Irish College of General Practitioners

Processing of Patient Personal Data:

A Guideline for General Practitioners v2.3

Authors: ICGP Data Protection Working Group

29 August 2019

Processing of Patient Personal Data: A Guideline for General Practitioners

File name: GP_GDPR_Guideline_v2.3.pdf
Date: 29/08/2019,
Version: 2.3
Governance: Irish College of General Practitioners (ICGP)
Authors: ICGP Data Protection Working Group

Document History

Date	Version	Comments
05/01/2018	0.1	First draft
25/01/2018	0.2	Editing of first draft, addition of multiple sections, addition of FAQs, addition of Appendices
02/02/2018	0.3	Editing of second draft, revision of tables, formatting
09/02/2018	0.4	Editing, formatting, inclusion of table captions
16/02/2018	0.5	Editing of the document in the context of a Guideline
27/02/2018	0.6	Editing following feedback from ICGP Working Group
28/03/2018	0.7	Editing following review by Office of the Data Protection Commissioner
03/04/2018	1.0	First public release version, following feedback from ICGP Working Group
26/04/2018	1.1	Added additional appendices, FAQs, and more detailed advice on information security audits
11/06/2018	1.2	Minor editing, additions to FAQs
19/10/2018	1.3	Changes to section 2c); addition of Appendix M; change to FAQ on PPSN; changes to the practice privacy statement around research; Bibliography links updated;
20/07/2019	2.0	Revision of document following publication of more information on application of GDPR in Ireland
08/08/2019	2.1	Addition of two new FAQs and revision of two others
23/08/2019	2.2	Minor re-wording and updates to bibliography
29/08/2019	2.3	Further additions to bibliography

Table 1 Document History

Disclaimer

The information contained in this document is for general guidance only and cannot be relied upon as legal advice. The ICGP accepts no liability for the accuracy of the information contained in this document and you should always obtain specific legal advice separately before taking any action based on the information provided herein or if you are unsure as to how to act in any situation.

Table of Contents

Part 1, Core Principles of Data Protection

1. Introduction

a) Purpose of the Guideline

Under the Charter of Fundamental Rights of the European Union, everyone has the right to respect for his or her private and family life, home and communications, and the protection of their personal data. A number of European and National Laws are in place to enforce these fundamental rights, detailing specific obligations when processing personal data.

Interpreting and applying some of these obligations by General Practitioners (GPs) is not always straightforward, particularly balancing the legitimate interest of the Data Subject against Data Protection obligations and requirements.

This document defines, as a Guideline, the requirements for GPs to be compliant with their data protection obligations. The document has been put together by the Irish College of General Practitioners (ICGP) as a service to GPs and their patients. The primary driver for this Guideline is the General Data Protection Regulation (GDPR). However this Guideline also references other related law, and National and European guidance. The GDPR took effect on May 25th 2018.

This Guideline is made up of three parts: the principles that general practitioners need to uphold, frequently asked questions that demonstrate how these principles apply, and appendices that help GPs and their support staff implement their data protection obligations in the practice.

b) Members of the Data Protection Working Group

The members of the Data Protection Working Group of the Irish College of General Practitioners are:

Dr Johnny Sweeney	National GPIT Project Manager (from January 2019)
Dr Brian O'Mahony	National GPIT Project Manager (up to December 2018)
Dr Conor O'Shea	National GPIT Co-ordinator and General Practitioner
Dr Brian Meade	National GPIT Co-ordinator and General Practitioner
Ms Niamh Killeen	ICT and Web Services Project Manager, Irish College of General Practitioners
Mr Brendan Fay	Head of Information Security Consultancy Practice, Ward Solutions Ltd
Mr John McWade	Information Security Consultant, Ward Solutions Ltd

Table 2 Members of ICGP Working Group on Data Protection Regulations

c) Scope and Application of the Guideline

This Guideline is specific to the handling of patient personal data in order to provide primary medical care whilst also ensuring GPs meet their data protection obligations.

It applies to patient personal data processed in all forms of media, including paper records, electronic records and documents, images, videos, SMS texts, online postings and electronic messages.

This Guideline does not cover the general processing of personal data in the context of employment or vendor personal data as other general guidance and requirements are available in these areas and are not specific to the general practice environment.
Nor does it cover areas where doctors are not working primarily as General Practitioners such as Occupational Health or Sports Medicine. GPs are advised to check with the relevant governing bodies for guidance on these areas of medicine.

d) Limitations and Cautions

There are many factors at play in relation to data protection. These include the EU General Data Protection Regulation (GDPR), the Irish Data Protection Act 2018, Department of Health regulations and the EU Article 29 Working Party guidance.

The interpretation of data protection regulations evolves continuously, and this Guideline will be reviewed periodically. Therefore, the Guideline will change over time as the implementation of data protection regulations become clear. The publication of this Guideline is to assist GPs in their implementation of GDPR, however it is important to check for the latest version of the Guideline which will be published on the ICGP web site at http://www.icgp.ie/data.

e) Definitions

The following definitions apply from Article 4 of GDPR:
'**consent**' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

> GPs need to be clear that we are discussing here the issue of consent for the processing of personal data and not the issue of consent for medical interventions. GPs should continue to seek and document informed patient consent for medical procedures and interventions such as immunisations and minor surgery.

'**controller**' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

> GPs are controllers of the data concerning health that they utilise to manage patient care. They process the information in the practice, using their GP practice software system, and they share the patient's personal data and data concerning health with recipients such as hospitals, consultants, and primary care teams. The hospitals and consultants with whom GPs share patient data concerning health are data controllers in their own right.

'**data concerning health**' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

‘**personal data**’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

‘**personal data breach**’ means 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;

‘**processing**’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

‘**processor**’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

> Examples of processors in the context of general practice are the GP practice software system vendors, providers of online data backup services, and Healthlink, the National electronic messaging broker.

‘**pseudonymisation**’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

‘**recipient**’ means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

2. Records of Processing Activities

As per Article 30 of GDPR, each data controller must maintain a Record of Processing Activities under their responsibilities. This record must contain:

a) the name and contact details of the data controller and, where applicable, the joint controller and the practice lead for data protection;
b) the purposes of the processing;
c) a description of the categories of data subjects and of the categories of personal data;
d) the categories of recipients to whom the personal data have been or will be disclosed;
e) where applicable, transfers of personal data to a third country;
f) the envisaged time limits for erasure of the different categories of data;
g) a general description of the technical and organisational security measures.

This section provides the records of processing activities in a typical GP practice. A template appears in the Appendices, allowing GPs to localise information on categories of data subjects, personal data and categories of recipients to their individual needs.

a) Identifying the Data Controller

If the general practice is a legal entity, then the practice is the data controller. Otherwise one or all of the GP Principals should be identified as the data controller or joint data controllers. The practice employees, GP Registrars in training and GP Locums are not data controllers.

b) Purpose of the Processing

In Ireland, the General Practitioner or Family Doctor provides life-long, cradle to grave, general medical services to individuals and families. The GP is the generalist in the health services and deals with patient problems across a range of specialties, everything from antenatal care to palliative care. The information collected and processed thus ranges from demographic information through physical, psychological and social data at all levels of granularity. The data ranges from the genetic aspects of a woman's breast cancer diagnosis to the trigger factors of a university student suffering from panic attacks and anxiety. The domain for this information is the domain of medicine in its broadest definition.

c) Categories of Personal Data

The following Table applies for both Public and Private Patients and shows the categories of personal data processed by GPs.

Category of Personal Data	Purpose of Processing	Lawfulness of Processing
Administrative: name, address, contact details (phone, mobile, email), dates of appointment	Necessary to support the administration of patient care in general practice	Article 6.1(d): processing is necessary in order to protect the vital interests of the data subject or of another natural person; Article 6.1(e): processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; Special Categories are processed under the derogations in Articles 9.2(h) and 9.2(i). Please see the notes under this table.
Medical Record: Individual Health identifier, GMS number, PPSN, date of birth, religion, sexual orientation, gender, family members, family history, contact details of next of kin, contact details of carers, vaccination details, medication details, allergy details, current and past medical and surgical history, genetic data, laboratory test results, imaging test results, near patient test results, ECGs, Ultrasound scan images, and other data required to provide medical care.	Necessary to provide patient care in general practice. The PPS number is needed for specific schemes such as sickness certification (Department of Social Protection), childhood immunisation programme, mother and child scheme, cervical screening, etc. (HSE). Please see Appendix M.	
Account Details: record of billable services provided, patient name, address, contact details, billing and payment records for GMS and private patients	Required for providing a service and billing. Also required for submission of reimbursement claims to the HSE Primary Care Reimbursement Service.	Article 6.1(c): processing is necessary for compliance with a legal obligation to which the controller is subject (Revenue, Medical and Legal Obligations), and Article 6.1(b) in relation to getting paid for providing a service to private patients.

Table 3 Categories of personal data processed by GPs

Notes on the Legal Basis for Processing of Data

It is not possible to undertake medical care without collecting and processing personal data and data concerning health. In fact, to do so would be in breach of the Medical Council's 'Guide to Professional Conduct and Ethics for Doctors'. The legal basis for processing of data by GPs is provided by the following articles in GDPR: Article 6.1(c), 6.1(d), 6.1(e) and Article 9.2(h) and 9.2(i).

Article 6.1(c) in relation to the lawfulness of processing states: 'processing is necessary for compliance with a legal obligation', for example for accounts and reimbursement claims.

Article 6.1(d) in relation to the lawfulness of processing, states: 'processing is necessary in order to protect the vital interests of the data subject or of another natural person'.

Article 6.1(e): in relation to the lawfulness of processing, states: 'processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller'. This includes the use of PPS numbers by GPs.

Article 9.2(h) in relation to the processing of special categories of personal data, states: 'processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3';

Paragraph 3 relates to the processing of data concerning health by medical practitioners subject to professional confidentiality under the regulation of the Irish Medical Council.

Article 9.2(i) relates to processing necessary for reasons of public health.

Article 6 and Article 9 need to work in conjunction with one another. So for instance a GP will rely upon a combination of Article 6 to process non sensitive data and Article 9 conditions to process special categories of data.

The processing of personal data in general practice is necessary in order to protect the vital interests of the patient and for the provision of health care and public health. The lawfulness of processing data for the provision of medical care in general practice is not based on consent.

However, explicit and informed consent is required for some defined data outflows, for example to insurance companies, solicitors and banks. This is covered in Section 3.

d) Categories of Recipients Whom We Share Personal Data

These are broken down into four categories as shown in the table below: sharing data in relation to the provision of medical care, sharing data with data processors where a contract is required, sharing data under legal arrangements, and sharing data for public health purposes.

Recipients with whom we share personal data

Categories of Recipient	Description
Health and Social Care Providers	Other GPs, Health Service Executive, Voluntary Hospitals, Private Hospitals and Clinics, Private Consultants, Physiotherapists, Occupational Therapists, Speech and Language Therapists, Social Workers, Palliative Care Services, Out of Hours Services, Pharmacies, Nursing Homes, Counselling Services, Diagnostic Imaging Services, Hospital Laboratories, Practice Support Staff, GP Locums and other health care providers
Data Processors, with a contract	GP Practice Software Vendors, Online Data Backup Companies, Healthlink
Legal Arrangements	Coroner, Revenue, Social Protection, Medical Council
Public Health	Infectious disease notifications, influenza surveillance, National Cancer Registry and other National Registries
Third Parties, with explicit patient consent	Solicitors, Insurance Companies, Health Insurance Companies, Banks

Table 4 Recipients with whom GPs share personal data

Health care is a community of trust. Each individual health care provider is subject to privacy and confidentiality ethics and rules overseen by their professional regulator, for example the Medical Council or the Nursing and Midwifery Board of Ireland. When a patient is referred by a GP to a Consultant this referral is discussed and agreed between the patient and the GP. As part of this decision is an understanding to be open and transparent, with all relevant medical information being shared with the Consultant in order to provide medical care. It is not possible to make a referral without sending the necessary information. In fact, to do so would leave the GP open to a medical negligence action. The transmission of personal data concerning health is part of the referral process and part of the practice of medicine. It does not need a separate signed patient consent form.

When sharing patient personal data with other data controllers in their own right, such as the HSE or Voluntary Hospitals, the responsibility for compliance with data protection regulations, including subject rights, falls to that party, for example, the Voluntary Hospital. There is a requirement to have appropriate governance arrangements in place where each entity understands their respective responsibilities.

e) Transfers to a Third Country

During standard operating procedures, patient records shall not be transferred outside of the European Economic Area (EEA). Where patient data is to be transferred, explicit consent will be sought having informed the patient of the risks of such transfers of the personal data outside of the EEA (Art 49.1(a)). In emergency situations where, for example, a patient has a medical event in the USA and needs their medical details transferred to support their care, or is physically or legally incapable of giving consent, this is allowable (Art 49.1(f)). It should, where possible, be associated with patient explicit consent, which should be retained for evidential purposes.

f) Time Limits

Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

The retention periods for medical records are taken from the HSE 'National Hospitals Office, Code of Practice for Healthcare Records Management". These periods are also in line with the recommendations of Medical Indemnity Agencies and the Health Information and Quality Authority (HIQA).

Type of Healthcare Record	**Retention Period**
General (adult)	8 years after last contact, unless in the interest of the Data Subject to retain *
Deceased persons	8 years after death
Children and young people (all types of records relating to children and young people)	Retain until the patient's 25th birthday or 26th if young person was 17 at the conclusion of treatment, or 8 years after death. If the illness or death could have potential relevance to adult conditions or have genetic implications, the advice of clinicians should be sought as to whether to retain the records for a longer period
Maternity (all obstetric and midwifery records, including those of episodes of maternity care that end in stillbirth or where the child later dies)	25 years after the birth of the last child
Mentally disordered persons (within the meaning of the Mental Health Acts 1945 to 2001)	20 years after the date of last contact between the patient/client/ service user and any healthcare professional employed by the mental health provider, or 8 years after the death of the patient/client/service user if sooner
Patients who have committed suicide (not included in mentally disordered persons as above)	10 years
Patients included in clinical trials	20 years
Cause of death certificate counterfoils	2 years

Table 5 Data retention periods for medical records

* At all times the interest of the patient must be to the forefront. If it is not in the interest of the data subject, then the medical records should not be deleted. For example, a 25-year-old man has treatment for a malignant melanoma and after recovery is not seen in the practice for 8 years. It would not be in the interest of the patient to delete his medical records. On the other hand, it would not be appropriate to retain data on an 87 year old woman who died 8 years ago, following a stroke, and had no history of a major mental health disorder.

g) Security Measures

The GP should commission regular information security audits to ensure that appropriate measures are in place to secure patient data in the practice. Such an audit should cover:

- Operating Systems and Security Patches;
- Hardware;
- Networks, including Wi-Fi;
- Anti-virus and anti-malware;
- Firewalls;
- Data Backup;
- Peripheral and medical devices;
- Access controls;
- Appropriate use of the Internet;

The information security audit should search for unencrypted patient identifiable information on the hard drives of practice computers and servers. Possible examples include downloaded electronic messages, GMS panel lists, referral and discharge letters, scanned documents and spreadsheets. Advice should be provided, by the information security auditors, on how to manage such files, whether through incorporation into the GP practice software management system, deletion, encryption at rest, or other means.

3. Compliance with Data Protection Principles

GPs are required to ensure all personal data is processed in line with the General Data Protection Regulation principles and good practices.

a) Lawfulness, Fairness and Transparency

GPs must ensure the lawful, fair and transparent processing of personal data. Section 2 of this Guideline provides GP Records of Processing Activities detailing the purpose of processing, lawfulness of processing, categories of recipients to whom the personal data will be disclosed, and envisaged time period for retention. Any processing activities outside of the areas detailed in Section 2 requires the practice to document the processing activity extensions in a similar form to Section 2.

In addition, a practice privacy statement should provide details to the data subject in a concise, transparent, intelligible and easily accessible form including:

- The identity and contact details of the data controller;
- The identity of the staff member with responsibility for data protection;
- What information is being collected;
- Purposes of processing;
- Recipients or categories of recipients with whom their data will be disclosed;
- Period of processing;
- Their rights;
- Lawful basis for the processing;

These privacy notices must be made available to data subjects when they register with the practice. It is recommended this notice is also displayed in general waiting areas in the practice. GPs should refer to Articles 12, 13 and 14 of GDPR in relation to what needs to be included in a privacy notice. A sample practice privacy statement is provided in the Appendices.

Where lawfulness is based on "consent"

The primary processing of patient personal data in general practice is necessary in order to protect the vital interests of the patient and for the provision of health care. The lawfulness of such processing in general practice is defined in Section 2 (lawfulness of processing) and is generally not based on consent.

However, there are specific processing conditions where consent is required, particularly when disclosing of personal data to recipients unrelated to the provision of medical or social care. GPs need to obtain explicit consent for these disclosures for example, sharing with Insurance Companies or Solicitors or Banks, and for other purposes which might not be obvious to the patient. The GP must be able to demonstrate that the data subject has consented to this processing, and this consent must be informed, freely given, and provided in a clear and transparent manner. Specifically, where the lawfulness of processing requires explicit consent, there shall be procedures for collecting this consent. The GP must also monitor all requests for removal or withdrawals of consent, document such requests in the patient record and ensure that all removals are completed without undue delay.

Overall the processing in the practice must be open and transparent and the patient should not be surprised by any disclosures outside of the practice.

b) Purpose Limitation

GPs are only permitted to collect and process information for an explicit purpose. If a general practice is carrying out any additional processing beyond what is normal practice, then it must be included in a GP's Record of Processing Activities as defined in Section 2 of this Guideline. There must also be a legal basis for such additional processing and it must be transparent to the patient.

c) Data Minimisation

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. GPs are only permitted to collect and process appropriate information to the extent needed for the provision of medical care and to comply with all applicable statutory, regulatory, contractual and/or professional duties.

d) Accuracy

Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

GPs must take all reasonable efforts to ensure the accuracy of the patient data. For example, if a patient has moved house from Galway to Ballinasloe, a record showing that he currently lives in Galway is obviously inaccurate. But a record showing that he once lived in Galway remains accurate, even though he no longer lives there.

However, a GP may legitimately wish to retain their opinion. For example, a misdiagnosis of a medical condition continues to be held as part of a patient's medical records even after the diagnosis because it is relevant for the purpose of explaining treatment given to the patient, or to additional health problems, and to protect the profession. It is acceptable to keep records of events that may have happened in error, provided those records are not misleading about the facts. In this scenario, the GP should add a note to clarify this within the patient record

e) Integrity and Confidentiality

The GP must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. The GP should commission regular information security audits to ensure that appropriate measures are in place to secure patient data in the practice. The audit should cover both technical and organisational aspects of information security. The results of the audit and the steps taken to resolve any issues identified should be recorded in the data protection accountability log.

f) Accountability

In order to be accountable under data protection regulations, there is a requirement on you to keep certain records. These include:

- Regular Information Security Audits;
- Records of Processing Activities, as shown in Section 2;
- Confidentiality agreements with Staff;
- Records of staff training and awareness;
- Processor contracts with GP Practice Software Vendors, Healthlink and any other data processors;
- Where processing on basis of consent, records of this consent;

Since the enactment of the Irish Data Protection Act 2018, GPs and GP Practices are no longer required to register with the Data Protection Commissioner. However, data controllers must show they are accountable in terms of GDPR, as shown above, in the list of records to be kept.

GP practices should display information on data protection regulations in their waiting room. A member of staff should be appointed to a lead role on data protection and should be available to patients to discuss any data protection questions and to facilitate access requests for medical records.

4. Compliance with Individual Rights

Patient personal data belongs to the individual, and individuals have a number of rights to their personal data. GPs must have procedures in place in the practice to support the individual rights discussed below.

a) Right to Access

Under Article 15 of GDPR, the patient, whether GMS or private, has a right to access a copy of their medical record. The GP shall provide a copy of the patient's medical record on receipt of a request or authorisation form. The request or authorisation form to satisfy these individual rights should be in writing or by email and should be signed by the Data Subject or legal guardian. An example of a request form for access to a medical record is shown in the Appendices.

The access request should be carried out as soon as possible, and no later than 30 days after the access request. No fee is chargeable for providing a copy of the medical record. It is important for the practice to verify the identity of the person making an access request or providing an access authorisation.

An individual can only make an Access Request for their own personal data. Legal guardians can also make an access request on behalf of a child. However, once a child is capable of understanding their rights to privacy and data protection, the child should normally decide for themselves whether to request access to data and make the request in their own name. This is not age dependent. It would also be important in such a case that the GP be satisfied that the person was genuinely acting on behalf of, and in the best interests of, the child whose data was being requested.

Revealing of medical information of a child who is capable of making decisions themselves will in most situations constitute a breach of the Data Protection Acts if undertaken without the consent of the child capable of making their own decisions.

The right to access may be restricted, as per Section 60 (5) of the Data Protection Act 2018, if the disclosure of the record to the patient 'would be likely to cause serious harm to the physical or mental health of the data subject'. In any situation where access is denied, the general practitioner must advise the patient of the reason invoked for the restriction either at the time access is denied or as soon as is advisable thereafter. In addition, only the part of the medical record likely to cause harm can be withheld, the rest of the medical record should be released in the usual way. The patient has a right to appeal the restriction to the Data Protection Commissioner.

b) Right to Rectification

Under Article 16 of GDPR, the patient has the right to obtain rectification of inaccurate patient data which is factually inaccurate. However, this is not an unqualified right and depends on the circumstances of each case (reference Irish Data Protection Commissioner case study 1 of 2007). A relevant dispute resolution may be addressed by the addition of a supplementary statement in the patient record. Inaccurate patient data should be noted as such.

For example, a patient may believe that a diagnosis of 'Depression' in their clinical record is inaccurate. This was the opinion of the GP at a point in time. The patient has the right for a note to be inserted in their clinical record that they disagree with the GP's diagnosis made at that time, but the contemporaneous record and clinical diagnosis by the GP does not have to be deleted or erased.

c) Right to Erasure

Article 17 of GDPR deals with the right to erasure. Because the GP has a requirement (Section 33 of Guide to Professional Conduct and Ethics for Registered Medical Practitioners, 8th Edition 2016) under Medical Council rules to keep medical records and also has a right to defend medico-legal claims, under Article 23.1(g) the right to erasure of medical records is not an absolute right and restrictions may apply. This would need to be examined on a case-by-case basis.

d) Right to Restriction of Processing

Article 18 of GDPR deals with the right to restriction of processing. Where a patient is in dispute with a GP, they may request that their medical record be locked or archived so that further processing of, or changes to, the record do not occur. The patient needs to be made aware that continuing medical care by the GP cannot take place while the medical record is locked. Requests from patients to restrict processing should be in writing and signed.

e) Right to Data Portability

The right to data portability, under Article 20 of GDPR, relates to circumstances where the processing is based on consent or a contract. Although this is not the case in general practice, the patient is entitled to receive a copy of their medical record in a format that allows them to transmit the data to another health care provider or GP. GPs should facilitate patients moving to another practice by providing their medical record in an electronic format where technically feasible or in a format which could be used by other GPs.

The protocol for transfer of medical records is for the receiving practice to provide a signed patient consent form for the transfer of medical records from the original or sending practice. The records should be transferred securely, for example using Healthmail, secure clinical email.

f) Right to Object

Individuals have a right to object at any time to processing of personal data for direct marketing purposes, in which case the personal data shall no longer be processed for such purposes. Other objections must be dealt with on a case-by-case basis.

g) Automated Individual Decision-making, Including Profiling

GPs do not base decisions solely on automated processing, and the point of view of the patient is central to any decision making in the provision of medical care.

5. Personal Data Breach Handling

"Personal Data breach" means 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.

Example of typical Data Breaches are:

- Misaddressing of e-mails/human error (sending a copy of a laboratory report or radiology result to the wrong patient);
- Loss or theft of data or equipment on which data is stored;
- Loss or theft of documents/folders;
- Unforeseen circumstances such as a flood or fire which destroys information;
- Inappropriate access controls allowing unauthorised use;
- A hacking/cyber-attack (such as ransomware);
- Obtaining information from the Practice by deception;

It is important to note that breaches also include the accidental loss of personal data (e.g. fire causing the loss of paper files). In addition, statistics indicate that most breaches are internal in nature and due to non-malicious user behaviour (e.g. loss of unencrypted laptop or USB, files etc.).

a) Notifying the Data Protection Commission

In the case of a personal data breach, the GP shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Data Protection Commissioner, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

b) Notifying the Data Subject

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay. The notification shall describe in clear and plain language the nature of the personal data breach and contain at least:

- The name and contact details of the data protection officer or other contact point where more information can be obtained;
- A description of the likely consequences of the personal data Breach;
- A description of the measures taken or proposed to be taken by the Practice to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects;

c) Data Breach Flow Chart and Examples

The Article 29 Data Protection Working Group has produced 'Guidelines on Personal data breach notification under Regulation 2016/679'. This is available at https://iapp.org/resources/article/wp29-draft-guidelines-on-data-breach-notification/

The Appendices to this ICGP Guideline include a data breach protocol and a data breach recording template.

6. Miscellaneous Provisions

a) Data Protection Impact Assessment (DPIA)

Data Protection Impact Assessments (DPIAs) are a method of assessing the level of data protection in place to safeguard patients' personal data. They are a useful learning process for practices and are helpful in identifying risk. DPIAs are important tools for ensuring good practice and accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate actions have been taken to ensure the correct measures are in place to protect the privacy of individuals.

A GP carrying out normal medical care for his or her patients and using an established and accredited GP practice software management system is not required to carry out a DPIA. We do not consider the processing of personal data by an individual general practice to be large-scale processing. In summary, DPIAs in general practice are a useful tool, are recommended, but are not mandatory.

Where a commercial organisation or company manages a number of different practices, or in the case of a large general practice, there may be a requirement for that organisation to undertake a Data Protection Impact Assessment.

It is important that any new projects, initiated by the HSE or other state agencies, that provide for the exchange of patient information should be subject to a DPIA before go live.

b) Data Protection Officers (DPO)

Article 37 of GDPR deals with the designation of a data protection officer (DPO). Recital 97 discusses the need to appoint a DPO 'where the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data'. We do not consider a general practice to be processing data on a large scale and thus do not believe that individual general practices need to appoint a DPO.

Where a commercial organisation or company manages a number of different practices, or in the case of a large general practice, there may be a requirement for that organisation to appoint a DPO.

Even when the GDPR does not specifically require the appointment of a DPO, general practices may sometimes find it useful to designate a DPO on a voluntary basis. The Article 29 Data Protection Working Party ('WP29') encourages these voluntary efforts.

c) Data Protection and Cyber Security Awareness and Training Details

It is the role of the data controller(s) to ensure that all staff have adequate awareness of and training for data protection and cybersecurity issues. A log of training activities should be maintained. Signed confirmation of training completed per employee should be retained.

d) Employee / Office Workers Confidentiality Agreements

Practice support staff, such as managers, secretaries, receptionists and allied health professionals must sign confidentiality agreements as part of their contract of employment. All staff joining and leaving the practice should be logged, including GP locums. Staff leaving the practice should have their access revoked, both to local and online applications and services, including backup services.

7. Bibliography

General Data Protection Regulation, GDPR, https://gdpr-info.eu

Medical Council Guide to Professional Conduct and Ethics for Doctors, http://www.medicalcouncil.ie/Existing-Registrants-/Professional-Conduct-and-Ethics/

Irish Data Protection Commissioner, https://www.dataprotection.ie/docs/Home/4.htm

Medical Records in Ireland, Medical Protection Society https://www.medicalprotection.org/docs/default-source/pdfs/Booklet-PDFs/ireland

Medical Records in General Practice, Medisec Ireland (available to Medisec members) https://medisec.ie/a-z/medical-records-in-general-practice

Working Party 29 Archived Material https://ec.europa.eu/newsroom/article29/news-overview.cfm

Managing Employee Data, Article 29 Working Party , Opinion 2/2017 on data processing at work, https://ec.europa.eu/newsroom/document.cfm?doc_id=45631

National Hospitals Office, Code of Practice for Healthcare Records Management, https://www.hse.ie/eng/about/who/qualityandpatientsafety/safepatientcare/healthrecordsmgt/

GPs as data controllers under the General Data Protection Regulation, British Medical Association (BMA) document, available at https://www.bma.org.uk/advice/employment/ethics/confidentiality-and-health-records/gps-as-data-controllers

Irish Data Protection Act 2018, available at https://data.oireachtas.ie/ie/oireachtas/act/2018/7/eng/enacted/a0718.pdf

Health Research Regulations 2018, available at http://www.irishstatutebook.ie/eli/2018/si/314/made/en/pdf

Health Research Board GDPR Guidance for health researchers, available at http://www.hrb.ie/funding/gdpr-guidance-for-researchers/

Data Sharing and Governance Act 2019, available at http://www.irishstatutebook.ie/eli/2019/act/5/enacted/en/html

Part 2, Frequently Asked Questions

Part 2 of this Guideline deals with Frequently Asked Questions.

Retirement or Death

Q1. I am a single-handed GP who is retiring shortly and facilitating a new doctor who has been appointed to my GMS list. What should I do with both my GMS and private patient records?

Answer (A). The incoming GP has a contract with the GMS and is entitled to the records of all patients on the GMS lists. It cannot be assumed that private patients will attend that GP, and records should be forwarded to that or other GPs on explicit consent from the Patient only. The existing (retiring) doctor should, however, maintain the patient medical records accumulated at that time for an adequate period consistent with meeting legal and other professional responsibilities. During that period, the provisions of the Data Protection Acts continue to apply to that information.

Transfer of Individual Records

Q2. I have received an email from a woman requesting that I forward the medical records of herself, her husband and her children to another GP in her new location. How should I proceed?

A. The fundamental rule is that an individual can only make an Access Request for their own personal data. Legal guardians can make an access request on behalf of a child or person incapable of making a request themselves. However, once a child is capable of understanding their rights to privacy and data protection, the child should normally decide for themselves whether to request access to data and make the request in their own name (this is not age dependent). It would also be important in such a case that the GP be satisfied that the person was genuinely acting on behalf of, and in the best interests of, the child whose data was being requested.

Revealing of medical information to a spouse, former spouse, or child who is capable of making decisions themselves will in most situations constitute a breach of the Data Protection Acts if undertaken without the consent of the other spouse, former spouse, or child capable of making their own decisions.

Solicitor Requests

Q3. A solicitor has sent me a letter, with patient consent attached, requesting that I send the solicitor the entire patient record including third party correspondence. The patient record contains several sensitive entries which have nothing to do with the personal injury claim he is pursuing. Am I ok to do this?

- Under Data Protection legislation the patient has an entitlement to this information. However, before releasing to the solicitor, you should confirm with the patient that they do indeed want *all* medical information to be released. You should ensure that it contains nothing that might be injurious to the patient's wellbeing, or to that of someone else referred to in the records.

It may be possible to provide the patient with an abstract of the medical record relevant to the claim which would satisfy the needs of the solicitor. It may also be appropriate to notify a colleague that a particular letter or result is being released, however you should not withhold it.

Data Access Request

Q4. A mother has requested access to her 16 year old daughter's medical record. How should I respond?

A. An individual can only make an Access Request for their own personal data. Legal guardians can also make an access request on behalf of a child. However, once a child is capable of understanding their rights to privacy and data protection, the child should normally decide for themselves whether to request access to data and make the request in their own name (this is not age dependent). It would also be important in such a case that the GP be satisfied that the person was genuinely acting on behalf of, and in the best interests of, the child whose data was being requested. Revealing of medical information of a child who is capable of making decisions themselves will in most situations constitute a breach of the Data Protection Acts if undertaken without the consent of the child capable of making their own decisions.

Health Insurance Company Requests

Q5. A patient of mine recently had a procedure in a private hospital. Her insurer is now requesting further information from me. Have they a right to this?

A. This is the patient's personal data. You must have the patient's explicit consent and must only release information which the Data Subject has explicitly consented to. It might be reasonable to suggest that the insurance company contact the consultant who performed the procedure and with whom they have a contract. Our advice would be to disclose to the patient themselves and allow them to disclose to whomever they wished.

Freedom of Information Requests

Q6. A General Medical Services (GMS) patient has submitted a Freedom of Information Request for their medical record. How should I proceed?

A. The HSE is a designated body under the Freedom of Information 2014. The medical card patient should submit the FOI request to the HSE and the HSE will then ask you for a copy of the patient's record. If there is a risk that disclosure of the record would be harmful to the patient, you should point this out to the HSE.

Phone Requests

Q7. A social worker who I don't know telephones me because of possible child abuse/neglect concerns relating to a child patient of mine. They want to know if I have any concerns about this child, its siblings or parents. How should I respond?

A. The general principle under Child Protection legislation is that the safety and well-being of children take priority. However, if you have any suspicion about the nature of the request, you should take steps to verify the identity of the caller. A written request from the

Department of Social Work, which explains the basis for seeking information, is required in most cases.

Email Communication

Q8. It would make life a lot easier for the practice if I could email results to patients. If I have the patient's permission, is it ok to do this?

A. If there is a specific request by email from a patient to send their results back by that format, then it is reasonable to acquiesce to that request. However, if you are contemplating a standardised process of returning results, you should restrict the content of any message, and consider the potential for a data breach. You should keep the information exchanged to a minimum. An explicit and informed request from the patient should be recorded.

Faxes

Q9. Is it OK to use Faxes in general practice?

A. Where possible, transmission of personal health information by Fax should be avoided. GPs are encouraged to use Healthlink and Healthmail, secure clinical email, to transfer confidential patient identifiable clinical information. Where medical information is required urgently, and a more secure mechanism is unavailable the following measures should be considered in relation to the use of Faxes:

- Ensure that the fax number to which the patient information is being sent is correct. Where an auto-dial function is being used, it is important to verify the recipient fax number from time to time to ensure that it has not been changed.
- Ask the recipient to confirm by phone that they have received the faxed document.
- Fax machines used for transmitting or receiving confidential information should be in secure areas not accessible to the general public.
- A fax cover sheet which clearly identifies the sender and intended recipient should be used. The fax cover sheet should also indicate that the information is confidential. Possible wording for a fax sheet is as follows

CONFIDENTIALITY *NOTICE:*
The information contained in this facsimile message is privileged and confidential information intended for the use of the individual or entity named above. If you have received this fax in error, please contact us immediately and then destroy the faxed material.

Use of Healthmail

Q10. Can I use email to send patient identifiable clinical information?

A. Documents sent by normal email are not secure and can be accessed inappropriately by others before reaching their intended recipients. Healthmail, secure clinical email, is an HSE service that allows exchange of patient identifiable clinical information between GPs and HSE clinicians and between GPs and voluntary, maternity and children's hospitals. Healthmail is suitable for the electronic exchange of patient identifiable clinical information, including attachments. The GP is the data controller of his or her Healthmail account.

SMS Texts

Q11. Is it OK to use SMS texts in general practice?

A. If you use SMS texts, you need to have a practice policy in place that covers consent, appropriate age groups, content of texts and confidentiality. Please refer to the 2018 ICGP Quality in Practice Committee document entitled 'Text Messaging In Irish General Practice'.

Access to Clinical Records by Secretarial and Administrative Staff

Q12. Is it appropriate for practice support staff to have access to the patient's medical record?

A. Access to patient records should be regulated to ensure that they are used only to the extent necessary to enable the secretary or manager to perform their tasks for the proper functioning of the practice. In that regard, patients should understand that practice staff may have access to their records for:

- Identifying and printing repeat prescriptions for patients. These are then reviewed and signed by the GP.
- Generating a social welfare certificate for the patient. This is then checked and signed by the GP.
- Typing referral letters to hospital consultants or allied health professionals such as physiotherapists, occupational therapists, psychologists and dieticians.
- Opening letters from hospitals and consultants. These could be clinic letters or discharge letters. The letters could be appended to a patient's paper file or scanned into their electronic patient record.
- Scanning clinical letters, radiology reports and any other documents not available in electronic format.
- Downloading laboratory results and Out of Hours Coop reports and performing integration of these results into the electronic patient record.
- Photocopying or printing documents for referral to consultants, attending an antenatal clinic or when a patient is changing GP.
- Checking for a patient if a hospital or consultant letter is back or if a laboratory or radiology result is back, in order to schedule a conversation with the GP.
- When a patient makes contact with a practice, checking if they are due for any preventative services, such as influenza vaccination, pneumococcal vaccination, ante natal visit, contraceptive pill check, cervical smear test, overdue childhood vaccination, etc.
- Handling, printing, photocopying and postage of medico legal and life assurance reports, and of associated documents.
- Sending and receiving information via Healthmail, secure clinical email.
- And other activities related to the support of medical care appropriate for practice support staff.

All persons in the practice (not already covered by a professional confidentiality code) should sign a confidentiality agreement that explicitly makes clear their duties in relation to personal health information and the consequences of breaching that duty.

GP Practice Software Management system should provide an audit log of when patient information has been accessed, and by whom. Such an audit log makes it possible for the data controller in a practice to detect any unauthorised access to personal health information.

Incidental Access to information

Q13. Certain non-practice members may have access to patient records when they are in the practice. These include medical students, HSE or pharma employed nurses, IT support staff and cleaners. How do we handle this?

A. You should take reasonable precautions to ensure that patient information is protected from unintended use. In the circumstances mentioned above, it is reasonable to ask those individuals to sign a confidentiality agreement.

Research Projects

Q14. Do I need a patient's consent to enrol them in research projects?

A. The capture and sharing of clinical patient information for research purposes should be anonymised. Exceptions to this arise where legislation is in place to allow analysis and research on patient identifiable clinical information. Examples of this include the National Cancer Registry and Infectious Disease regulations. Where research involves identifiable patient clinical information, explicit patient consent must be sought by the GP and documented in the patient record. Where the data is anonymised, it is no longer personal data and data protection regulations do not apply. It will be a matter for each GP to carry out an assessment in this regard and to review that assessment periodically to ensure that the data remain anonymous or unlikely to be re-identified.

In general, the concept of data minimisation and anonymization should be maintained. Where informed patient consent is used as the legal basis for research, the data controller must be able to demonstrate that consent has been forthcoming and must allow for the right of the patient to withdraw consent at any time. Researchers must comply with the Health Research Regulations 2018.

Employment Data

Q15. With regards to the record of processing activity the template is just for the patient data but I'm assuming that under GDPR we have to record the processing of staff employment data as well. Can you confirm that we need to do that?

A. The scope of the ICGP Guideline on Data Protection is the processing of patient data. This ICGP Guideline document does not cover employment data, but GPs as employers do need to manage employment data under GDPR. GPs should refer to other sources of information for the processing of employment data, including the advice from the Article 29 Working Party 'Opinion 2/2017 on data processing at work – wp249' available here.

Personal Public Service number (PPS number)

Q16. Can a GP ask for a patient's PPS number?

A. GPs are not specified bodies under the Social Welfare Acts, but they may ask patients for their PPSN as part of specified HSE schemes such as the Mother and Child scheme, Childhood Immunisations and Cervical Screening or Sickness Certification for the Department of Social Protection. The Data Protection Commissioner acknowledges that entities such as the Department of Social Protection (DSP) or the HSE are legally permitted to seek the PPSN in the context of the provision of a service.

The PCRS Circular 027/18, shown in Appendix M, states that for GPs operating under a contract of service "the use of and the retention of an eligible person's PPSN is a prerequisite in the provision of general practitioner medical and surgical service to that person, or to his/her spouse or partner and child dependants that are also eligible to such services". This should provide reassurance to GPs that having obtained and stored a PPSN, it is reasonable to retain that number in the patient medical records, for purposes of audit if necessary or further lawful use. We would still advise that the capture of the PPSN must not be made on a "just-in-case" basis or be used as a practice identifier.

Picking Up Prescriptions

Q17. We have a lot of people who would have their prescriptions or sick certs picked up by someone else for various reasons, for example, it could be an elderly parent, or a person with mobility problems. Can you please advise if this is okay to do so now?

A. It is important to be clear about the duties and responsibilities of the data controller. You have a duty to keep the patient's information private and confidential and only to share information with a third party if patient consent to do so is in place. Thus, for example, giving a prescription out to the wrong patient would be a data breach and giving a copy of laboratory results out to the wrong person would be a data breach.

When it comes to third parties picking up prescriptions and social welfare certs on someone else's behalf, you should consider the following:

- Does this behaviour expose the practice to a data breach?
- If so, how can I best minimise this exposure while fulfilling my duty of care to the patient and ensuring the practice can continue to function?
- Should all certs and prescriptions being collected by third parties go in an envelope addressed to the patient and marked 'private and confidential'?
- Should I require that signed patient consent be documented in the notes before a prescription can be picked up by a third party?
- In urgent cases, should verbal patient consent be recorded in the patient notes before collection by a third party?

This is a new issue for GPs and practice staff. It is likely that advice will evolve as experience is gained at the front line.

Destruction of medical records

Q18. Our Practice has boxes of old medical records in an attic above our surgery. These are over 20 years old and many of the patients are now deceased. Can we just shred these?

Data protection law applies to both paper and electronic records. Some of the paper records in these boxes may belong to current patients of the practice and therefore must be kept. If conditions in your attic pose a risk to the security or integrity of these records they should be scanned and retained in an electronic format. In general, where patients are deceased or have not been active for more than eight years, you would be within your rights to securely dispose of these records. There are several exceptions to this however and Section 2.f of this guideline covers this issue in more detail. If you use an outside contractor to dispose of your old medical records, you will need to get them to sign a confidentiality agreement and they should provide you with a certificate confirming that the files have all been destroyed.

In summary while it is correct to dispose of obsolete medical records especially if they are at risk of being damaged, care is required in choosing which ones to retain and which to destroy.

Access to deceased patient records

Q19. The estranged wife of one of my deceased patients is seeking a copy of his medical records. Is she entitled to receive these under GDPR?

Data protection legislation does not apply to the records of your deceased patients and instead your decision must be based on Medical Council guidelines and other legislation such as the Freedom of Information Act. This area can get quite complicated but in general you owe the same duty of confidentiality to your patient now as when he was alive. If it is your view that he would have been unlikely to consent to the release of the records when he was alive, or the records contain information of a highly sensitive nature then seek legal advice.

If the deceased was a GMS patient, then the estranged wife could apply for access to the HSE under the Freedom of Information Act. The same principles will apply here, and access is unlikely to be granted unless there is a sound reason for the request. If disclosure could cause harm to the reputation of the deceased or cause distress to those who knew him this would have to be taken into consideration also.

Part 3: Appendices

Appendix A: Data Protection Check List

It is good practice to review this check list annually. This check list should form part of your data protection accountability folder.

Tasks	Yes	No
1. Have you voluntarily adopted this document: 'Processing of Patient Personal Data: A Guideline for General Practitioners'?		
2. Have you commissioned an information security audit of your practice computers and network?		
3. Have you identified a person in the practice with responsibility for data protection?		
4. Have you reviewed your records of processing activities to ensure all your data processing and data outflows are documented? See Part 1, Section 2 of Guideline.		
5. Have you started to be accountable for data protection by assembling a folder of the required documents and by keeping a log of activities? See Part 1, Section 3(g) of Guideline.		
6. Are you using Healthmail, secure clinical email, and eReferrals to transmit patient identifiable clinical information within the healthcare environment?		
7. Do you have confidentiality agreements in place with your practice support staff?		
8. Do you have data processing agreements in place with your GP Practice Software Vendor, your online backup service, Healthlink and any other data processors you use?		
9. Do you have processes in place to manage individual subject rights, such as the right to access? See Part 1, Section 4 of Guideline.		
10. Do you have a protocol in place to manage a Data Breach? See Part 1, Section 5 of Guideline.		
11. Have you identified the person or legal authority that is the data controller in your practice?		
12. Do you have a practice privacy statement on display in the waiting room and available to patients?		

Check List Reviewer:

Date of Review:

Appendix B: Sample Request for Transfer of GP Records

Dr Joseph Bloggs
Anytown Medical Centre
Main Street, Anytown
Phone: 01 123456

<*Date*>

To: *<GP Name>*
<GP Address>

Re: *<Patient Name>* **DOB:** *<Patient DOB>*

Dear *<GP Name>*
The above has decided to register with this practice. I would be grateful if you could send me a copy of their medical records. Signed patient consent in accordance with Data Protection Regulations has been provided below.

Yours Sincerely

_____
Dr Joseph Bloggs (M.C.R. 34567)

PATIENT SECTION

<*Date*>

I _____ (PRINT NAME)
consent to the release of my medical records to Dr Bloggs

_____
Patient Signature

Appendix C: Request form for Access to Medical Records

Access Request for Medical Records

I wish to obtain a copy of the medical record held at:

Practice

Name of Practice	
Name of General Practitioner	

Patient

First Name	
Family Name	
Date of Birth	
Address	
Signature	
Date	

For Practice Use Only:
Date request received:
Method of identification:
Date record provided:
Person managing access request:

Notes:
No fee is chargeable for providing a copy of the medical record. It is important for the practice to verify the identity of the person making an access request or providing an access authorisation.

Data Protection Regulations

Medical Records

A General Practice is a trusted community governed by an ethic of privacy and confidentiality.

In order to provide for your care, we need to collect and keep information about you and your health in your personal medical record.

Our policies are consistent with the Medical Council guidelines and the privacy principles of the Data Protection Regulations.

This practice has voluntarily adopted the requirements of 'Processing of Patient Personal Data: A Guideline for General Practitioners'.

For further details please ask at reception for a copy of our Practice Privacy Statement or access the Guideline at http://www.icgp.ie/data

Thank you.

Appendix E: Practice Privacy Statement

Practice Name	
Practice Address	
Practice Phone Number	
Data Controller	
Lead for Data Protection	

Practice Privacy Statement

This Practice wants to ensure the highest standard of medical care for our patients. We understand that a General Practice is a trusted community governed by an ethic of privacy and confidentiality. Our approach is consistent with the Medical Council guidelines and the privacy principles of the Data Protection Regulations. It is not possible to undertake medical care without collecting and processing personal data and data concerning health. In fact, to do so would be in breach of the Medical Council's 'Guide to Professional Conduct and Ethics for Doctors'. This leaflet is about advising you of our policies and practices on dealing with your medical information.

Legal Basis for Processing Your Data

This practice has voluntarily signed up for the ICGP Data Protection Guideline for GPs. The processing of personal data in general practice is necessary in order to protect the vital interests of the patient and for the provision of health care and public health. You can access the Guideline at http://www.icgp.ie/data. In most circumstances we hold your data until 8 years after your death or 8 years since your last contact with the practice. There are exceptions to this rule and these are described in the Guideline referenced above.

Managing Your Information

In order to provide for your care here we need to collect and keep information about you and your health on our records.

- We retain your information securely.
- We will only ask for and keep information that is necessary. We will attempt to keep it as accurate and up to-date as possible. We will explain the need for any information we ask for if you are not sure why it is needed.
- We ask you to inform us about any relevant changes that we should know about. This would include such things as any new treatments or investigations being carried out that we are not aware of. Please also inform us of change of address and phone numbers.
- All persons in the practice (not already covered by a professional confidentiality code) sign a confidentiality agreement that explicitly makes clear their duties in relation to personal health information and the consequences of breaching that duty.

- Access to patient records is regulated to ensure that they are used only to the extent necessary to enable the secretary or manager to perform their tasks for the proper functioning of the practice. In this regard, patients should understand that practice staff may have access to their records for:
  - Identifying and printing repeat prescriptions for patients. These are then reviewed and signed by the GP.
  - Generating a sickness certificate for the patient. This is then checked and signed by the GP.
  - Typing referral letters to hospital consultants or allied health professionals such as physiotherapists, occupational therapists, psychologists and dieticians.
  - Opening letters from hospitals and consultants. The letters could be appended to a patient's paper file or scanned into their electronic patient record.
  - Scanning clinical letters, radiology reports and any other documents not available in electronic format.
  - Downloading laboratory results and Out of Hours Coop reports and performing integration of these results into the electronic patient record.
  - Photocopying or printing documents for referral to consultants, attendance at an antenatal clinic or when a patient is changing GP.
  - Checking for a patient if a hospital or consultant letter is back or if a laboratory or radiology result is back, in order to schedule a conversation with the GP.
  - When a patient makes contact with a practice, checking if they are due for any preventative services, such as vaccination, ante natal visit, contraceptive pill check, cervical smear test, etc.
  - Handling, printing, photocopying and postage of medico legal and life assurance reports, and of associated documents.
  - Sending and receiving information via Healthmail, secure clinical email.
  - And other activities related to the support of medical care appropriate for practice support staff.

Disclosure of Information to Other Health and Social Care Professionals
We may need to pass some of this information to other health and social care professionals in order to provide you with the treatment and services you need. Only the relevant part of your record will be released. These other professionals are also legally bound to treat your information with the same duty of care and confidentiality that we do.

Disclosures Required or Permitted Under Law
The law provides that in certain instances personal information (including health information) can be disclosed, for example, in the case of infectious diseases.

Disclosure of information to Employers, Insurance Companies and Solicitors:
- In general, work related Medical Certificates from your GP will only provide a confirmation that you are unfit for work with an indication of when you will be fit to resume work. Where it is considered necessary to provide additional information we will discuss that with you. However, Department of Social Protection sickness certs for work must include the medical reason you are unfit to work.
- In the case of disclosures to insurance companies or requests made by solicitors for your records we will only release the information with your signed consent.

Use of Information for Training, Teaching and Quality Assurance
It is usual for GPs to discuss patient case histories as part of their continuing medical education or for the purpose of training GPs and/or medical students. In these situations the identity of the patient concerned will not be revealed.

In other situations, however, it may be beneficial for other doctors within the practice to be aware of patients with particular conditions and in such cases this practice would only communicate the information necessary to provide the highest level of care to the patient.

Our practice is involved in the training of GPs and is attached to a General Practice Training Programme. As part of this programme GP Registrars will work in the practice and may be involved in your care.

Use of Information for Clinical Audit
It is usual for patient information to be used for clinical audit in order to improve services and standards of practice. GPs on the specialist register of the Medical Council are required to perform yearly clinical audits. Information used for such purposes is done in an anonymised or pseudonymised manner with all personal identifying information removed.

If it were proposed to use your information in a way where it would not be anonymous or the Practice was involved in external research we would discuss this further with you before we proceeded and seek your written informed consent. Please remember that the quality of the patient service provided can only be maintained and improved by training, teaching, audit and research.

Your Right of Access to Your Health Information
You have the right of access to all the personal information held about you by this practice. If you wish to see your records, in most cases the quickest way is to discuss this with your doctor who will review the information in the record with you. You can make a formal written access request to the practice and receive a copy of your medical records. These will be provided to you within thirty days, without cost.

Transferring to Another Practice
If you decide at any time and for whatever reason to transfer to another practice we will facilitate that decision by making available to your new doctor a copy of your records on receipt of your signed consent from your new doctor. For medico-legal reasons we will also retain a copy of your records in this practice for an appropriate period of time which may exceed eight years.

Other Rights
You have other rights under data protection regulations in relation to transfer of data to a third country, the right to rectification or erasure, restriction of processing, objection to processing and data portability. Further information on these rights in the context of general practice is described in the Guideline available at http://www.icgp.ie/data. You also have the right to lodge a complaint with the Data Protection Commissioner.

Questions

We hope this leaflet has explained any issues that may arise. If you have any questions, please speak to the practice secretary or your doctor.

Appendix F: Data Protection Accountability Log

Overview
One of the new principles of GDPR is to be accountable for how you collect, hold and manage patient data. You need to be able to demonstrate to the Data Protection Commissioner (DPC) that you are upholding your responsibilities as a data controller for sensitive personal health information. The DPC will audit general practices to ensure they are accountable under GDPR.

Accountability Log
To demonstrate that you are accountable, you need to keep a log. Consider this as akin to your Professional Competence log. In this accountability log you will document:

- Named data protection lead person within the practice;
- External training sessions on GDPR, such as CME meetings, ICGP meetings, online courses
- Internal training sessions for clinicians and support staff on GDPR;
- Yearly information security audits of your practice hardware, software, networks, anti-virus, firewall and backups;

Date	Event	Description
18/11/2017	ICGP Winter Meeting	Attendance by Dr Green at information session on GDPR
08/01/2018	Practice Meeting	All staff meeting to review ICGP data protection guidelines
01/04/2018	Security Audit	Information Security audit by SecureSystems Ltd, audit report discussed by GP partners
26/05/2018	ICGP AGM	Attendance by practice manager at workshop on GDPR

Table 6 Sample entries for Accountability Log

Accountability Folder
You also need a folder, either electronic or manual, of all the practice documents related to GDPR. These could include:

- Regular Information Security Audits;
- Records of Processing Activities, as shown in Section 2;
- Confidentiality agreements with Staff;
- Records of staff training and awareness;
- Processor contracts with GP Practice Software Vendors, Healthlink and any other data processors;
- Where processing on basis of consent, records of this consent;
- Circular 027/18 from PCRS on the use and retention of PPSNs;

Accountability Log for General Data Protection Regulation (GDPR)

Practice Name	
Practice Address	
Practice Phone Number	
Practice Healthmail Address	
Data Controller	
Lead for Data Protection	
GP Practice Software System	

Date	Event	Description

Appendix G: Medical Student Confidentiality Agreement

Dr Joseph Bloggs
Anytown Medical Centre
Main Street, Anytown
Phone: 01 123456

Name of Medical Student (block capitals)	
Student ID Number	
Medical School	
Date attachment commenced	
Date attachment finished	
Name of responsible GP	

I confirm that, while attached to the Anytown Medical Practice, I agree to the following principles of confidentiality:

- Any personal data concerning patients which I have learned by virtue of my position as medical student attached to this practice will be kept confidential both during and after my attachment.
- I will only discuss cases seen during the course of my attachment with GPs from the practice or at recognised teaching sessions organised by the medical school. Patient information will be kept anonymous during these discussions. Likewise, if writing about patients for assignments, learning logs etc. I shall retain the patient's anonymity e.g. by not using any potentially identifying information such as name, address, date of birth or any other patient identifiers.
- I will not remove any documents or property from the practice without advanced authorisation from the responsible GP.
- I will not access medical records belonging to me, members of my family or those known to me without advanced authorisation from the responsible GP.

Medical Student

Name (block capitals)	
Signature	
Date	

Responsible GP

Name (block capitals)	
Signature	
Date	

Appendix H: Staff Confidentiality Agreement

Practice Name	
Practice Address	
Date	

Name of Staff Member	
Role	

I understand and accept that I have a duty of privacy and confidentiality to the practice and the patients both during and after my period of employment. I undertake:

- To treat all patient information, accessed as part of my role in the practice, as private and confidential.
- To only use my own username and password when accessing or editing patient records.
- Only to access medical records where I have a duty of care to the patient.
- Not to remove documents or digital records from the practice without the consent of the responsible GP.
- Not to access records belonging to me, members of my family or those known to me without advance authorisation from the responsible GP.
- Not to discuss confidential patient information with my family or in public.
- To maintain the privacy of patient records by ensuring that records are stored securely, and that documents, results and computer screens are not open to public view.

I understand that a breach of patient confidentiality is grounds for censure or dismissal.

Name of Staff Member	
Signature	
Date	

Appendix I: Template for Records of Processing Activity

Practice Name	
Practice Address	
Practice Phone Number	
Data Controller	
Lead for Data Protection	

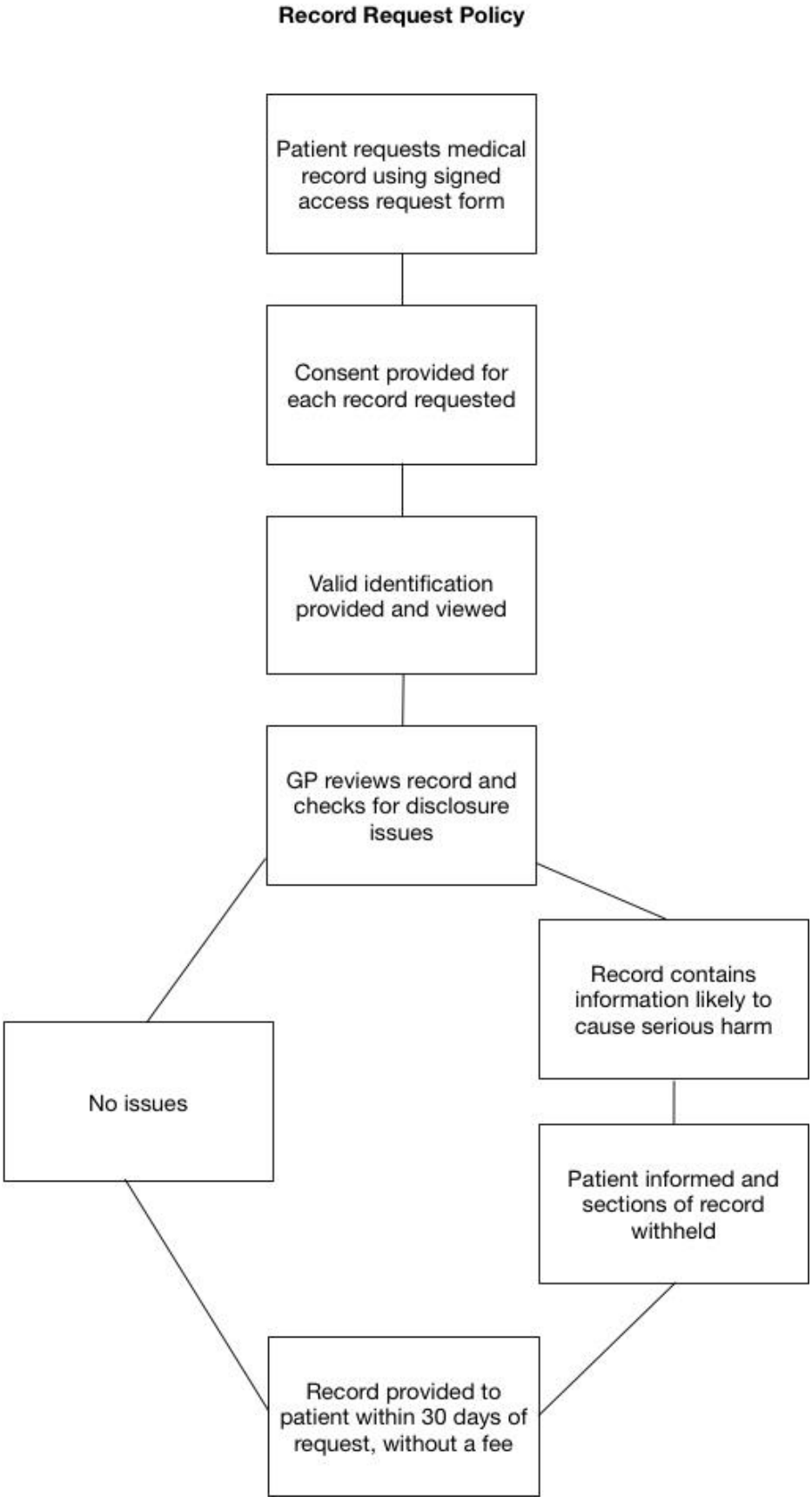
The following Table applies for both Public and Private Patients and shows the categories of personal data processed by this practice.

Category of Personal Data	**Purpose of Processing**	**Lawfulness of Processing**
Administrative: name, address, contact details (phone, mobile, email), dates of appointment	Necessary to support the administration of patient care in general practice	Article 6.1(d): processing is necessary in order to protect the vital interests of the data subject or of another natural person; Article 6.1(e): processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; Special Categories are processed under the derogations in Articles 9.2(h) and 9.2(i).
Medical Record: Individual Health identifier, GMS number, PPSN, date of birth, religion, sexual orientation, gender, family members, family history, contact details of next of kin, contact details of carers, vaccination details, medication details, allergy details, current and past medical and surgical history, genetic data, laboratory test results, imaging test results, near patient test results, ECGs, Ultrasound scan images, and other data required to provide medical care.	Necessary to provide patient care in general practice. The PPS number is needed for specific schemes such as sickness certification (Department of Social Protection), childhood immunisation programme, mother and child scheme, cervical screening, etc. (HSE).	
Account Details: record of billable services provided, patient name, address, contact details, billing and payment records for GMS and private patients	Required for providing a service and billing. Also required for submission of reimbursement claims to the HSE Primary Care Reimbursement Service.	Article 6.1(c): processing is necessary for compliance with a legal obligation to which the controller is subject (Revenue, Medical and Legal Obligations), and Article 6.1(b) in relation to getting paid for providing a service to private patients.

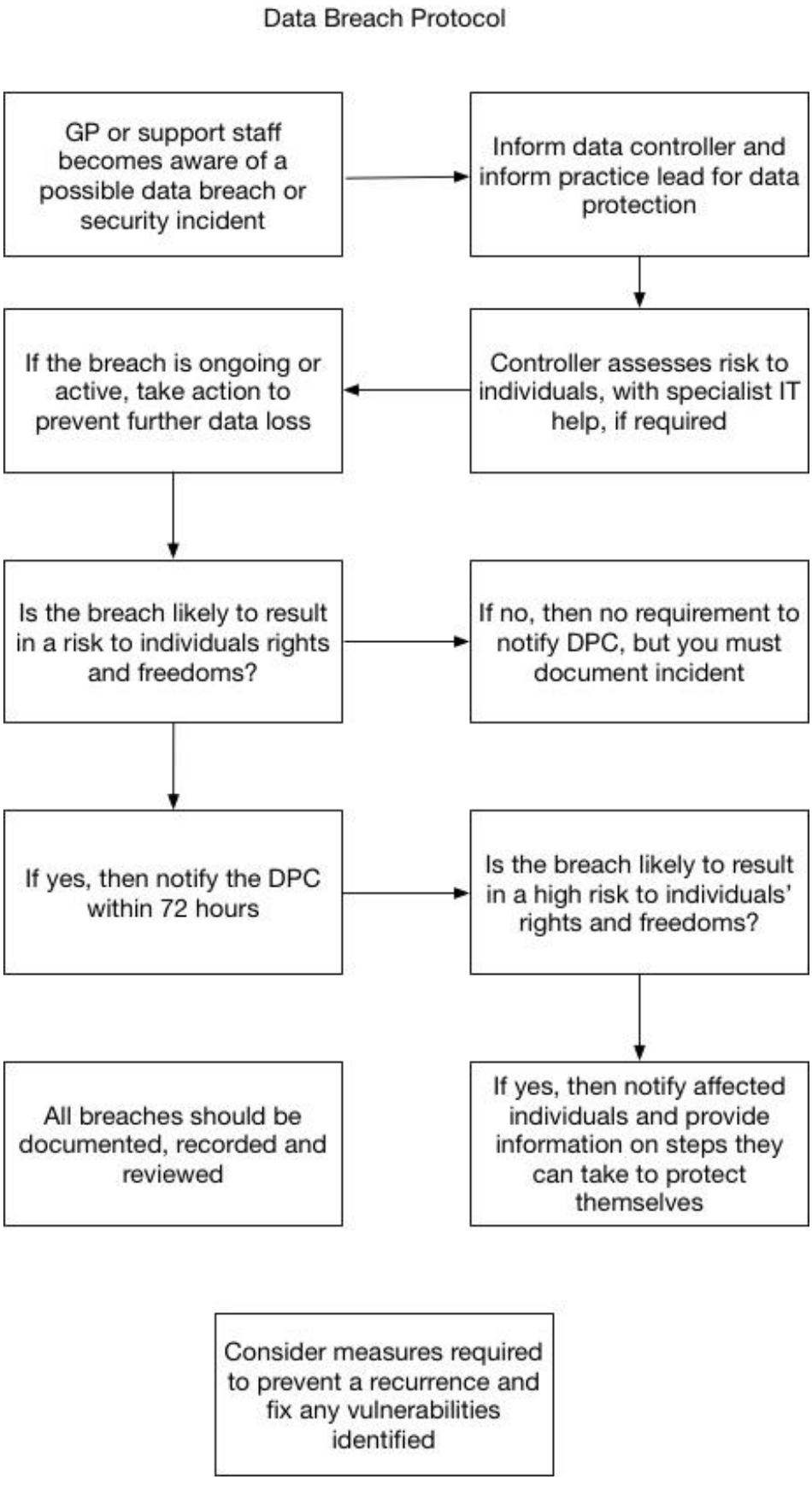
Recipients with whom we share personal data

Categories of Recipient	Description
Health and Social Care Providers	Other GPs, Health Service Executive, Voluntary Hospitals, Private Hospitals and Clinics, Private Consultants, Physiotherapists, Occupational Therapists, Speech and Language Therapists, Social Workers, Palliative Care Services, Out of Hours Services, Pharmacies, Nursing Homes, Counselling Services, Diagnostic Imaging Services, Hospital Laboratories, and other health care providers
Data Processors, with a contract	GP Practice Software Vendors, Online Data Backup Companies, Healthlink,
Legal Arrangements	Coroner, Revenue, Social Protection, Medical Council,
Public Health	Infectious disease notifications, influenza surveillance,
Third Parties, with explicit patient consent	Solicitors, Insurance Companies, Health Insurance Companies, Banks,

Appendix J: Protocol for Managing Patient Record Access Request



Appendix K: Protocol for Managing a Data Breach



Appendix L: Data Breach Reporting Template

This template may be used as a recording tool in conjunction with the Protocol for Managing a Data Breach

Breach	Response
Summary of the event and circumstances in which it occurred	*When, What, Who?*
Type and amount of personal data involved	*Nature of documents. What sensitive information did they contain?*
Have the Data Controller and Data Protection Lead been informed?	*Who and when?*
Is breach ongoing? If so, is immediate further action required?	*Was this an isolated incident?* *Has data been retrieved or destroyed?* *Do other parties need to be informed/involved?*
Is breach likely to result in a risk to individual rights or freedoms?	*Yes/No. Why?*
Is it necessary to inform the Data Protection Commissioner within 72 hours?	*Notify DPC if answer Yes to question above*
Has the affected Data Subject been notified?	*What advice has been given to them?*
What lessons have been learnt to prevent a recurrence? What specific actions have been taken?	

Reviewed by:

Date:

Appendix M: PCRS Circular 027/18 on Use and Retention of PPSN

Feidhmeannacht na Seirbhíse Sláinte, Seirbhís Aisíocaíochta Cúraim Phríomhúil
Bealach amach 5 an M50, An Bóthar Thuaidh, Fionnghlas
Baile Átha Cliath 11, D11 XKF3
Guthán: (01) 864 7100 Facs: (01) 834 3589

Health Service Executive, Primary Care Reimbursement Service
Exit 5, M50, North Road, Finglas, Dublin 11, D11 XKF3
Tel: (01) 864 7100 Fax: (01) 834 3589

Circular 027/18 5th September 2018

Use and Retention of

Personal Public Service Number (PPSN)

Dear Doctor,

The purpose of this Circular is to clarify the use of and the retention of a Personal Public Service Number (PPSN) for the effective administration and the transaction of the business of public health schemes.

The HSE, as a specified body in SOCIAL WELFARE CONSOLIDATION ACT 2005 Schedule 5, is authorised to use the PPSN. Accordingly, the use of a PPSN by persons authorised by such specified bodies (HSE) to act on their behalf (e.g. GPs operating under a contract for service) is therefore permissible.

Section 262(4) SOCIAL WELFARE CONSOLIDATION ACT 2005 outlines:

> A person shall give to a specified body his or her personal public service number and the personal public service numbers of his or her spouse and children, where relevant, as required by the body for the purposes of the person s transaction.

Article 6 of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) sets out the **Lawfulness of processing** of personal data, which includes inter alia:

> 1(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

For the avoidance of doubt, the use of and the retention of an eligible person s PPSN is a prerequisite in the provision of general practitioner medical and surgical service to that person, or to his/her spouse or partner and child dependants that are also eligible to such services.

Yours sincerely,

Anne Marie Hoey
Assistant National Director
Primary Care Reimbursement and Eligibility

Seirbhís Sláinte Níos Fearr á Forbairt | Building a Better Health Service