GI DOCTORS

GDPR Data Protection Policy

Issue Date = 1st December 2020
Version Number **= v1.0**

GI Doctors GDPR Data Protection Policy – Document Overview:

Policy name:	Data protection policy
Policy reference:	ICO GDPR Policy Document
Policy owner:	TBA
Policy writer(s):	TBA
Policy approver:	TBA

GI Doctors GDPR Data Protection Policy – Document Control:

Version no:	Approved by:	Date:	Key changes:	Sections affected:
Version 1.0	Pending	1st December 2020	None	None

GI Doctors GDPR
Data Protection Policy

Document Contents

Document Contents:

GI Doctors GDPR
Data Protection Policy

SECTION 1 - Policy Governance

This policy is owned by GI Doctors. TBA are the designated policy owners. The policy owners are responsible for ensuring the following:

- That this policy remains up to date.
- That this Policy is effectively implemented through appropriate process and procedural development, training and staff communication.
- That any lack of compliance with this policy is appropriately raised and dealt with and that any breaches to the policy, reported by either the business teams or the data compliance team, are addressed and reported as required.

This policy is designed to make clear to GI Doctors Clinical staff, Reception staff and site Managers their data protection responsibilities.

- The role of GI Doctors Clinical staff, Reception staff and site Managers is to ensure they understand their data protection responsibilities and act in accordance with GI Doctors data protection policy and procedures.
- The role of GI Doctors Managers is to ensure that site Clinical and Reception staff comply with this policy and to report breaches of this policy in accordance with GI Doctors breach procedures. This includes ensuring that all site staff have appropriate knowledge of and training in their data protection responsibilities and knowledge of and training in how to raise and report breaches to Senior Management.
- The role of TBA is to ensure it is carrying out effective monitoring to affirm that the standards laid down in this policy are being adhered to by all Clinical, and Reception staff and where they are not, to raise them as a matter of urgency with the Board and Senior Management.

GI Doctors GDPR
Data Protection Policy

SECTION 2 - Executive Summary

2.1 Policy Purpose:

The purpose of this policy is to articulate GI Doctors approach to data protection - providing details of the principles, ethos and approach GI Doctors takes to its data protection practices ensuring that it is treating its customers and data subjects fairly – thus ensuring positive outcomes for its customers and data subjects. It also provides details of how GI Doctors assures and monitors its data protection activities to ensure it is delivering positive customer outcomes and meeting the Information Commissioner's Office (ICO) and other related regulatory standards. GI Doctors is committed to limiting processing and maintaining the rights of data subjects.

The General Data Protection Regulation (GDPR) is enforceable in the UK from 25 May 2018. The GDPR is based on and builds out from the Data Protection Act 1998 (DPA). This policy is based on this legislation.

2.2 Policy Content Summary:

At GI Doctors, protection of the information we collect about the customers, individuals and Data Subjects with whom we deal, is at the heart of our intentions and actions. Carrying out our Data Protection responsibilities effectively and well is very important to us. The information, we collect, whether Personal Data or Sensitive Personal Data, must be managed, processed and stored appropriately irrespective of how it is collected or recorded.

Key changes from previous version

This is the first release of this document. In future release any changes will be listed here, along with the drivers leading to such changes.

2.3 Key Policy Monitoring Considerations:

It is the responsibility of stakeholders of GI Doctors to ensure that they are complying with the policy. It is also the responsibility of the Senior Management Team to raise and report any breaches to the operation or application of the policy to the Board of Directors and Share Holders. It is the responsibility of the Senior Management Team to monitor the organisation’s compliance with this policy.

GI Doctors GDPR
Data Protection Policy

SECTION 3 - Scope

3.1. Inclusions:

This policy applies to the following groups at GI Doctors:

- All permanent staff, temporary staff, contractors and any suppliers of data services.

The geographies covered by this policy are the territorial United Kingdom. The key organisation areas impacted by this policy are:

- Clinical (Dentists, Hygienists and Nurses).
- Administrative (Reception Staff).
- Technical (IT Support and Projects).
- Senior Management.
- Marketing and PR.
- Legal and Finance staff / contractors.
-

The key processes and procedures of the organisation impacted by this policy are:

- Patient History data gathering (both electronic and paper based).
- Patient Treatment Plans (both electronic and paper based).
- OPG and medical imaging data.
- General data protection.
- Information security
- Marketing
- Customer service etc.

The key stakeholders of the organisation impacted by this policy are:

- Clinical staff (Dentists, Hygienists and Nurses).
- Patients.
- The Board of Directors and Senior Management.
- Permanent staff, temporary staff, contractors, consultants and partners working with GI Doctors.
- Shareholders.

3.2. Exclusions:

This policy does not cover the following aspects, which are covered in other policies and should be read in conjunction with this policy:

- Clinical Policies.
- Specific and detailed information security policies such as:
    - Password policy
    - Email policy
    - Internet usage policy
    - Information classification policy

- Cryptographic controls policy
- Backup policy
- Mobile and remote working policy
- Public wi-fi policy
- Equipment Disposal and destruction policy
- Marketing Policies.

GI Doctors GDPR
Data Protection Policy

SECTION 4 - Purpose

This data protection policy is important to GI Doctors. GI Doctors is committed to collect, manage and store data on its patients and data subjects in a transparent manner that ensures that data is safe, protected and liable to cause no detriment to patients or data subjects.

GI Doctors also understands the importance of designing its products and services in such a way that ensures its patients and data subjects privacy is assured and that they are 'private by default'. GI Doctors also understands the importance of ensuring data subjects and customers have effective access to their data and can easily and simply request their data be amended or erased where incorrect or inappropriately collected, managed or stored.

This data protection policy is consistent with GI Doctors business objectives and planned corporate strategies. Furthermore this data protection policy is written to be compliant with the General Data Protection Regulation (GDPR). Its purpose is to ensure that all the GI Doctors stakeholders have a usable reference guide to help direct their attitudes and behaviors in relation to the proper collection, management and storage of data as laid out in the DPA and GDPR. It builds specifically on the eight data principles listed in the DPA and the subsequent guidance detailed in the GDPR.

The outcome that this policy is designed to foster is the safe, transparent and effective collection, management and storage of data to ensure the risk of customer and/or data subject detriment is minimised in all of GI Doctors services, products and activities.

GI Doctors GDPR
Data Protection Policy

SECTION 5 - Policy Statement

This data protection policy is a key reference document for all GI Doctors staff and key stakeholders. Collecting, managing and storing personal data in a transparent, safe and effective manner is of real importance to GI Doctors.

GI Doctors wishes to ensure that it is effectively collecting and protecting customer and data subject data in a manner that minimises the risk of detriment to those parties.

GI Doctors wishes to ensure that its staff and key stakeholders have access to this policy and have read and understood its contents and requirements. This is important to Gi Doctors as it expects all of its stakeholders to comply with the policy and its guidelines.

GI Doctors is committed to developing effective data protection processes and procedures to enact the ethos and standards contained within this policy.

GI Doctors is committed to ensuring that its staff and key stakeholders are appropriately informed of and trained in the data protection activities associated with this policy.

GI Doctors is committed to identifying, reporting and remediating any significant breaches to this policy to the data compliance team, the board and any external regulators as detailed in the guidelines within this policy.

GI Doctors will not tolerate a failure to abide by this policy and will take management action against those who fail to follow this policy and its guidelines.

Gi Doctors GDPR
Data Protection Policy

SECTION 6 - Policy Standards

This GI Doctors data protection policy has the following key policy standards.

6.1 Governance:

GI Doctors commits to put in place effective governance arrangements to ensure the management of data protection activities. These include:

6.1.1 - Discussion of GI Doctors data protection activities at board level on a monthly basis.

6.1.2 - If required by regulation, and/or deemed useful by the board, GI Doctors will appoint a data protection officer and establish their standing and their reporting arrangements in line with the GDPR requirements – specifically that they are able to report directly to the Board with independence

6.1.3 - The development of and approval by the Board of a GI Doctors data protection policy and associated processes that comply with the GDPR

6.1.4 - The set up and support of a suitable data compliance team to monitor data protection activities and report on compliance with the GDPR regulation to the Board and if necessary following a significant breach to ICO, affected individuals and other regulated authorities within the timeframe specified within the GDPR

6.2 New Staff (General)

GI Doctors commits to provide new staff and stakeholders who are not directly handling personal data with access to the data protection policy and associated training within one month of joining the firm.

6.3 Existing Staff (General)

GI Dictors commits to provide existing staff and stakeholders who are not directly handling personal data with access to the data protection policy and associated recap training annually.

6.4 New Staff (Data Handlers)

GI Doctors commits to provide new staff and stakeholders who are directly handling personal data with access to the data protection policy and associated training before they handle any client data.

6.5 Data Protection Impact Assessments

Where there is a possibility that GI Doctors will be engaging in a potentially high-risk data processing activity (see GDPR guidelines) then Gi Doctors commits to undertake a data protection impact assessment (DPIA).

6.6 Lawful Basis

GI Doctors also commits to reviewing, approving and documenting its 'lawful basis' for collecting data prior to collecting or processing new data sets.

6.7 Purpose

GI Doctors commits to only using the data it collects from data subjects for the purpose(s) it was collected. Further consent will be sought if the data is to be used in a different manner.

6.8 Rights

GI Doctors commits to respecting the rights of individuals in relation to the protection of their data as detailed in the GDPR and including:

6.8.1 - The right to be informed: GI Doctors, when collecting data, commits to inform individuals of the following:

6.8.1.1 - The firm's identity
6.8.1.2 - How the firm will use the information
6.8.1.3 - The lawful basis under which the data is being collected
6.8.1.4 - The duration the data will be retained for
6.8.1.5 - The individuals' right to and process for complaining to ICO

6.8.2 - **The right of access:** GI Doctors commits to respond to subject access requests:

6.8.2.1 - Within one month of receiving a request
6.8.2.2 - Without charge unless the request is manifestly unfounded or excessive
6.8.2.3 - Without refusal unless a clear and compelling reason for the refusal can be provided and details of the process for complaining are provided with the refusal.

6.8.3 - The right to rectification: GI Doctors commits to rectify any errant information within one month of it being acknowledged as errant by GI Doctors.

6.8.4 - The right to erasure: GI Doctors commits to erase any unwarranted information that it holds within one month of it being acknowledged as unwarranted by GI Doctors.

6.8.5 - The right to restrict processing: GI Doctors commits to restrict the processing of any information within one month of it being acknowledged as necessary to do so by GI Doctors.

6.8.6 - The right to data portability: GI Doctors commits to provide requested personal data in a structured commonly used and 'machine readable' form

6.8.7 - The right to object: GI Doctors commits to ensure that all individuals are provided with details about how to register a complaint with ICO at the time a complaint is raised

6.8.9 Rights in relation to automated decision making and profiling: GI Doctors commits to ensure that individuals' data is not used to make automated decisions or complete individual profiling without explicit consent.

6.9 Consent

GI Doctors commits to ensure that all data is collected with appropriate consent. Specifically that when data is collected the consent obtained is:

6.9.1 - Specific and granular in nature

6.9.2 - Clearly articulated in plain English
6.9.3 - Prominent within the collection process and documentation
6.9.4 - Requires the individual giving consent to opt-in
6.9.5 - Properly documented and stored
6.9.6 - Easily withdrawn
6.9.7 - Not gained from children under the age of 16 who do not have the ability to give informed consent without the consent of a parent or guardian

6.10 Duration:

GI Doctors commits to keeping its data in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

6.11 Quality:

GI Doctors commits to keep its data accurate and up to date and will take reasonable steps to ensure that personal data that is inaccurate with regard to the purposes for which it is processed, is erased or rectified within one month of being recognised as such.

6.12 Information Security:

Gi Doctors commits to ensure the appropriate security of the personal data it collects, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage by using appropriate technical or organisational measures. A number of these are detailed in separate information security policies.

6.13 International Data:

GI Doctors commits to the guidelines provided in GDPR and the DPA with regard to sharing data internationally and recognises that the level of protection afforded by GDPR must not undermined if any personal data is transferred outside of the European Union.

GI Doctors GDPR
Data Protection Policy

SECTION 7 - Policy Controls & Processes

7.1. Monitoring Structure

7.1.1 - It is the responsibility of the first line of defense (Clinical and Reception staff) to ensure that it is enacting and following the policy guidelines and meeting the policy standards.

7.1.2 - It is also the responsibility of the first line of defense (Clinical and Reception staff) to raise and report any breaches to the operation or application of the policy to the Senior Management Team and the Board of Directors.

7.1.3 - To support the first line of defense (Clinical and Reception staff) the Senior Management Team (the second line of defense) will carry out additional monitoring activities on both a scheduled and unscheduled basis:

7.1.3.1 - The scheduled monitoring will take place on a monthly and annual basis and will involve regular site checks to ensure that all data protection policies are being formally followed across all GI Doctors sites. These activities will review the first line of defense and carry out additional monitoring activities on both a scheduled and unscheduled basis as required.

7.1.3.2 - The unscheduled monitoring is likely to be triggered by a specific incident (e.g. a specific breach) and will review and assess compliance with any relevant aspects of the data protection policy or process.

7.2. Reporting Procedures

Gi Doctors takes very seriously the reporting of management information in relation to the carrying out of its data protection activities. In particular it is very aware of the need to and is committed to reporting significant breaches of the regulations to ICO as soon as is possible after the breach has come to the attention of the Senior Management Team and Board of Directors. All breaches should be reported to Senior Management immediately.

GI Doctors also acknowledges that on occasions it may also need to inform data subjects if they are impacted by a data breach and that GI Doctors is committed to ensuring it has the procedures in place to be able to carry this out if required.

GI Doctors expects, that in addition to the normal flow of management information (detailing any data related risks and issues) from the business areas handling data that the GI Doctors Board of Directors will receive a quarterly report from the Senior Management Team detailing the risks and issues generated by the monitoring it has completed in relation to GI Doctors data protection activities.

7.3. Policy Communication and Training

This data protection policy is stored in the Site CQC file each GI Doctors location maintains and can be accessed {directly or on request to the manager responsible for each Gi Doctors site by all key stakeholders.

In addition to the initial post-recruitment training provided by GI Doctors to all staff and the additional training provided to those staff handling data, GI Doctors commits to provide annual refresher training in data protection for all its staff and further commits to keep key stakeholders informed of (and if necessary, trained in) any changes made to the data protection policy. The Senior Management team will be asked to provide evidence on the quality and coverage of the requisite training as part of its reports to the board.

GI Doctors GDPR
Data Protection Policy

SECTION 8 - Policy Review & Update Process

Events that will trigger a policy review:

Standard Triggers:

- Calendar-based, annual review.
- Business change-based e.g. changes to business strategy or policies that relate to this policy.

Emergency Triggers:

- Incident-based e.g. as a result of identifying a major issue either during the monitoring process or as the result of an incident or breach that is the outcome of a weakness in the policy
- Regulatory-based e.g. as a result of the implementation of new regulation
- Customer sensitivity based e.g. as a result of customer perceptions changing that may require the policy to drive different outcomes or behaviors.

GI Doctors GDPR
Data Protection Policy

SECTION 9 - Definitions & Glossary

This section itemises a list of the key technical terms used within this policy document and provides a simple explanation of their meaning:

Board of Directors:
The team directly responsible to the Shareholders for the executive operations of the company.

Breach Management Policy:
The process, which is implemented in the occurrence of a data loss by GI Doctors.

Business Team:
Any specific function, department or division within the organisation that has 'first line' responsibilities for handling data and ensuring compliance with data protection regulations.

Business Manager:
The individual who heads up a business team, or in GI Doctors terms a Site Manager.

Controller:
A person or an organisation who determines the purposes and means of the processing of personal data. The processing may be carried out jointly or in common with other persons.

Data Compliance Team:
The compliance team is the individual who determines the purposes and means of the process of compliance of the organisation's business teams with the data protection regulations.

Data Protection Impact Assessment (DPIA):
The assessment required to be carried out by the organisation if its planned data collection/processing activity carries an inflated risk of detriment to customers or data subjects. See GDPR legislation for specific risk triggers.

Data Protection Officer:
An individual who has responsibility for informing and advising the firm and its employees about their obligations to comply with the GDPR and other data protection requirements; monitoring compliance with the GDPR; and acting as the first point of contact for supervisory authorities.

Data Services:
Services related to the collection, management, processing or storing of data.

Data Subject:
An identified, or identifiable natural person to whom data collected, stored or processed refers.

First Line of Defense:
A term that derives from the three lines of defense model where the first line of defense is the business, the second is the compliance function and the third is the audit function and board.

Information Security Policies:
The specific policies that relate directly to the securing and storage of data by the organisation.

Policy:
This specific data protection policy.

Policy Owner:
The individual responsible for the development and maintenance of the policy.

Policy Writer:
The individual responsible for drafting and updating the policy.

Processor:
A person or an organisation that processes data on behalf of the controller.

Personal Data:
Information relating to an identified or identifiable person (data subject). An identifiable person is one who can be identified directly or indirectly in particular by reference to an identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural or social identity.

Special Categories of Personal Data:
Article 9 of the GDPR sets out special categories of personal data. The processing of such personal data (which includes a) racial or ethnic origin; b) political opinions; c) religious or philosophical beliefs; and d) trade union membership) is prohibited, except where the data subject has given their explicit consent. There are other select circumstances.

GI Doctors GDPR
Data Protection Policy

SECTION 10 - Further Associated Reading

None specified or defined.

GI Doctors GDPR
Data Protection Policy

SECTION 11 - Associated Documents Table

Associated documents will include related policies, processes, how to guides and procedures. None are currently listed.

Document reference	Document Name	Hyperlink	Stored location
-	Data Protection Act	-	-
-	General Data Protection Regulation	-	-
-	General TCF GDPR guidance	-	-

End of Document