DATA PROTECTION POLICY

Document name:	**Data Protection Policy**
Document Classification:	Information Governance
Document No:	DPP001
Version:	2.0
Name of originator/author:	**Catherine Turner**
Date created	November 2020
Policy Reviewer	Lorraine Gallier
Review Date	May 2021
Responsible committee:	Operational Committee
Superseded policy (if applicable):	N/A
Target audience:	Directors, Managers, Clinicians, Staff
Other relevant policies	• Agency Worker Handbook • Grievance & Disciplinary Policy • Safer Recruitment Policy • Privacy Notice • Confidentiality Policy

SOSMedical

CONTENTS

1.0 Introduction
2.0 Aims
3.0 Scope
4.0 Roles & Responsibilities
5.0 Definitions
6.0 Legal Framework
7.0 GDPR explained
8.0 Access to IT Systems
9.0 Access to Records
10.0 Computers
11.0 Telephone
12.0 E-Mails
13.0 Monitoring Compliance and Policy Review
14.0 Training
15.0 Data protection Impact assessments (DPIAs)
16.0 Do's and Don't's
17.0 Breach of Policy
18.0 Disposal of Data
19.0 Dissemination
20.0 Appendices
21.0 Links and References

1.0 INTRODUCTION

Thank you for choosing to be part of our workforce at SOS Medical. We are committed to protecting your personal information and your right to privacy. If you have any questions or concerns about our policy, or our practices with regards to your personal information, please contact us at admin@sosmedical.co.uk

GDPR stands for **General Data Protection Regulation** and was implemented on 25th May 2018 - meaning companies should **already be compliant**.

GDPR is a game-changing new privacy law that regulates how companies handle our personal information.

It is a law created in the European Union (EU) to protect the personal data of its citizens. Although it was passed in Europe, it affects businesses worldwide and companies of all sizes that target customers in the EU must evaluate and adjust their data collection practices to meet the stringent requirements of the GDPR.

These efforts include taking the initial steps to achieve compliance, as well as integrating the key principles of the GDPR into every part of SOS Medical's operations.

This policy is not, and should not be confused with, a privacy notice (a statement informing data subjects how their personal data is used by SOS Medical).

It is however, to be used in conjunction with any assignment site areas own GDPR Policy. Temporary staff must familiarise themselves with the Unit's policies and procedures when undertaking work on behalf of SOS Medical.

Complying with this European regulation on data protection means ensuring data is collected legally, informing users of how it is treated, and keeping data secure (i.e., protected from breaches).

2.0 SCOPE

This policy provides guidance to ensure that information processed by SOS Medical employees is handled in a safe and secure manner which complies with current legislation and best practice relating to data protection and confidentiality.

It will apply to all areas of SOS Medical and all staff who handle information. It will be of particular relevance to staff members who handle personal and sensitive information relating to both patients and staff.

This policy applies to all members of staff, including non-executive directors/ Temporary staff/apprentices/Locums/contractors and sub-contractors.

3.0 AIMS

This policy aims to set out in a comprehensive manner, the regulations SOS Medical are required to meet GDPR and to ensure all staff understand their responsibilities and obligations pertaining to their role, including personal data, personnel files and data subject access requests.

It will also aim to show SOS Medical's commitment to the confidentiality of Clients, Staff and Service Users information and its responsibilities with regard to the disclosure of such information.

SOS Medical will document the ways in which we ensure that client, patient and staff data is handled effectively and securely and promote best practice and innovative use of personal information.

By making this policy available to all staff on the SOS Medical Website we aim to protect staff by making them aware of the correct procedures for maintaining confidentiality of patient information so that they do not inadvertently breach any requirements of law or good practice.

4.0 ROLES AND RESPONSIBILITIES

Currently Ankit Goyal has overall responsibility for the implementation of this policy.

The role is accountable for the overall development and maintenance of information governance which includes:

- Promoting a culture for protecting and using data

- Provides a focal point for managing information risk and incidents

- Is concerned with the management of all information assets

This is then delegated to the Registered Manager for operational actions and requirements to ensure compliance.

Individual Responsibilities

Everyone working for SOS Medical has a legal duty to keep information about patients and clients and other individuals such as staff or volunteers confidential.

They are required to adhere to confidentiality agreements i.e. common-law duty of confidentiality, contract of employment, NHS Confidentiality Code of Practice.

All staff will, whilst undertaking employment with SOS Medical, have access to confidential information relating to temporary workers, clients, patients and employees,

Staff must not use such information for your own benefit nor disclose it to other persons without consent of the party concerned unless required to so by law. This will apply both during and after the termination of your employment.

If any member of staff is found to have revealed confidential information without consent, disciplinary action may be taken.

If you are in any doubt regarding the use of information in the pursuit of your duties, please contact your consultant or the Nurse Manager for SOS Medical before communicating such information to any third party.

Individual health professionals will also be subject to professional regulatory codes of conduct which include standards related to confidentiality and information handling.

All staff are responsible for ensuring they keep up to date with Information Governance and Data Protection training in accordance with SOS Mandatory training requirements

If employees have any questions about data protection in general, this policy or their obligations under it, they should direct them to Anik Goyal and/or Nurse Manager, Lorraine Gallier.

5.0 DEFINITIONS (See appendix 1 for further explanations)

GDPR Personal data

Any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

Personal data under the GDPR is any information that could be pieced together to identify an individual, such as name, email address, and credit card number.

Examples of personal data:

Name / phone number / address / date of birth / bank account / passport number / social media posts / geotagging / health records / race / religious and political opinions

Now that smartphones and social media are ubiquitous, this information includes location and biometric data (Google Maps and retina scans), IP addresses, plus everything you share online — from your salary to your political opinions.

This broader definition of personal data is one of the major differences between the GDPR and DPD. (Data Protection Directive)

Data controller

The person (or company) who determines the purposes for which and the manner in which any personal data are, or are to be, recorded.

Data flow

A continuing or repeated flow of information which takes place between individuals or organisations and includes personal data.

Data processor

Any person who processes data on behalf of the data controller.

Direct care

The provision of clinical services to a patient that require some degree of interaction between the patient and the health care provider. Examples include assessment, performing procedures and implementation of a care plan.

Duty of confidence

A duty of confidence arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence. It arises from common law.

Information governance

Information governance is a combination of legal requirements, policy and best practice designed to ensure all aspects of information processing and handling are of the highest standards.

Legitimate relationship

A relationship that exists between a patient and an individual or group of record users involved in their treatment which provides the justification for those users to access a patient record.

Processing

This term covers the collection, recording or holding of information or data, or carrying out any operation or set of operations on the information or data, including but not restricted to alteration, retrieval, disclosure and destruction or disposal of the data.

Non care or secondary purpose

Purposes other than direct care such as healthcare planning, commissioning, public health, clinical audit and governance, benchmarking, performance improvement, medical research and policy development.

6.0 Legal Framework (See Appendix 2 for full list)

The legal and best practice guidance informing the development of this policy includes:

- Common law duty of confidence
- All Contracts of employment issued by SOS Medical
- Data Protection Act 2018
- Human Rights Acts 1998
- NHS Confidentiality code of practice
- General Data Protection Regulation (GDPR)

7.0 GDPR EXPLAINED

How do GDPR rules affect users?

The GDPR's new rules affect users by giving them more rights and control over how their data is used.

The GDPR tells companies of all sizes **what they can and can't do with your information**.

In addition to increased consent measures affecting the online experience, there are considerable changes behind the scenes that many users aren't aware of.

Seven Core GDPR Guidelines

There are seven key principles to the GDPR that dictate how businesses should process data in order to conform to new EU data protection standards.

7.1 Lawfulness, fairness, and transparency

Data processing must be legal and the information collected and used fairly. Users must not be mislead about how their data is used

To ensure 'fair processing' SOS Medical aim to be lawful, fair and transparent about the way we will use the personal data we hold.

We must demonstrate that we:

- are open and honest about our identity
- tell people how we intend to use any personal data we collect about them
- usually handle their personal data only in ways they would reasonably expect
- do not use their information in ways that unjustifiably have a negative effect on them
- help people to understand their rights

To meet this requirement SOS Medical publishes a Privacy Policy to inform staff about the way we handle and use their personal data. This is published on the SOS Medical Website in Nurse Lounge.

There are 6 lawful purposes for processing data. At least one of these must apply whenever personal data is processed:

Consent:

The individual has given clear consent in the Application for employment for SOS Medical to process their personal data for a specific purpose. The GDPR gives a specific right to withdraw consent. The individual has the right to withdraw.

Contract:

The processing is necessary for a contract

Legal obligation:

The processing is necessary for SOS Medical to comply with the law (not including contractual obligations).

Vital interests:

The processing is necessary to protect someone's life.

Public task:

The processing is necessary for SOS Medical to perform a task in the public interest or for the agency's official functions, and the task or function has a clear basis in law.

Legitimate interests:

The processing is necessary for SOS Medical Agency 's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

7.2. Purpose limitation

The purpose of processing must be clear from the start, recorded, and changed only if there is user consent

7.3. Data minimization

Only data required for the stated processing purpose should be collected

7.4. Accuracy

Reasonable steps must be taken to ensure the collected data is accurate and up to date

7.5. Storage limitation

Data should not be kept longer than necessary

7.6. Integrity and confidentiality

Appropriate cybersecurity measures must be put in place to protect personal data being stored

7.7. Accountability

Organizations are accountable for how they handle data and comply with the GDPR

7.8 Additional GDPR Basics and Concepts

To ensure companies abide by its seven core guidelines, the GDPR details several additional features that are integral to successful compliance. These concepts reshape how businesses interact with their customer

7.9 Privacy by Design

Privacy by Design (PbD) means that data protection should be built into the very core of your business. Article 25 states:

"The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed".

This practice should ultimately **minimize data collection**. Privacy by Design is not a new concept in the data protection sphere, but only now is it a legal requirement in the EU.

To implement PbD, data integrity should be secured in the design stages of a product, and then proactively kept in mind throughout development.

7.10 Summary of New GDPR Data Subject Rights

One of the ways that the GDPR has empowered users is by giving them an array of new rights regarding their personal data.

These are as follows:

- **The Right to be Informed**: The GDPR emphasizes transparency in data collection practices, meaning individuals have the right to be fully informed about the collection and use of their personal data.

- **The Right of Access** (Article 15): Individuals can request to view any personal data that has been collected from them. This information must be provided within one month and be free of charge.

- **The Right to Rectify Information** (Article 16): If data collected about an individual is inaccurate, the individual has the right to request a correction (rectification). The organization processing the data must respond within one month.

- **The Right to Erasure / The Right to be Forgotten** (Article 17): After information has been collected about them, individuals can request it be permanently deleted, either because the information is no longer relevant, or because the user chooses to withdraw their consent.

- **The Right to be Informed**: The GDPR emphasizes transparency in data collection practices, meaning individuals have the right to be fully informed about the collection and use of their personal data.

- **The Right of Access** (Article 15): Individuals can request to view any personal data that has been collected from them. This information must be provided within one month and be free of charge.

- **The Right to Rectify Information** (Article 16): If data collected about an individual is inaccurate, the individual has the right to request a correction (rectification). The organization processing the data must respond within one month.

- **The Right to Erasure / The Right to be Forgotten** (Article 17): After information has been collected about them, individuals can request it be permanently deleted, either because the information is no longer relevant, or because the user chooses to withdraw their consent.

- **The Right to Restrict Data Processing** (Article 18): An individual can request to limit how their data is processed when certain conditions apply, such as if the processing is unlawful or if the individual has objected to it.

- **The Right to Data Portability** (Article 20): When users request to view their data, it must be given to them in a clear format so it can be easily transferred to another organization.

- **The Right to Object** (Article 21): Individuals can object to the processing of their data in certain situations, such as direct marketing.

8.0 ACCESS TO IT SYSTEMS

It is essential that IT systems holding personal data have adequate controls in place to prevent loss, unlawful processing or inappropriate access.

No staff of SOS Medical should ever attempt to access or use electronic record systems they have not been trained to use or authorised to access. Temporary staff undertaking shift on behalf of SOS Medical in Acute Trusts must adhere to the assignments own policies for documenting care. Staff should not allow others to access systems using their login credentials. Sharing system passwords is a disciplinary offence and viewed as a serious breach of Trust procedure.

9.0 ACCESS TO RECORDS

Any registered staff member acting on behalf of SOS Medical must follow the Acute Trusts Policies for accessing records.

While it is clearly necessary for many members of staff to routinely access and use these records to carry out their work, it is important staff know that any access to records which is not legitimate or authorised is prohibited and may be unlawful.

Many of our clients use digital systems and will allow a user to access any individual record held in that system. Users should only access individual personal records for those data subjects (patients) that they have authorisation to access for specific purposes or in the case of patient records where they have a 'legitimate relationship' with the patient.

Acute Trusts that SOS Medical supply staff to, will intermittently carry out audits of access to personal data and any member of staff who is found to be in breach of this guidance by inappropriately accessing their own or other peoples' record data may face disciplinary action.

In addition, SOS Medical holds personal records for present and former members of staff and others it does business with. Some staff are in a position to potentially access personal data held about them in SOS Medical records (e.g. their personal medical records). Therefore SOS Medical employees should not access their own data held in any records without specific authorisation.

Requests for obtaining access to or copies of personal information held by SOS Medical about individuals are to be made in writing under a Subject Access Request.

10.0 Computers

For those staff working in Acute Trusts, patient's information must only be stored on Trust equipment

For staff needing to work from home, access will be limited to the Senior Management Team via a secured shared drive.

Patient named data should not be kept on the hard drives of PCs due to the risk of theft and breach of confidentiality.

Users should not leave terminals logged in and unattended unless the account is locked for short term absences from the terminal.

11.0 Telephone

All possible steps must be taken to ensure that information is not divulged over the phone to anyone without appropriate authority. For staff working in Acute Trusts they must follow the assignments policy on sharing information on the telephone.

Where there is any doubt regarding the identity of the person requesting the information, guidance should be sought from the Nurse in Charge at the assignment or and inform SOS Medical using the incident reporting form published on SOS Medical Website, Nurse Lounge.

If advice is not immediately available then the information should not be disclosed. If the caller is claiming to be from an organisation e.g. social services then the switchboard telephone number should be obtained, checked and then used to ensure that the caller is from the agency stated

12.0 E-mail

SOS Medical's policy is that e-mails that include personal data should be sent 'securely 'to avoid the risk of accidental disclosure through misdirection or interception. This is best achieved by ensuring that the email is encrypted

13.0 Monitoring Compliance and Policy Review

The purpose of monitoring is to provide assurance that the agreed approach is being followed – this ensures we get things right, use resources well and protect our reputation. Any issues will be recorded on the Incident Reporting Form published on the SOS Medical Website, Nurse Lounge.

This policy will be reviewed annually or if new legislation comes into force.

14.0 Training

All staff employed by SOS Medical will undergo training for Information Governance and Data Protection. This will be refreshed every three years unless further training is indicated either by appraisal, complaints or incidents.

15.0 Data protection Impact assessments (DPIAs)

SOS Medical do not use DPIA's at present as we do not undertake high risk activities such as those listed below.

Examples of high-risk activities include:

- Using new technology
- Tracking anyone's location
- Processing genetic or biometric data (think 23andMe or DNA testing)
- Marketing to children

16.0 Do's and Don'ts

Do: Collect information legally and use it fairly

Don't: Mislead users about what you'll do with their private details

Do: Collect as little data as possible

Don't: Collect lots of data just because you can

Do: Protect data with strong security systems

Don't: Assume data will take care of itself

Do: Only store data for as long as necessary

Don't: Keep old data you don't need anymore

17.0 BREACH OF THIS POLICY

Consequences of Violating the GDPR Regulation

Companies that violate the EU General Data Protection Regulation face a maximum fine of €20 million ($23 million) or 4% of their annual global turnover (whichever is higher).

Summary of GDPR Data Breach Notifications

Under the GDPR, users must be notified if their data is compromised - for example through a breach or technical error.

According to **Article 33** of the European Union General Data Protection Regulation, a business must inform its supervisory authority of a data breach within 72 hours of when the problem is first discovered. Users must then be notified "without undue delay."

Data breach notifications are one of the most important changes introduced by the GDPR and are designed to keep companies accountable while giving users peace of mind.

What Is a 'Breach' Under GDPR?

Any incident that leads to personal data being **lost, stolen, destroyed, or changed** is considered a data breach.

Breach of this policy may result in disciplinary action.

18.0 DISPOSAL OF DATA

Where information is disposed of, employees should ensure that it is destroyed securely. This may involve the permanent removal of the information from the server, so that it does not remain in an employee's inbox or trash folder. Hard copies of information may need to be confidentially shredded. Employees should be careful to ensure that information is not disposed of in a wastepaper basket/recycle bin.

Employees of SOS Medical can contact the IT department for assistance in this matters.

If an employee is in any doubt about what they may or may not do with personal information, they should seek advice from Ankit Goyal and or Lorraine Gallier.

If they cannot get in contact them immediately, information should not be disclosed and should await contact.

19.0 Dissemination

This policy will be issued to all staff via SOS Medical website, Nurse Lounge. See also Appendix 3 which covers consent for staff information to be shared.

SOSMedical

Table 1 Appendix 1 *Explanation of terms*

What is a data subject?	I'm one and so are you. A data subject is anyone who has their data collected by a company. Basically everyone who ever used the internet.
What is a data controller?	A data controller is any entity that gathers and stores data — for example, a business.
What is a data processor?	This is who a large corporation hires to process data on their behalf. For example, a payroll company.
What is a supervisory authority?	Each country in the EU has its own supervisory authority. Like a data privacy sheriff, they enforce the GDPR in their region and hand out those hefty fines mentioned earlier.
What is a data protection officer (DPO)?	Companies and public bodies that process lots of data need to appoint an officer (DPO) to handle all their GDPR activities and paperwork.

Appendix 2 – Further legislation

Data Protection Act 1998 - Data protection principles

1. Personal data shall be processed fairly and lawfully.

2. Personal data shall be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Human Rights Act 1998

This Act binds public authorities including Health Authorities, Trusts, Primary Care Groups and individual doctors treating NHS patients to respect and protect an individual‟s human rights.

This will include an individual‟s right to privacy (under Article 8) and a service user‟s right to expect confidentiality of their information at all times.

Article 8 of the Act provides that ***“everyone has the right to respect for his private and family life, his home and his correspondence”.***

However, this article also states: “***there shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention or disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others”.***

Each organisation must act in a way consistent with these requirements. It must take an individual‟s rights into account when sharing personal information about them.

Freedom of Information Act 2000

This Act gives individuals rights of access to information held by public authorities.

Regulation of Investigatory Powers Act 2000

This Act combines rules relating to access to protected electronic information as well as revising the „Interception of Communications Act 1985‟. The Act aims to modernise the legal regulation of interception of communications in the light of the Human Rights laws and rapidly changing technology.

Crime and Disorder Act 1998

This Act introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in that local area.

The Act allows disclosure of person identifiable information to the Police, Local Authorities, Probation Service or the Health Service but only if the purposes are defined within the Crime and Disorder Act.

The Computer Misuse Act 1990

This Act makes it a criminal offence to access any part of a computer system, programs and/or data that a user is not entitled to access. Each organisation will issue an individual user id and password which will only be known by the individual they relate to and must not be divulged/misused by other staff. This is to protect the employee from the likelihood of their inadvertently contravening this Act.

Each organisation will adhere to the requirements of the Computer Misuse Act 1990 by ensuring staff are made aware of their responsibilities regarding the misuse of computers for personal gain or other fraudulent activities. Any member of staff found to have contravened this Act will be considered to have committed a disciplinary offence and be dealt with accordingly.

The Access to Health Records 1990

This Act gives patient‟s representatives right of access to their manually held health records, in respect of information recorded on or after 1 November 1991.

This Act is only applicable for access to deceased person’s records.

All other requests for access to information by living individuals are provided under the access provisions of the Data Protection Act 1998.

Access to Medical Reports Act 1988

This Act allows those who have had a medical report produced for the purposes of employment and/or insurance to obtain a copy of the content of the report prior to it being disclosed to any potential employer and/or prospective insurance company.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

This Act defines the scope for legitimate monitoring of communications within an organisation

Protection from Harassment Act 1997

This Act was passed following concern that stalking was not suitably dealt with under existing legislation, however it does not refer solely to stalking and covers harassment in a wider sense.

The Act says that it is unlawful to cause harassment, alarm or distress by a course of conduct and states that

"***A person must not pursue a course of conduct (a) which amounts to harassment of another, and (b) which he knows or ought to know amounts to harassment of the other."***

Equalities Act 2010

This Act states that it is unlawful to discriminate against a person in the workplace and wider society.

Appendix 3

GDPR CONSENT FORM

1. Do you consent for us using your personal information i.e. your email address and telephone number to send you emails and text messages regarding Available shifts and Marketing material?
   YES ☐ NO ☐

2. Do you consent for us using your personal information i.e. your email address and telephone number to send you compliance and training updates?
   YES ☐ NO ☐

3. Do you consent for us using your personal information i.e. your telephone number to call you regarding available shifts?
   YES ☐ NO ☐

4. Do you consent for us using your personal information i.e. your bank details to be used within our payroll department to process your pay?
   YES ☐ NO ☐

5. Do you consent for us to send your telephone number to our approved umbrella payroll companies when necessary i.e. when you are being paid via an umbrella company and are not being paid PAYE or via your Ltd. Company?
   YES ☐ NO ☐

6. Do you consent for us using your personal information where necessary i.e. when working with vulnerable groups to be sent to U-Check to obtain a DBS/ Access NI/ PVG?
   YES ☐ NO ☐

7. Do you consent to us saving a hard copy of your DBS/ Access NI/ PVG?
   YES ☐ NO ☐

8. Do you consent to us doing apply for DBS annually on your behalf via U-Check (unless you are on update services)?
   YES ☐ NO ☐

9. Do you consent for us sending your personal information such as your immunisations to Arumas Health Services to obtain a Fitness to work declaration
   YES ☐ NO ☐

10. Do you consent for us to approach external certificate issuers to verify your training certificates?
    YES ☐ NO ☐

11. Do you consent to us carrying out monthly PIN checks?
    YES ☐ NO ☐

12. Do you consent to us doing Home Office checks on your right to work where necessary?
    YES ☐ NO ☐

13. Do you consent for us to send your personal information on to hospital trusts?
    YES ☐ NO ☐

14. Do you consent for us to send your personal information to the NHS Staff Bank?
    YES ☐ NO ☐

15. DO you consent to us contacting your previous employers to obtain a reference?
    YES ☐ NO ☐

16. Do you consent for your personnel file being checked by an external auditor when the company has an audit?
    YES ☐ NO ☐

17. Do you consent for us to process your occupational health records to assess your suitability for work?
    YES ☐ NO ☐

18. Do you consent for us to send your occupational health records to prospective clients/employers so they can assess your suitability for their jobs?
    YES ☐ NO ☐

We will be keeping your data for the statutory retention periods. For a list of these, please visit www.sosmedical.co.uk

☐ I understand and agree to SOS Medical disclosing this information to their clients for the purpose of finding me assignments. I have read, understood and accept the information contained within the Staff Handbook I have read and agree to adhere to the SOS Medical Terms of Engagement.

☐ I consent to SOS Medical and its associated Companies for storing my details securely on its Database for the purpose of finding suitable assignments and advise me regarding medical services. I understand I can be offered work through SOS Medical.

Please note, if you wish to withdraw your consent for any of the above points please email info@sosmedical.co.uk with the required withdrawal changes and we will amend them for you

NAME: _____ DATE: _____

SIGNED: _____

Links and references

https://termly.io/resources/articles/gdpr-for-dummies

For more GDPR help, here are some useful resources:

- EU GDPR Homepage
- The ICO's GDPR Guide - This UK authority's guide is helpful for businesses in any country
- Termly's GDPR Resources — We have everything you need to be compliant with the GDPR, including a free privacy policy generator for your website

www.nhsbsa.nhs.uk/sites/default/files/2017-05/nhsbsa-data-protection-policy.pdf

www.england.nhs.uk/wp-content/uploads/2019/10/data-protection-policy-v5.1.pdf

Data protection - GOV.UK (www.gov.uk)