purposes, or statistical purposes, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

7.3 Where such an objection is made, we shall, unless there is an exemption (see *Paragraph 9* below), no longer process a data subject's personal data.

7.4 Where personal data are processed for direct marketing purposes, data subjects have the right to object at any time to the processing of their personal data for such marketing. If a data subject makes such a request, we shall stop processing the personal data for such purposes.

8. RESPONDING TO REQUESTS NOT TO BE SUBJECT TO AUTOMATED DECISION-MAKING

8.1 Data subjects have the right, in certain circumstances, not to be subject to a decision based solely on the automated processing of their personal data, if such decision produces legal effects concerning them or similarly significantly affects them. Where such a request is made, we shall, unless there is an exemption (see *Paragraph 9* below), no longer make such a decision unless it: -

(a) is necessary for entering into, or the performance of, a contract between us and the data subject;

(b) is authorised by applicable law which lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

8.2 If the decision falls within *Paragraph 8.1(a)* or *Paragraph 8.1(c)*, we shall implement suitable measures to safeguard the data subject's rights, freedoms and legitimate interests, including the right to obtain human intervention, to express their point of view and to contest the decision.

9. EXEMPTIONS

9.1 Before responding to any request we shall check whether there are any exemptions that apply to the personal data that are the subject of the request. Exemptions may apply where it is necessary and proportionate not to comply with the requests described above to safeguard: -

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(e) other important objectives of general national public interest, in particular an important national economic or financial interest, including monetary, budgetary and taxation matters, public health and social security;

(f) the protection of judicial independence and judicial proceedings;

(g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in *Paragraph 9.1(a)* and *Paragraph 9.1(g)* above;

(i) the protection of the data subject or the rights and freedoms of others; or

(j) the enforcement of civil law claims.

Appendix B - Data Breach Incident Plan

10. INTRODUCTION

10.1 Lifestar Medical LTD is committed to the protection and security of personal data. We have implemented appropriate policies and procedures to ensure we handle personal data appropriately and lawfully.

10.2 The General Data Protection Regulation (*(EU) 2016/679)* (GDPR) places an obligation on organisations acting as data controllers to report breaches of personal data to the relevant lead supervisory authority. In the UK the relevant authority is the Information Commissioner's Office (ICO). We are the data controller in circumstances where we determine the purposes and means of the processing of personal data.

10.3 If we are acting as a data processor (processing personal data on behalf of a data controller) we must notify the data controller, without undue delay, after becoming aware of a personal data breach and so much of this Data Breach Incident Plan will assist us in satisfying that obligation.

10.4 We recognise that it is possible for data breach incidents to occur. Data breaches may have a range of significant adverse effects on individuals which can result in physical, material, or non-material damage. Under GDPR, we will be required to report certain personal data breaches to the ICO within 72 hours. Failing to notify the ICO of a breach when required to do so could result in a fine up to EUR20 million or 2 per cent global turnover (or potentially attract fines up to EUR20 million or 4 per cent global turnover in some cases). Accordingly, it is necessary for us to have in place this Data Breach Incident Plan so that, should a data breach incident occur, we are properly prepared to deal with that incident in an efficient, effective manner and, if necessary, report the incident to the ICO (and potentially the data subject(s) concerned) in accordance with the relevant law.

10.5 Annex A of this Data Breach Incident Plan includes a Data Breach Incident Timeline which should be used to record key actions and decisions carried out in accordance with this Policy.

10.6 This Data Breach Incident Plan is related to our IG and GDPR Policy

10.7 The Managing Director is responsible for overseeing this Policy. Any questions about the operation of this Policy should be submitted to the Managing Director.

11. IDENTIFYING A DATA BREACH INCIDENT

11.1 The GDPR defines a personal data breach as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

11.2 Broadly, a personal data breach can be defined as any act or omission that compromises the security, confidentiality, integrity or availability of personal data or the physical, technical administrative or organisational safeguards that we (or our third-party service providers) put in place to protect it. This also means that a breach is more than just about losing personal data.

11.3 Personal data breaches include breaches that are the result of both accidental and deliberate causes and, for example, can include (but are not limited to): -

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;

- alternation of personal data without permission; and
- loss of availability of personal data.

11.4 If you know or suspect that a personal data breach has occurred, immediately contact the managing director and preserve all evidence relating to the potential breach.

12. CONTAINMENT AND RECOVERY

12.1 The Managing Director will consider any potential personal data breach and determine whether personal data is involved and whether there is a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.

12.2 The Managing Director will investigate the potential breach and determine the cause of the breach and whether or not the breach has been contained. If the breach has not been contained, it will be necessary to establish what measures can be taken to contain the breach, recover data and avoid any further adverse consequences. Key actions and decisions made under this Data Breach Incident Plan should be logged in the Timeline of Incident Management (Annex A).

13. ASSESSMENT OF RISKS

13.1 We should gather as much information as possible regarding the breach and use the information obtained to assess and manage risks and inform the direction of the investigation into the breach. This will assist in determining the appropriate actions and decision to be taken.

13.2 In the course of the investigation The Managing Director will produce a report outlining: -

- the cause of the breach;
- how the breach was detected
- when the breach was detected;
- when the breach occurred;
- the categories of personal data included in the breach;
- whether the breach has been contained or is ongoing;
- what measures have been taken to contain or attempt to contain the breach and mitigate adverse effects;
- the number of data subjects that could be affected;
- the categories of data subjects affected;
- the potential consequences of the breach;
- the likelihood that data subjects will experience significant consequences as a result of the breach;
- whether professional advice should be or has been sought;
- any other considerations.

14. NOTIFICATION

14.1 We are required to notify the ICO of a personal data breach without undue delay, and within 72 hours of becoming aware of the breach, where it is likely to result in a risk to the rights and freedoms of individuals. If we are unable to notify the ICO within 72 hours then we must provide the ICO with reasons for the delay. If a risk is unlikely then we do not have to report the breach. However, if we decide that we do not need to report a breach, we must be able to justify our decision and should document it.

14.2 We will consider the findings made during the course of the investigation into the breach and the report produced by The Managing Director in order to determine whether the requirement for notifying the ICO has been triggered, as well as any further action(s) needed to address the

breach.

14.3 When determining whether notification to the ICO is required, we will focus on the on the potential negative consequences for individuals. Personal data breaches can have a variety of adverse effects on individuals and we will assess breaches on a case by case basis. If in doubt about the likelihood of risk to the rights and freedoms of individuals we should elect to notify.

14.4 Notifications to the ICO must include the following information: -

- a description of the nature of the personal data breach including, where possible: -
  - the categories and approximate number of the individuals concerned; and
  - the categories and approximate number of personal data records concerned;
- the name and contact details of The Managing Director where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken or proposed in order to deal with the personal data breach and including, where appropriate, the measures taken to mitigate possible adverse effects.

14.5 We should be able to extract the required notification information from the report of the Managing Director

14.6 The GDPR allows us to provide the required notification information in phases if we have been unable to investigate the breach fully within 72 hours. We must still provide the information we have obtained within the 72 hour time limit and must submit the further information about the breach without delay. If we are unable to provide the full details required within 72 hours then we should explain the delay to the ICO and also inform the ICO as to when we expect the further information will be submitted.

14.7 If a breach is likely to result in a **high risk** to the rights and freedoms of individuals then we must also inform the relevant individuals directly and without undue delay (as soon as possible). The threshold for communicating a breach to individuals is therefore higher than for notifying the ICO.

14.8 The main purpose of notifying individuals is to provide them with specific information about measures they should take to protect themselves from any negative consequences of the breach. If we decide that we must communicate with individuals, we must tell them, in clear and plain language, the nature of the breach and, at a minimum: -

- the name and contact details of The Managing Director where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken or proposed in order to deal with the personal data breach and including, where appropriate, the measures taken to mitigate possible adverse effects.

14.9 The GDPR states that breach communications to individuals should be made in close cooperation with the relevant supervisory authority, so it may be appropriate for us to seek advice from the ICO about information individuals about a breach and also in relation to the appropriate messages to be sent and the most appropriate way to contact the individuals.

14.10 There are exceptions to the requirement of notifying individuals of the breach, which are: -

- if the data controller has implemented appropriate measures that mean the personal data are unintelligible to unauthorised persons (e.g. encryption);
- if the data controller has taken subsequent measures which ensure that the high risk to the individuals is no longer likely to materialist;
- it would be a disproportionate effort for the data controller to notify the affected individuals. In this case, the data controller would still need to make a public communication to inform the individuals in an equally effective manner.

15. EVALUATION AND RESPONSE

15.1 Whether a breach needs to be notified or not, we are required to document all breaches where we are the data controller. We have discretion in the method and structure we use when documenting a breach, however, we must record: -

- facts relating to the breach, including its causes, what took place and the personal data affected;
- the effects and consequences of the breach;
- any remedial action we take.

15.2 We should also document our reasoning for particular decisions taken in response to the breach, such as: our justification if we decide a breach is not notifiable; any reasons for delay in notifying; and any information communicated to individuals affected by the breach.

15.3 It is possible that evidence gathered during the investigation of the breach may be required to defend legal claims or potentially used for proactive civil litigation or criminal prosecution against potential perpetrators of the data breach. Retention periods for such relevant documentation should be considered carefully.

15.4 Following a data breach incident we will conduct a thorough post-incident review in order to evaluate our response to the incident and the effectiveness of our processes and procedures.

Annex A: Data Breach Incident Timeline

Date	Time	Activity	Decision	Authority (Name/Position)

Fair Processing Notice – Appendix C

1. WHAT IS THE PURPOSE OF THIS DOCUMENT?

Lifestar Medical LTD is committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the General Data Protection Regulation (GDPR). It applies to all employees, workers and contractors.

Lifestar Medical LTD is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to current and former employees, workers and contractors. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time but if we do so, we will provide you with an updated copy of this notice as soon as reasonably practicable.

It is important that you read and retain this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information and what your rights are under the data protection legislation.

2. DATA PROTECTION PRINCIPLES

We will comply with data protection law. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

3. THE KIND OF INFORMATION WE HOLD ABOUT YOU

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

This information will vary dependent on whether you are an employee, patient or customer.

There are “special categories” of more sensitive personal data which require a higher level of protection.

We will collect, store, and use the following categories of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Marital status and dependants.
- Next of kin and emergency contact information.
- National Insurance number.
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information.
- Start date and, if different, the date of your continuous employment.
- Leaving date and your reason for leaving.
- Location of employment or workplace.
- Copy of driving licence.
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).
- Employment records (including job titles, work history, working hours, holidays, training records and professional memberships).
- Compensation history.
- Performance information.
- Disciplinary and grievance information.
- CCTV footage and other information obtained through electronic means such as swipe card records.
- Information about your use of our information and communications systems.
- Photographs.
- Results of HMRC employment status check, details of your interest in and connection with the intermediary through which your services are supplied.

We may also collect, store and use the following “special categories” of more sensitive personal information:

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions.
- Information about your health, including any medical condition, health and sickness records, including:

  - where you leave employment and under any share plan operated by a group company the reason for leaving is determined to be ill-health, injury or disability, the records relating to that decision;

- details of any absences (other than holidays) from work including time on statutory parental leave and sick leave; and
- where you leave employment and the reason for leaving is related to your health, information about that condition needed for pensions and permanent health insurance purposes.

- Information about criminal convictions and offences.

4. HOW IS YOUR PERSONAL INFORMATION COLLECTED?

We collect personal information about employees, workers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies.

We collect information about customers and patients through our booking procedure, telephone, contact portals on social and digital media as well as during face to face assessments. Information will also be requested and documented on patient report forms.

We may also collect personal information from the trustees or managers of pension arrangements operated by a group company.

We will collect additional personal information in the course of job-related activities throughout the period of employment.

5. HOW WE WILL USE INFORMATION ABOUT YOU

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to perform the contract we have entered into with you.

2. Where we need to comply with a legal obligation.

3. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

1. Where we need to protect your interests (or someone else's interests).

2. Where it is needed in the public interest [or for official purposes].

5.1 Situations in which we will use your personal information

We need all the categories of information in the list above (see *Paragraph 1*) primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below. We have indicated by the purpose or purposes for which we are processing or will process your personal

information, as well as indicating which categories of data are involved.

- Making a decision about your recruitment or appointment.
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the UK.
- Paying you and, if you are an employee or deemed employee for tax purposes, deducting tax and National Insurance contributions (NICs).
- Providing additional benefits to you where appropriate and lawful.
- Enrolling you in a pension arrangement in accordance with our statutory automatic enrolment duties.
- Liaising with the trustees or managers of a pension arrangement operated by a group company, your pension provider and any other provider of employee benefits.
- Administering the contract we have entered into with you.
- Business management and planning, including accounting and auditing.
- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Gathering evidence for possible grievance or disciplinary hearings.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.
- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- To conduct data analytics studies to review and better understand employee retention and attrition rates.
- Equal opportunities monitoring.

- To complete Treatment and journeys plans and risk assessments.
- To ensure appropriate treatment plans can be followed and shared with appropriate professionals when necessary.
- To fulfil safeguarding duties, in line with relevant safeguarding guidance.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

5.2 If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Failure to supply necessary information may impact on our ability to fulfil our contractual obligations when transporting or treating the service user.

5.3 Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

6. HOW WE USE PARTICULARLY SENSITIVE PERSONAL INFORMATION

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.
2. Where we need to carry out our legal obligations or exercise rights in connection with employment.
3. Where it is needed in the public interest, such as for equal opportunities monitoring.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about members or former members in the course of legitimate business activities with the appropriate safeguards.

6.1 Our obligations as an employer

We will use your particularly sensitive personal information in the following ways:

- We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.
- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits including statutory maternity pay, statutory sick pay, pensions and permanent health insurance.
- If you apply for an ill-health pension under a pension arrangement operated by a group company, we will use information about your physical or mental health in reaching a decision about your entitlement.
- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

6.2 Do we need your consent?

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent.

7. INFORMATION ABOUT CRIMINAL CONVICTIONS

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our IG and GDPR

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us.

We will use information about criminal convictions and offences as part of the employment process to ascertain fitness for a role.

We are allowed to use your personal information in this way to carry out our legal obligations to ensure we follow appropriate safeguarding procedures. We have in place an appropriate policy and safeguards which we are required by law to maintain when processing such data.

8. AUTOMATED DECISION-MAKING

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

1. Where we have notified you of the decision and given you 21 days to request a reconsideration.

2. Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights.

3. In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

9. DATA SHARING

We may have to share your data with third parties, including third-party service providers and other entities in the group.

Patient Data will only be shared when and where it is legally appropriate and not under any circumstance not made essential by treatment plans and safeguarding regulations.

We require third parties to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the EU.

If we do, you can expect a similar degree of protection in respect of your personal information.

9.1 Why might you share my personal information with third parties?

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

9.2 Which third-party service providers process my personal information?

“Third parties” includes third-party service providers (including contractors and designated agents) and other entities within our group. The following activities are carried out by third-party service providers: payroll, pension administration, benefits provision and administration, IT services

How secure is my information with third-party service providers and other entities in our group?

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

9.3 When might you share my personal information with other entities in the group?

We will share your personal information with other entities in our group as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data.

9.4 What about other third parties?

We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business. In this situation we will, so far as possible, share anonymised data with the other parties before the transaction completes. Once the transaction is completed, we will share your personal data with the other parties if and to the extent required under the terms of the transaction.

We may also need to share your personal information with a regulator or to otherwise comply with the law.

This may include making returns to HMRC, disclosures to stock exchange regulators [(including a Regulatory News Service)] and disclosures to shareholders such as directors' remuneration reporting requirements.

10. DATA SECURITY

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

11. DATA RETENTION

11.1 How long will you use my information for?

We will only retain your personal information 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.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal information in accordance with the Data Retention and Acquisition regulations 2018.

12. RIGHTS OF ACCESS, CORRECTION, ERASURE, AND RESTRICTION

12.1 Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

12.2 Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a “data subject access request”). This enables you to receive a copy of the personal information we hold

about you and to check that we are lawfully processing it.

- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).

- **Object to processing** of your personal information 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. You also have the right to object where we are processing your personal information for direct marketing purposes.

- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

- **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Managing Director in writing.

12.3 No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

12.4 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 the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

13. RIGHT TO WITHDRAW CONSENT

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Managing Director Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

14. DATA PROTECTION OFFICER

We have appointed the Managing Director as a data protection officer to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the Managing Director. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

15. CHANGES TO THIS PRIVACY NOTICE

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

If you have any questions about this privacy notice, please contact the Managing Director