GP MATTERS LTD

Data Compliance & Security Policy

Data Compliance Policy

This Data Protection Compliance Policy sets out the steps taken by GP Matters Ltd to ensure that its data processing practices are in accordance with UK data protection law. GP Matters Ltd acknowledges that the personal data it processes is, and shall remain, the property of the Client/Patient. Upon termination of the contractual relationship with the Client/Patient, GP Matters Ltd (or other properly appointed responsible agent) will continue to hold the personal data on behalf of the Client/Patient. The Client/Patient reserves the rights to access their personal data in accordance with this data protection statement at any time. Personal data will not be given to any other third parties for any purpose. GP Matters Ltd has in place appropriate technical and organisational measures against the accidental, unauthorised or unlawful processing, destruction, loss, damage or disclosure of personal data and adequate security programmes and procedures to ensure that unauthorised persons do not have access to personal data or to any equipment used to process personal data. GP Matters Ltd provides individuals (including the Client/Patient HR) with the right of access, rectification, blocking, erasure and/or destruction available to such individuals under the applicable data protection laws in the UK. GP Matters Ltd acknowledges that the personal data it processes is, and shall remain; the property of the Client/Patient and it will return to the Client/Patient all copies of the relevant data upon termination of the contractual relationship with them as and when requested.

GDPR May 2018

The EU General Data Protection Regulation (GDPR) becomes enacted on the 25th May 2018 and will standardise data privacy and protection laws across Europe. The UK government is equally committed to this process. As a result, there may be some further fine tuning of this process following on from the Brexit transition. It will also affect companies outside of Europe as it applies to any entity that processes personal data tied to offering goods and services to, or monitoring behaviour of, European data subjects. The GDPR has implications for all healthcare service operators; with in the NHS and Private sectors.

GP Matters Ltd is very much aware of its obligations as a data processor under the GDPR and we are committed to discharging these obligations in a robust and professional manner. All the activities here at GP Matters Ltd remain underpinned by the same ongoing obligations regarding patient and client confidentiality and always remain an essential part of the core “duties of a doctor” and there are high expectations which are also enforceable by our professional body (General Medical Council) and this will continue in the same vein. This applies to Occupational Health (business to business) related activities just as much as it does for ordinary private GP services. As part and parcel of our ongoing GDPR compliance efforts we will continue to review, improve, refine and document our security measures to protect any of our patients and clients against any unauthorised access, use or disclosure of the content we protect. As well as providing direct private patient care, GP Matters Ltd also provides occupational and Company medical services on behalf of

third party employers and it is important that all service users and agents have confidence in all aspects of our service and the data that we must process to effectively do so.

The medical director (Dr Carole McAlister) is the Data Controller for GP Matters Ltd and will remain so and he will also be primarily responsible for dealing with any of the measures required to facilitate best practice and all related data/GDPR matters and taking full cognisance of the newly emerging legislation. Dr McAlister also welcomes any informal or other feedback about any of these statements and how they are interpreted by others (carole@gpmatters.com). We have (as per legislation) produced **a privacy notice** which is available on our website (www.gpmatters.com): Please go to the foot of any web page to click on the "data compliance policy" option. Furthermore, as part of our extensive obligations to the inspectorate here in Scotland (**Healthcare Improvement Scotland**) all policies (including those relating to data processing and the GDPR) are assessed and monitored by them for appropriate compliance.

What GDPR will mean for patients/staff?

Your data:

- Must be processed lawfully, fairly and transparently.
- Collected only for specific, explicit and legitimate purposes.
- Must be limited to what is necessary for the purposes for which it is processed.
- Must be accurate and kept up to date.
- Must be held securely.
- It can only be retained for as long as is necessary for the reasons it was collected.

Patients/staff rights:

- Being informed about how their data is used.
- To have access to their own data.
- To ask to have incorrect information changed.
- To restrict how their data is used.
- Move their patients/staff data from one organisation to another.
- To object to their personal information being processed (in certain circumstances).

The GDPR will supersede the current Data Protection Act (DPA). It is like the Data Protection Act (DPA) 1998, with which GP Matters Ltd already fully complies with: but further strengthens many of the DPA's principles.

The main changes are:

- The Practice must comply with Subject Access Requests (see appendix 1 – below) – a written signed request from an individual to see what information is held about them – like where we require your consent to process data. This must be freely given, specific, informed and unambiguous.
- New special protection for personal data.
- The Information Commissioner's Office must be notified within 72 hours of a data breach.
- Higher fines for data breaches.

There is a lot of guidance available on line to explain all these issues in much greater detail. The Information Commissioners Office website is generally highly informative and very reliable: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ Information for individuals is also available there; for example, a subject access request SAR) can be read about at: https://ico.org.uk/for-the-public/personal-information (or ask GP Matters Ltd reception/(see appendix 1 – below)
Existing patients and clients of GP Matters Ltd are very welcome to make direct contact with us at any time to make any kind of enquiry about their existing data and how this is stored/protected. Every effort will be made to reply to you as quickly as possible but initially, all queries will be dealt with only by the Medical Director. Thank-you for your forbearance and be rest assured, that for most of services provided by GP Matters Ltd; business and service will essentially continue along the same lines.

We will in due course be asking all existing users coming back for future appointments to review our new patient form (also on the website) and re-sign a copy for their GP Matters Ltd records: to update and refresh this professional service 'relationship'.
Thank-you.

Daniel Diez 19th November, 2018
Practice Manager

Privacy Notice for patients 2018
Further information on the Privacy Notice for Patients can be found on this webpage or by request (please email info@gpmatters.com) .

Security Policy
GP Matters Ltd has in place and undertakes to maintain appropriate technical and organisational measures against the accidental, unauthorised or unlawful processing, destruction, loss, damage or disclosure of data. Likewise, adequate security programs and procedures are in place to ensure that unauthorised persons do not have access to the data or to any equipment used to process the data.

Appendix 1

General Data Protection Regulation 2016 (GDPR)

Subject Access Request Form

The General Data Protection Regulation (GDPR) gives people the right to know what personal information an organisation has about them. To use this right, you can make what is known as a ‘subject access request’.

Only the following people may apply for access to personal information.

• The person who the information is about.

• Someone acting on behalf of the person who the information is about.

You have a right to know whether or not we have any information about you, and a right to have a copy of that information. You have a right to know the following.

• What kind of information we keep about you.

• The reason we are keeping it and how we use it.

• Who gave us your information

• Who we might share your information with and who might see your information.

You also have the right to have any codes or jargon in the information explained. You won’t be able to see information that could:

• Cause serious harm to your physical or mental health, or anyone else’s

• Identify another person (except members of NHS clinical staff who have treated the patient) unless that person gives their permission.

If you need any more advice about your rights under the General Data Protection Regulation, please contact the GP Matters Data Protection Officer or, you can contact the Information Commissioner’s Office:

Data Protection Officer Medical Director: Dr Carole McAlister, GP Matters, 87 Barrington Drive, Glasgow G4 9ES, tel 0141 339 0894, email: info@gpmatters.com

The Information Commissioner’s Office – Scotland 45 Melville Street Edinburgh EH3 7JL. Phone: 0131 244 9001 Email: Scotland@ico.org.uk

Fee

Data will be provided free of charge. There may be a charge of a ‘reasonable fee’ when a request is manifestly unfounded or excessive, particularly if it is repetitive.

A reasonable fee may occur when complying with requests for further copies of the same information. This does not mean that there will be a charge for all subsequent access requests.

The fee must be based on the administrative cost of providing the information.

Response time

We will deal with your request as quickly as possible and within 30 days of receiving your request. If we have any problems getting your information we will keep you up to date on our progress.

How long records are kept

The usual rules to do with keeping records are that:

• GP Matters records are kept for 20 years after last contact

• maternity records are kept for 25 years after the birth of the last child;

• children’s and young people’s records are kept until the child’s or young person’s 25th birthday;

• mental-health records are kept for 20 years after the date of the last contact.

This may help you in considering what types of records you are applying to see.

Points to consider

Making false or misleading statements to access personal information which you are not entitled to is a criminal offence.

Accessing health records and information is an important matter. Releasing information may in certain circumstances cause distress. You may want to speak to an appropriate health professional before filling in the form below.

GP MATTERS LTD

APPLICATION FORM FOR ACCESS TO HEALTH RECORDS
in accordance with the General Data Protection Regulation (GDPR)
DATA SUBJECT ACCESS REQUEST

This form must be completed in blue or black ink and signed in order for us to process your request.

Section 1: Patient details

Surname		**Maiden name**	
Forename		**Title (i.e. Mr, Mrs, Ms, Dr)**	
Date of birth		**Address:**	
Telephone number		**Postcode:**	
NHS number (if known)		**Hospital number (if known)**	

Section 2: Record requested

The more specific you can be, the easier it is for us to quickly provide you with the records requested. Record in respect of treatment for: (e.g. leg injury following a car accident)

Please provide me with a copy of all records held	
Please provide me with a copy of records between the dates specified below:	
Please provide me with a copy of records relating to the incident specified below:	
Please provide me with a copy of records relating to the condition specified below:	

Section 3: Details and declaration of applicant

Please enter details of applicant if different from Section 1

Surname		**Title (Mr, Mrs, Ms, Dr)**	
Forename(s)		**Address**	
Telephone number		**Postcode**	

Declaration
I declare that the information given by me is correct to the best of my knowledge and that I am entitled to apply for access to the health records referred to above under the terms of the GDPR.

Please tick:

⁄⁄ I am the patient

⁄⁄ I have been asked to act by the patient and attach the patient's written authorisation

⁄⁄ I have full parental responsibility for the patient and the patient is under the age of 18 and:
(a) has consented to my making this request, or
(b) is incapable of understanding the request (delete as appropriate)

⁄⁄ I have been appointed by the court to manage the patient's affairs and attach a certified copy of the court order appointing me to do so

⁄⁄ I am acting *in loco parentis* and the patient is incapable of understanding the request

⁄⁄ I am the deceased person's Personal Representative and attach confirmation of my appointment (Grant of Probate/Letters of Administration)

⁄⁄ I have written, and witnessed, consent from the deceased person's Personal Representative and attach Proof of Appointment

⁄⁄ I have a claim arising from the person's death (Please state details below)

Signature of applicant: ..... Date: ……..

You are advised that the making of false or misleading statements in order to obtain personal information to which you are not entitled is a criminal offence which could lead to prosecution.

Section 4: Proof of identity

Please indicate how proof of ID has been confirmed. Please select ‘A’ or ‘B’:

	Method in which identity is confirmed	**Option taken**	**Documents attached**
A	Attached copies of documents as noted in section 4A below	Yes/No	If Yes, please indicate here which documents have been attached
B	Countersignature (section 4B). This should only be completed in exceptional circumstances (e.g. in cases where the above cannot be provided)	Yes/No	Please indicate reason why this section was completed

4A – Evidence

Evidence of the patient’s and/or the patient’s representative identity will be required. Please attach copies of the required documentation to this application form. Examples of required documentation are:

	Type of applicant	**Type of documentation**
A	An individual applying for his/her own records	One copy of identity required, e.g. copy of birth certificate, passport, driving licence, plus one copy of a utility bill or medical card, etc.
B	Someone applying on behalf of an individual (Representative)	One item showing proof of the patient’s identity and one item showing proof of the representative’s identity (see examples in ‘**A’** above)
C	Person with parental responsibility applying on behalf of a child	Copy of birth certificate of child & copy of correspondence addressed to person with parental responsibility relating to the patient
D	Power of Attorney/Agent applying on behalf of an individual	Copy of a court order authorising Power of Attorney/Agent plus proof of the patient’s identity (see examples in ‘**A’** above)

4B – Countersignature

This section is to be completed by someone (other than a member of your family) who can vouch for your identity. This section may be completed if 4A cannot be fulfilled.

I (insert full name).....

Certify that the applicant (insert name).....

Has been known to me personally as ..... for .....years
(Insert in what capacity, e.g. employee, client, patient, relative etc.)

and that I have witnessed the signing of the above declaration. I am happy to be contacted if further information is required to support the identity of the applicant as required.

Signed .....Date .....

Name ..... Profession. .....

Address .....

.....

Daytime telephone number .....

Additional notes

Before returning this form, please ensure that you have:

a) signed and dated this form

b) enclosed proof of your identity or alternatively confirmed your identity by a countersignature

c) enclosed documentation to support your request (if applying for another person's records)

Incomplete applications will be returned; therefore please ensure you have the correct documentation before returning the form.

Form to be brought to Reception with identity documents or can be emailed, with scanned copies of ID to – info@gpmatters.com