Irish College of GPs

Coláiste Dhochtúiri Teaghlaigh Éireann

Processing of patient personal data – a guide for GPs

November 2025

Processing of Patient Personal Data: A Guideline for General Practitioners

File name: GP_GDPR_Guideline_v3 pdf

Date: 2025
Version: 3
Governance: Irish College of GPs
Authors: Irish College of GPs Data Protection Working Group

Document History

Date	Version	Comments
03/04/2018	1.0	First public release version, following feedback from Irish College of GPs Working Group
20/07/2019	2.0	Revision of document following publication of more information on application of GDPR in Ireland
12/11/2025	3.0	Revision of document to reflect implementation of GDPR and any relevant associated updates

Table 1 Document History

Table of Contents

Part1,Core Principles of Data Protection **4**
1. Introduction 4
2. Records of Processing Activities 7
3. Compliance with Data Protection Principles 13
4. Compliance with Individual Rights 17
5. Personal Data Breach Handling 21
6. Miscellaneous Provisions 22
7. Health Information Bill 2025 24
8. Bibliography 25
Part 2, Frequently Asked Questions **26**
Part 3, Appendices **35**
Appendix A: Data Protection Check List 35
Appendix B: Sample Request for Transfer of GP Records 36
Appendix C: Request form for Access to Medical Records 37
Appendix D: Waiting Room Notice 38
Appendix E: Practice Privacy Statement 39
Appendix F: Data Protection Accountability Log 46
Appendix G: Medical Student Confidentiality Agreement 48
Appendix H: Staff Confidentiality Agreement 49
Appendix I: Template for Records of Processing Activity 50
Appendix J: Protocol for Managing Patient Record Access Request 52
Appendix K: Protocol for Managing a Data Breach 53
Appendix L: Data Breach Reporting Template 54

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.

Update to GDPR Guidelines

The College is publishing an update to its document "Processing of Patient Personal Data: A Guideline for General Practitioners", which was originally produced in response to the General Data Protection Regulation (GDPR) and the subsequent Irish Data Protection Act. The College issued its previous guidance in 2019, and the update reflects maturity in the application of data protection and related legislation. There is also an awareness that the forthcoming Health Information Bill and legislation related to Artificial Intelligence may necessitate further updates; however, it was felt reasonable to issue a reflection of the status quo in 2025.
The entire guideline has been reviewed; however, most of the document will be familiar to those in practice who are responsible for data protection issues. It would be recommended that practices review the full document, and particular attention would be drawn to

- Clarity on the Lawful Basis for Processing
- Updates on the Rights of Individuals, including subject access requests.
- Guidance on recording of Processing Activities

The practical use of Appendices has been updated and modified, and it is hoped that this document will continue to be useful for practices.

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 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 GPs 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. The 2025 version of this guidance reflects updates in the application of data protection and related legislation.

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 GPs 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	GPIT Advisor and General Practitioner
Ms Niamh Killeen	Head of IT, Irish College of GPs
Mr Shantanu Kulkarni	Data Protection Advisor, Trilateral Research Ltd. Data Protection Officer for the Irish College of GPs
Ms Paula Swales	Service Manager, Trilateral Research Ltd.

Table 2 Members of Irish College of GPs 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 message

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 European Data Protection Board.

The interpretation of data protection regulations evolves continuously, and this Guideline will be reviewed periodically. Therefore, the Guideline continues to change over time as the implementation of data protection regulations becomes 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 Irish College of GPs website here.

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. The conditions for consent are discussed in section 3(a) of this guidance.

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.

‘special category data’ of GDPR states that “Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.”

However,) states that Article 9.1 does not apply if processing is necessary for purposes of preventive or occupational medicine, assessment of working capacity, medical diagnosis or the provision of health or social care; or where processing is necessary for reasons of public interest in the area of public health.

2. Records of Processing Activities

As per , 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 to both Public and Private Patients and shows the categories of personal data processed by GPs, with links to the relevant articles of the General Data Protection Regulation (GDPR). The lawful basis for processing personal data is to be determined by considering the nature of the data and the purpose for which it is being processed. Each processing activity should have an independent lawful basis; for example, data used for billing or other administrative uses, such as allocation of appointments, etc, may have a different lawful basis. Whereas data used for determining medical situations may be on the basis of contract if the individual is conscious. However, if the individual is unable or unconscious, the lawful basis may be covered by vital interests. This will have to be assessed by each GP practice individually.

See "Notes on the Legal Basis for Processing of Data" below

Category of Personal Data	Purpose of Processing	Lawful basis for Processing
Administrative: name, address, Eircode, contact details (phone, mobile, email), dates of appointment	Necessary to support the administration of patient care in general practice	processing is necessary for the performance of a contract to which the data subject is a party processing is necessary in order to protect the vital interests of the data subject or of another natural person 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	Required for providing a service and billing. Also required for submission of reimbursement claims to the HSE Primary Care	processing is necessary for compliance with a legal obligation to which the controller is subject (Revenue, Medical and Legal Obligations), and in

patients	Reimbursement Service.	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 Registered Medical Practitioners'. The legal basis for the processing of data by GPs is provided by the following articles in GDPR:
, and refer to the categories of special data

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.

Another lawful basis that may be applicable to general practice is to process personal data for the protection of vital interests of the patient and for the provision of health

care to the public. However, it is essential to note the circumstances under which the vital health lawful basis may be used, i.e. only when the data subject himself or herself is incapacitated to provide his or her consent and in the absence of another lawful basis to help urgently save the life of the data subject.

Explicit and informed consent may be 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, 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, Laboratory Services, 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, Insurance Companies, Garda, 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 upon 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.

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 its respective responsibilities.

e) Transfers to a Third Country

The GDPR restricts transfers to third countries that are outside the European Economic Area (EEA). It states that transfers to such third countries may only be undertaken if certain transfer mechanisms are imposed, these safeguards have been provided in Chapter V of the GDPR.

Applicable transfer mechanisms:

a) Article 45 of the GDPR: Adequacy Decision: An adequacy decision is granted by the European Commission to countries that ensure equivalent levels of protections to personal data processing when compared to the EEA countries. These decisions are reviewed by the European Commission from time to time, and thus it is advisable to consult the European Commission Website to ascertain the latest list of countries with adequacy decisions.
b) Article 46 of the GDPR: Standard Contractual Clauses: These are pre-approved contractual clauses by the European Commission that provide for the necessary set of assurances and guarantees that an organisation based in a third country must provide. These clauses have been provided on the European Commission's Website and may be consulted from time to time as the need arsis for transfer of personal data.
c) Article 46 (2)(a) of the GDPR also provides for a legally binding and enforceable agreement between public authorities or bodies as a recognised means of transferring data from the EEA to a third country.
d) Other alternatives available are Binding Corporate Rules and transfer through an approved Code of Conduct. Both these mechanisms need prior Data Protection Commission approval.
e) Only in the absence of the above (i.e. when none of the transfer mechanisms are applicable) can reliance be placed on the derogations stated in Article 49 of the GDPR.

In any circumstance, the Court of Justice of the European Union in the Schrems II decision has made it mandatory for all organisations contemplating a data transfer to a third country without an adequacy decision to conduct a Transfer Impact Assessment.

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 (). 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 is processed. There are no national guidelines for the retention of healthcare records other than those produced by the National Hospitals Office for public hospitals. These minimum retention periods, however, are based on common-sense principles that are equally applicable in general practice. The value of retaining records for longer periods may also be that they can assist in responding to a complaint or claim. (Medical Council, Guide to Professional Conduct & Ethics for Registered Medical Practitioners 9th Edition 2024) The recommended minimum retention periods are guidelines only, and it may sometimes be necessary to take an individual approach to some records and retain them for longer periods.

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 the 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 at 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 consider commissioning 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 and email;

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. More information can be found on the college website.

It may be beneficial for practices to consider undertaking vulnerability testing (such as a penetration test of the IT system) of their electronic system.

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 require 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 that this notice is also displayed in general waiting areas in the practice. GPs should refer to , and 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 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 should be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay.

GPs must make 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 health professional. 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 consider commissioning 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 for GPs to keep certain records. These include:

- Security Audit Reports;
- Records of Processing Activities, as shown in Section 2;
- Confidentiality agreements with Staff;
- Records of staff training and awareness;
- Data processing/sharing agreements with GP Practice Software Vendors, Healthlink and any other data processors;
- Where processing on basis of consent, records of provision of consent and withdrawal of consent.
- Logs: Data Breach logs and data subject access request logs.

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 and on any practice website. A member of the practice should be available to patients to discuss any data protection questions and to facilitate access requests for medical records. Alternatively, the GP Practice may consider appointing a DPO as provided by .

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 , the patient, whether GMS or private, has a right to access a copy of their medical record. Such a right may be exercised by the above-mentioned individuals by submitting a request to the GP practice. Such a request may be submitted by an individual in either written format, i.e. by post, email or by completing a form that may be provided by the GP practice. The request may also be made by the individual verbally over a phone call or in person. In such instances where the request is verbal, the GP practice may acknowledge the verbal communication and seek a written request explaining the data sought would aid in resolving the individual's request. This written request can be a mere confirmation of the conversation held verbally in a written form or an email. Once a legitimate request is received, the GP practice shall provide a copy of the individual's medical record. To assess the legitimacy of a request the GP practice may request additional documentation such as a signed letter of authority or a power of attorney or proof of legal guardianship or parenthood. 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 is received, be that written or verbal. No fee is chargeable for providing a copy of the medical record. However, for repeated requests or for requests that are excessive, the GP practice may charge a reasonable fee based on administrative costs.

It is important for the practice to verify the identity of the person making an access request or providing an access authorisation. This can be done by seeking additional documentation such as a passport or a driver's license which can be compared to a copy on record to confirm the individual's identity. It must be noted that an ID verification is required when the individual is seeking their own personal data, whereas an access authorisation is needed when another individual is seeking someone else's personal data, for example: a spouse is seeking access to personal data or when a lawyer/ solicitor is seeking or when the GARDA is seeking access to personal data of the patient, etc.

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 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.

b)Exemptions to the right to access of personal data

The right to access can be limited only in specific circumstances as per Article 12(5) of the GDPR. This Article states that, a controller (GP practice) may refuse to act on the request should it be manifestly unfounded or excessive. It must also be noted that should such a refusal to provide access to personal data be challenged by the individual the burden of proving that the request was manifestly unfounded or excessive is on the controller (i.e. the GP practice). Other applicable exceptions are as follows:

1. Opinion expressed in confidence i.e. Section 60 (3)(b)of the Data Protection Act 2018

2. Data, if provided, will adversely affect the rights and freedoms of third parties i.e. Article 15(4) of the GDPR

3. In contemplation of or for the establishment, exercise or defense of, a legal claim, prospective legal claim, legal proceedings or prospective legal proceeding whether before a court, statutory tribunal, statutory body or an administrative or out of court proceeding Section 60 (3)(a)(iv) of the Data Protection Act 2018

4. For the enforcement of civil law claims, including matters relating to any liability of a controller or processor in respect of damages, compensation or other liabilities or debts related to the claim. Section 60(3)(a)(v) of the Data Protection Act 2018

5. For the purposes of estimating the amount of the liability of a controller on foot of a claim for the payment of a sum of money, whether in respect of damages or compensation, in any case in which the application of those rights or obligations would be likely to prejudice the commercial interests of the controller in relation to the claim. Section 60(3)(a)(vi) of the Data Protection Act 2018

6. If in the opinion of the health professional or facility the release of personal data or some/any of the information could potentially be damaging to your physical or mental health. Data Protection Act 2018 (Access Modification) (Health) Regulations 2022, S.I. No. 121 of 2022

While applying the above exceptions to the access requests, it must be noted that they apply only to the extent that is necessary and proportionate, or for as long as necessary, only to protect the health of the data subject.

When resolving a subject access request, the individual should be provided with the following information in addition to their data as per :

1. the purposes of the processing;

2. the categories of personal data concerned;

3. the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

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

5. the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

6. the right to lodge a complaint with a supervisory authority;

7. where the personal data are not collected from the data subject, any available information as to their source;

8. the existence of automated decision-making, including profiling, referred to in (1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

c) 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 (). 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.

d) Right to Erasure

deals with the right to erasure. Because the GP has a requirement (Section 38 of Guide to Professional Conduct and Ethics for Registered Medical Practitioners, 9th Edition 2024) under Medical Council rules to keep medical records and also has a right to defend medico-legal claims, under 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. However, we recommend consulting with a data protection advisor or your DPO before proceeding.

e) 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 does 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. Such requests can also be submitted in either written format or can be communicated verbally. In instances where the request is verbally communicated the GP practice may seek a written representation from individual requesting the restriction of processing. While this is not a GDPR requirement GP practices may deem it necessary as a procedural and administrative step.

f) Right to Data Portability

The right to data portability, under , 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.

g) 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.

h) Automated Individual Decision-making, Including Profiling

GPs should not base decisions solely on automated processing, and when this may be the case inform the individual along with an opportunity to seek human intervention.

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);
- Phishing or social engineering
- 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.).

The Office of the Data Protection Commissioner has produced guidelines on data breaches which is available at https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Data%20Breach%20Notification_Practical%20Guidance_Oct19.pdf

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 at https://forms.dataprotection.ie/breach-notification, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. If 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 Example

The Appendices to this Irish College of GPs 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. DPIAs 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.

Carrying out a DPIA is not always mandatory under the GDPR, however the GDPR does define certain cases in which a DPIA would be mandatory under Article 35 of the GDPR. Should a GP practices processing activities meet the threshold of resulting in a high risk to the rights and freedoms of individuals, it would then be mandatory to complete a DPIA. More information on when a DPIA is mandatory can be found in the Data Protection Commission's guidance on DPIAs. 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)

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. Any practice may appoint a DPO on a voluntary basis. The following link provides an interactive tool to assess if a DPO is required https://www.edpb.europa.eu/sme-data-protection-guide/data-protection-officer_en

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 by each 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. Health Information Bill 2025

The Health Information Bill 2025 would legislate for a duty for health services providers to share, in certain circumstances, a patient's personal health data with other health services providers also providing care and treatment to the patient; it also provides for the creation and assignment of a Digital Health Record in respect of every patient.

Once enacted, GPs would have a duty to share information for the purposes of providing integrated care and treatment and continuity of care and treatment. The Bill stipulates that GPs would be empowered to create and manage health records for all patients. The Bill also provides a basis for the sharing of relevant information amongst healthcare providers for patient care and treatment, and is in alignment with the European Health Data Space Regulations (EHDS). The Bill, in its current form, stipulates that a Digital Health Record would contain the following categories of health information:

- A patient summary
- Prescriptions
- Dispensation (prescriptions filled at the pharmacy)
- Medical imaging studies (scans and X-rays)
- Medical test results, and
- Discharge reports

The Bill, once enacted as a law, would need to be interpreted in harmony with the General Data Protection Regulations. Therefore, all GPs would have specific obligations under the Bill; however, obligations mentioned under the GDPR would also have to be satisfied. The GDPR applies to the processing of all personal data, whereas the Bill only focuses on facilitating the sharing of health information between relevant parties.

It is likely that the Bill is currently in the Dáil Éireann stage and would need to complete the Seanad Éireann stage before gaining the President of Ireland's signature, making it a law. Implications for GPs' obligations for data processing will be further reviewed when the law is enacted

8. 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/

Medical Records in Ireland, Medical Protection Society https://www.medicalprotection.org/ireland/booklets/medical-records-in-ireland-an-mps-guide

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

HSE National Records Retention Policy https://assets.hse.ie/media/documents/ncr/20240806_HSE_Record_Retention_Policy_V3.pdf

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

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. What should happen to patient records when a GP retires or dies?

Answer (A). The Health Information Act 2024 obliges GPs as health care providers to take all reasonable steps to notify each patient of when they will cease to provide services, and of the arrangements that will be in place to transfer their records to another health care provider

When a GP retires as a member of a group practice, the care of those patients and their medical records will usually remain with that practice unless a patient requests a change to another practice. If a GMS panel of patients is awarded to a GP outside of that practice, then the new GP is entitled to the records of all patients on the GMS list and may request record transfer in the usual way.

If a single-handed practitioner retires and a successor is appointed, the same guidance as for group practice applies. If a single-handed practitioner retires and no successor is appointed, the existing (retiring) doctor should maintain the patient's 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, and appropriate arrangements should be put in place for GPs or patients to request medical records, which should be dealt with in a timely way.

In the unfortunate eventuality of the death of a single-handed practitioner in post, then it would be the responsibility of their estate to facilitate the transfer of medical records on receipt of appropriate requests.

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 a 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 medical information to a spouse, former spouse, or child capable of making decisions themselves will, in most situations, constitute a breach of the Data Protection Acts if done without the consent of the other spouse, former spouse, or child. Transfer of the husband's data should be on the basis of his written authorisation.

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 it 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 authorise the release of the data or to request access to the 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 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 wish. The GP practice may also offer the patient an opportunity to review the information before providing it to the insurance company. Alternatively, if the GP practice deems the request by the insurance company excessive, they may request the company to reconsider the scope or consult the patient before releasing the information.

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 whom 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. If in doubt, it is sensible to ask for a written request from the Department of Social Work, explaining the basis for their request.

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. Where possible, transmission of personal health information by email should be avoided. Email is often a very useful and convenient method of communication; however, in a general practice setting, there are specific issues to consider, including confidentiality and security, professional boundaries, and duty of care. If you are contemplating a standardised process of returning results, you should consider other methods, such as using secure patient portals. However, if you must use email, you should consider password-protecting the report/ attachment and sharing the password of such an attachment through a separate message.

If there is a specific request by email from a patient to send their results back in that format, then it may be reasonable to acquiesce to that request; however, you should restrict the content of any message and consider the potential for a data breach. You should also take good care while typing the email address of the recipient to ensure that the email is issued to the person for whom it was intended. An explicit and informed request or consent from the patient should be recorded.
More detail is available in the GPIT publication "Use of Email in General Practice"

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, a 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's information is being sent is correct. Where an auto-dial function is being used, it is important to verify the recipient's 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 fax 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 the exchange of patient-identifiable clinical information between GPs and clinicians in primary and secondary care. More information about connected agencies can be found at 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 Irish College of GPs 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 preparing repeat prescriptions for patients. These are then reviewed and forwarded 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. 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 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 contacts 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 associated documents.
- Sending and receiving information via Healthmail, a 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 (see Appendix H) that explicitly makes clear their duties in relation to personal health information and the consequences of breaching that duty.

The 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. (see Appendix G)

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's 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 this Irish College of GPs Guideline on Data Protection is the processing of patient data. This Irish College of GPs 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 ''

Picking Up Correspondence for Patients

Q16. We have a lot of people who would have letters, forms or certificates 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 the patient's consent to do so is in place. Thus, for example, giving any patient identifiable letter, form or result out to the wrong patient would be a data breach

When it comes to third parties picking up letters, forms or certificates 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 correspondence being collected by third parties go in an envelope addressed to the patient and marked 'private and confidential'?

Destruction of medical records

Q17. 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. However, there are several exceptions to this, 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

Q18. 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.

Garda Request for Medical Records

Q19. How should I respond to a request from the Gardaí for medical records on one of my patients?

Gardaí are not automatically entitled to patient identifiable information without consent; therefore, your initial response would be to ask them to make a written application under GDPR, ideally with the patient's consent.

However, section 41 (b) of the Data Protection Act, 2018, does allow for the processing of data other than for a purpose for which it was collected for the purposes of "preventing, detecting, investigating or prosecuting criminal offences". The legislation is very clear that the processing of the data for another purpose without consent must be necessary and proportionate. Therefore, this does not *oblige* you to disclose information, but it does allow for it at your discretion. It would be reasonable to discuss this with your medical indemnifier. If disclosing information, you should restrict that to information which is essential to the Garda investigation.

It is open to the Gardaí to seek a Court Order or Warrant to obtain information or records. If the Gardaí obtain a Court Order for the release of the details, you would be required to release same. You should also always bear in mind that the Criminal Justice (Withholding of Information on Offences Against Children and Vulnerable Persons) Act 2012 makes it an offence to withhold information from Gardaí in relation to specified offences against a child or vulnerable person.

If the Gardaí request a medical report, rather than medical records, this does not fall under the Data Protection Act or GDPR, however you should have the consent of the patient to prepare a report.

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? Or have you appointed a Data Protection Officer?		
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 or on your websites?		

Apart from the above, GP practices may also consult the Data Protection Commission's Self-Assessment Checklist when necessary.

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 (IMC 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	
Scope of the request	
Signature	
Date	

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

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.

Appendix D: Waiting Room Notice

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 visit our website to view our Privacy Statement

Thank you.

Appendix E: Practice Privacy Statement

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 Medical Practitioners.' The purpose of this privacy notice is to explain how we collect and use personal data for the provision of our services and the day-to-day running of this GP practice.

The personal data we process

In order to provide for your care here we need to collect and keep information about you and your health on our records. This information/ data may include:

- Personal details about you, such as name, date of birth, PPS Number, address, next of kin, contact details (mobile phone number) etc.
- Information relating to your treatment and care; notes and reports about your health which assist our staff in providing care and treatment to you; results of investigations, such as x-rays and blood tests
- Relevant information from other health and social care professionals, other healthcare agencies and your carers and relatives
- Financial and health insurance information

We may also process certain special categories of information, which may include racial or ethnic origin, religious or philosophical beliefs, the processing of genetic data, biometric data for the purpose of uniquely identifying a person, data concerning health or data concerning a person's sex life or sexual orientation.

Legal Basis for Processing Your Data

This GP Practice's lawful basis for processing personal data of service users are as follows:

- Processing is necessary for the performance of a contract or to take steps to execute a contract with you as the data subject as per Article 6(1)(b) of the GDPR. This would apply to the provision of basic administrative services and the performance of office tasks.
- The processing is necessary in order to protect the vital interests of the person (referred to as the data subject in data protection language) as per Article 6(1)(d) of the GDPR. This would apply in emergency situations when the patient is unconscious, sharing information with other emergency services for rescue or relocation in storms, etc.
- The processing is necessary for a task carried out in the public interest or in the exercise of official authority vested in the controller as per Article 6(1)(e) of the GDPR.

Special categories of data are defined by the GDPR and include things like racial or ethnic origin, religious or philosophical beliefs, genetic data, biometric data, health data, sex life details and sexual orientation. The processing of special categories of personal data is permitted in circumstances as set out in Article 9 of the GDPR.

We will only process special categories of personal data where it is necessary:

- for the purposes of preventative or occupational medicine,
- for medical diagnosis,
- for the provision of healthcare, treatment or social care,
- for the management of health or social care systems and services, or contract with a health professional pursuant to a contract with the health professional.

Processing is lawful where it is undertaken by or under the responsibility of

- a health practitioner, or
- a person who, in the circumstances, owes a duty of confidentiality to the data subject
- that is equivalent to that which would exist if that person were a health practitioner, for example, the GP practice secretary, Receptionist, GP practice staff, etc.

If the purpose of the processing is for a reason other than the reasons outlined above, we will seek explicit consent to process your sensitive personal data (referred to as special categories of data under the GDPR)

How we obtain information

We may obtain your information from a variety of sources, including information you give to us. During your treatment and care within the GP practice, health-specific data will be collected by the doctors, nurses and other healthcare professionals taking care of you and will be held in your patient/client file (this can be paper and/or electronic). We may also receive your personal information from third parties, for example, your previous GP, dentist, social worker, or pharmacist. There may also be times when information is collected from your relatives or next of kin, e.g. if you are in a Medical Emergency or are very unwell and unable to communicate.

Your rights

You have certain legal rights concerning your information and the manner in which we process it. This includes:

- a right to get access to your personal information;
- a right to request us to correct inaccurate information, or update incomplete information;
- a right to request that we restrict the processing of your information in certain circumstances;
- a right to request the deletion of personal information, excluding medical records;
- a right to receive the personal information you provided to us in a portable format;
- a right to object to us processing your personal information in certain circumstances; and
- a right to lodge a complaint with the Data Protection Commission (DPC). Contact details for the DPC are available at

Some of these rights only apply in certain circumstances and so are not guaranteed or absolute rights. Please contact our Reception if you have any queries or concerns about your rights.

Access to your records

You can access your records by making a subject access request (SAR) and forms are available for this purpose at the reception**.** You can also call the reception with a

request; however, you will still need to submit a written request clarifying the scope of your request. It is important that you provide satisfactory evidence of identification and a sufficient description of the information that you are looking for.

How do we use your information?

We use your information to manage and deliver your care and treatment to ensure that the treatment is safe and effective, that the right decisions are made about your care, and so that we can coordinate with other organisations that may be involved in your care.

Your information may be used to:

- 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.
- Accurately verify your identity and associate you with your healthcare records.
- Review the care and treatment provided to ensure it is of the highest standard possible and to evaluate and improve the safety of our services. This can be carried out by multiple quality improvement methods e.g. audits, clinical audit, patient experience and satisfaction surveys.
- Investigate complaints, legal claims and adverse incidents.
- Plan the future demand in the health services e.g. analysing peak attendance times, staffing levels and average length of stay; establishing the projected demand by disease/condition.
- Protect the wider public interests e.g. Influenza, winter vomiting bug, COVID-19.
- Provide training and development to health professionals who may join our GP practice.
- Invoicing, billing and account management.
- Remind you of appointments by text.
- To identify patients/service users who might be suitable for clinical trials/research.
- Handling, printing, photocopying and postage of medico-legal and life

assurance reports, and of associated documents.

- Sending and receiving information via Healthmail, a secure clinical email.
- And other activities related to the support of medical care appropriate for practice support staff.

Transferring information overseas

We may transfer your information to organisations in other countries, which is necessary to provide you with health and social care services, on the basis that anyone to whom we pass it protects it in the same way we would and in accordance with applicable data protection laws.

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.

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 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 certificates 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.

How do we keep your records secure and confidential?

We are committed to ensuring that your information is secure with us and with the third parties who act on our behalf. We have a number of security precautions in place to prevent
the loss, misuse or alteration of your information. All staff working for the GP practice have a duty to keep information about you confidential. The GP practice has strict information security policies and procedures in place to ensure that information about you is safe, whether it is held in paper or electronic format.

Retention period

The GP practice will only retain your personal data for as long as is necessary to fulfil the purpose for which the data was collected. This period will also include and in certain instances be informed by legislations that create a legal obligation for the GP practice to retain your personal data for regulatory purposes. In certain circumstances, the GP practice may anonymise your personal data so that it can no longer be associated with you.

Contact details

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

Appendix F: Data Protection Accountability Log

Overview

One of the 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 may audit general practices to ensure they are accountable under GDPR.

Accountability Log

To demonstrate that you are accountable, you should 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, Irish College of GPs meetings, and online courses
- Internal training sessions for clinicians and support staff on GDPR;
- Security audits of your practice hardware, software, networks, anti-virus, firewall and backups;

Date	Event	Description
18/11/2024	Irish College of GPs Winter Meeting	Attendance by Dr Green at the information session on GDPR
08/01/2025	Practice Meeting	All staff meeting to review the Irish College of GPs data protection guidelines
01/04/2025	Security Audit	Information Security audit by SecureSystems Ltd, audit report discussed by GP partners
26/05/2025	Irish College of GPs 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;

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 a 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

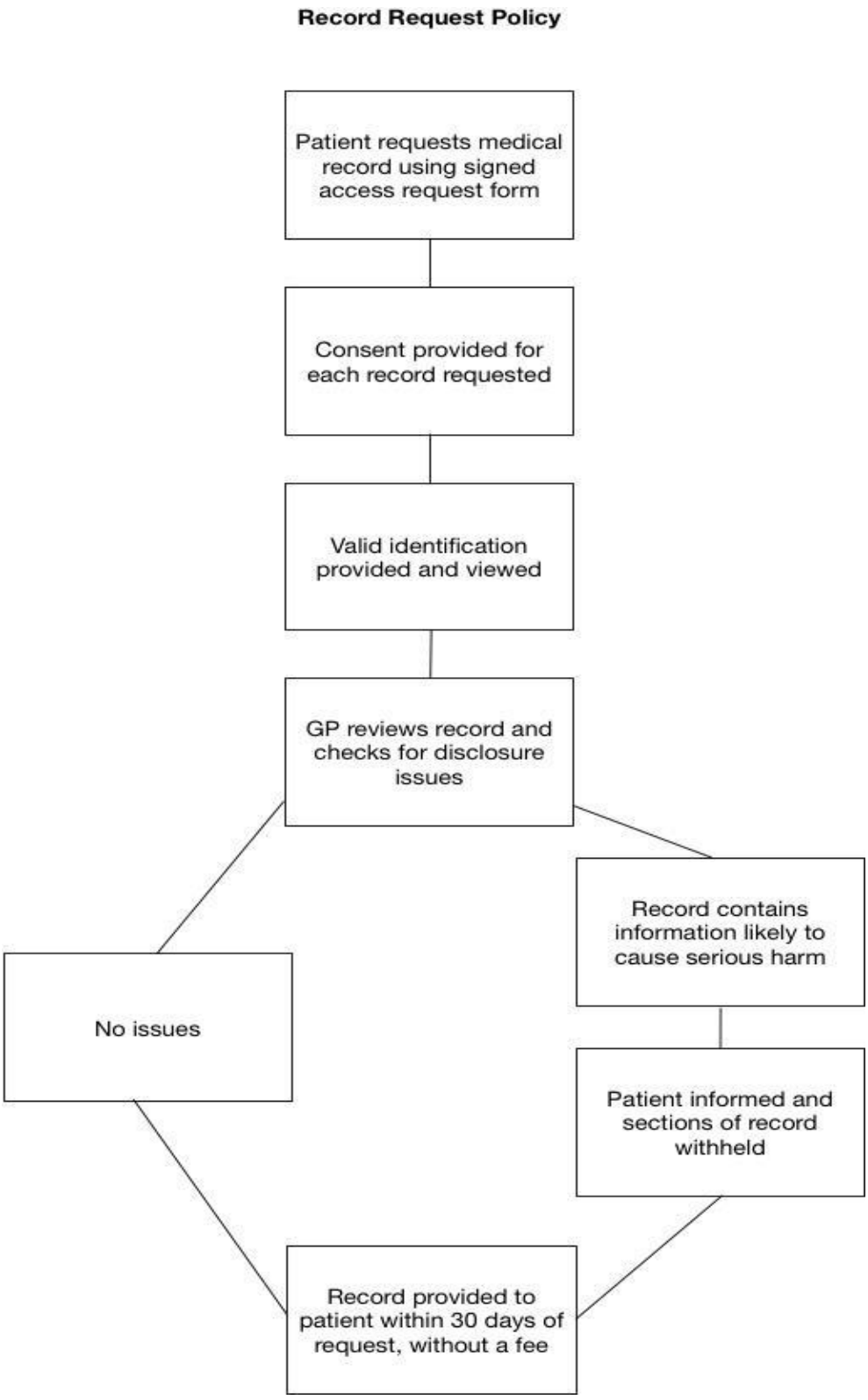
Practice Name	
Practice Address	
Practice Phone Number	
Data Controller	
Lead for Data Protection	

Article 30 of the General Data Protection Regulation (GDPR) requires Data Controllers to maintain a Record of Processing Activities (RoPA) under their responsibility. The GDPR also requires Data Processors to maintain a record of all categories of processing activities carried out on behalf of each Data Controller they work with. Practices may consider the assistance of a Data Protection Officer (DPO) service in completing this task. The RoPA is a living document and therefore would have to be updated on a time-to-time basis. More information on how to update a RoPA may be found here.

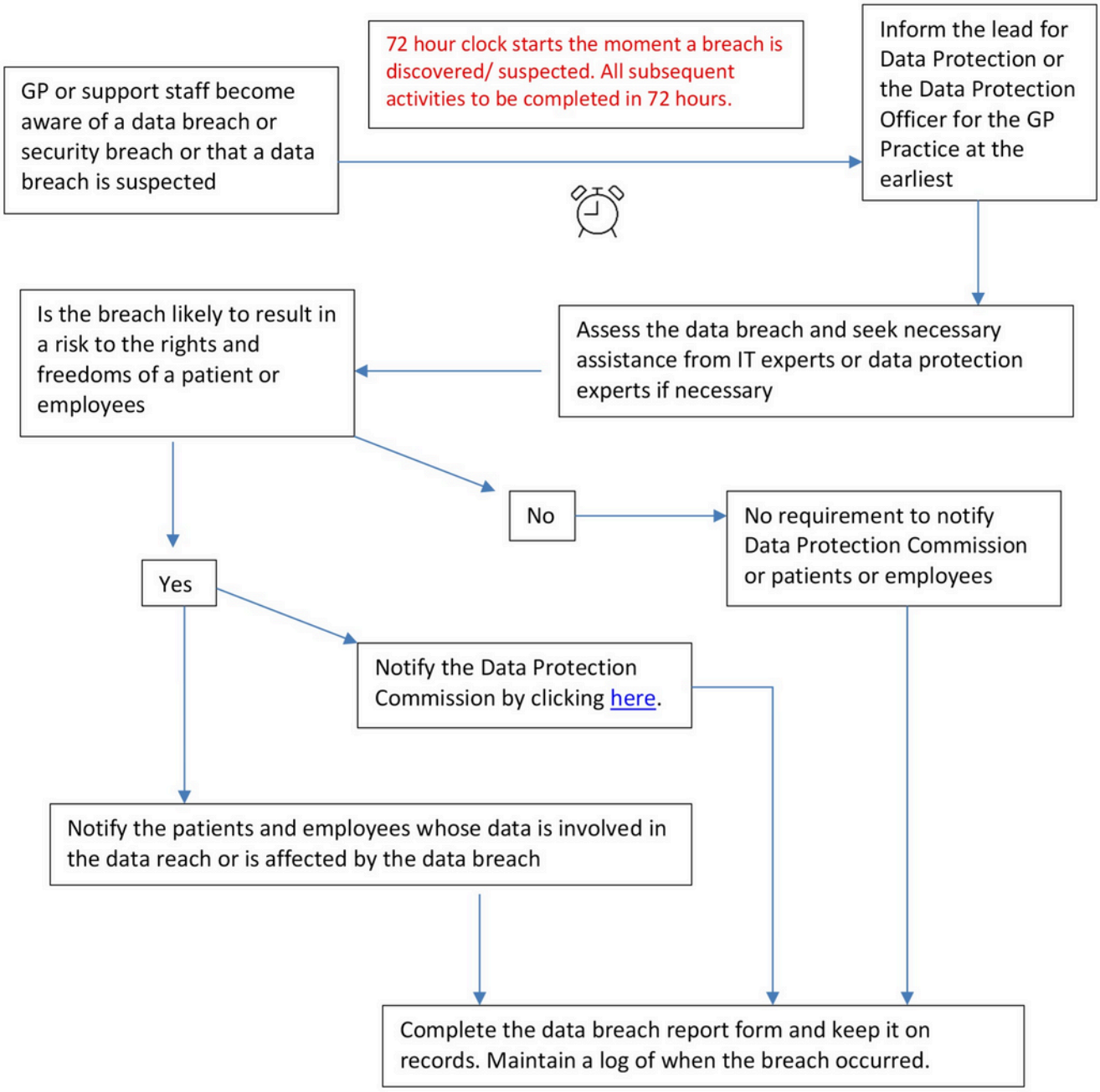
The following Table applies to both Public and Private Patients and shows the categories of personal data processed by this practice. It is, however, not exhaustive, and practices should note that all personal data being processed, including staff data, should be reflected in their RoPA

Sr. No.	Business function	Purpose of Processing	Role of GP Practice i.e. controller/ Joint Controller/ Processor	Categories of Data Subject	Personal Data	Recipient	Third County/ International Organisation Transfer	Safeguards	Retention Period	Technical & Organisational Measures	Lawful Basis
1	Medical Care	Necessary to provide patient care in general practice.	Controller	Patients	Individual Health identifier, GMS number, PPSN, date of birth, religion, sexual orientation, gender, family members, family history, contact details of next of kin/carers, vaccination details, medication details, allergy details, current and past medical and surgical history, test results (e.g.laboratory tests,imaging ,ECGs) and other data required to provide medical care.	HSE services, Hospitals, Private Consultants and other Health Care Providers. GP software vendors. Dept of Social Protection. *Other third parties with explicit consent*	Not Applicable	Not Applicable	Duration of the data subject being a patient + 7 years		Article 6.1(d): Article 6.1(e): Special Categories processed under the derogations in Articles 9.2(h) and 9.2(i).
2	Admin	Necessary to support the administration of patient care in general practice	Controller	Patients and next of kin	name, address, Eircode, contact details (phone, mobile, email), dates of appointment	HSE, hospitals,	Not Applicable	Not Applicable	Duration of the data subject being a patient + 7 years	Password protected and encrypted devices	Article 6.1(b)
3	Finance	Required for providing a service and billing; and for submission of claims to the HSE Primary Care Reimbursement Service.	Controller	Patients and next of kin	Records of billable services provided, patient name, address, contact details, billing and payment records for GMS and private patients	Payment gateways, HSE (PCRS)	Not Applicable	Not Applicable	Duration of the data subject being a patient + 7 years	Password protected and encrypted devices	Article 6.1(b) and 6.1(c)

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

Name of the person notifying the breach	
Contact details of the person notifying the breach	
Date on which the breach was discovered	
Date on which the breach was notified	
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?*
Amount of data subjects likely to be affected by the data breach	
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?*
Assessment of data breach by Data Controller or Data Protection Lead or Data Protection Officer	
Date of Assessment	
Type of data breach	*Loss of confidentiality (data disclosure/unauthorised access)* ☐ *Loss of integrity (data alteration)* ☐ *Loss of availability (data loss or inaccessibility)* ☐
Actions taken before reporting	
Follow-up actions required/ recommended	
Is breach likely to result in a risk to individual rights or freedoms?	*Yes/No. Why?*
Notification requirement *(within 72 hours of discovery)*	*Reportable to DPC: Yes* ☐ *No* ☐ *Notification to the Data Subjects: Yes* ☐ *No* ☐
If notified to data subject what was the notification comprising of?	
What lessons have been learnt to prevent a recurrence? What specific actions have been taken?	