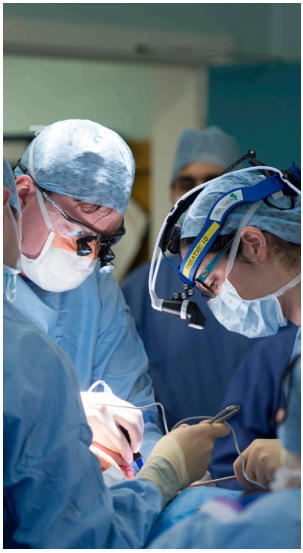
RCSI SURGICAL AFFAIRS


GENERAL DATA PROTECTION REGULATIONS (GDPR)

A GUIDE FOR SURGEONS

RCSI
2018

Leading the world
to better health

CONTENTS

1. INTRODUCTION

Purpose of these Guidelines

The Charter of Fundamental Rights of the European Union guarantees that every individual the right to respect for his or her private and family life, home and communications, and the protection of their personal data. These rights have been codified into directives and regulations and ultimately into national law in Ireland. The most recent regulations (General Data Protection Regulation or GDPR) came into force on the 25th May 2018, replacing the existing data protection framework under the EU Data Protection Directive.

The GDPR emphasises transparency, security and accountability by data controllers and processors, while at the same time standardising and strengthening the right of European citizens to data privacy.

In general, employers will be responsible for Interpreting and applying these obligations (though there are responsibilities on individual employees) but for those surgeons in part-time or wholetime private practice, there will be an individual obligation to ensure data is held in accordance with the regulations.

This document provides guidance as to how individual practitioners could ensure that their Private Practice is compliant with the regulations. We have drawn heavily on the work of the Data Protection Woking Group of the ICGP who have produced an excellent set of guidelines as a service to GPs and their patients. RCSI would like to thank ICGP for their permission to reuse and adapt their guideline for this booklet.

These guidelines apply to **patient personal data** processed in all forms of media, including paper records, electronic records and documents, images, videos, SMS texts, online postings and electronic messages as used in the provision of routine surgical (including pre-operative and post-operative) care.

These guidelines do not address issues arising from processing of personal data in the context of employment or other contractual relationships and surgeons should seek specialised advice in these areas.

The law in this area is in evolution and you should refer to our website for the latest version of our guidelines. Please note that these guidelines are for advice only and should not replace personalised legal advice.

GLOSSARY

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. This is distinct from consent for examination or treatment which is covered in more detail in Code of Practice for Surgeons 2018 and in the HSE National Policy on Consent.

'Data 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. As a medical practitioner, you are the data controller for your patients records.

'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. For example, 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. In surgical practice, this might include your secretary or others working with you who have access to patient data including the supplier of your patient record system.

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

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

2. RECORDS OF PROCESSING ACTIVITIES

Article 30 of GDPR specifies that 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.

A template Record of Processing Activities is included in the appendices. It may assist you in completing this template to consider the following issues:

a) Identifying the Data Controller

If your practice is established as a legal entity, then the practice is the data controller. Otherwise, you (and/or your colleagues if working in a group) should be identified as the data controller or joint data controllers. Employees are not data controllers.

b) Purpose of the Processing

The data collected as part of the process of surgical care will include a wide variety of information all of which is necessary as part of the process of making a diagnosis, recording the rational for treatment and the treatment provided and appropriately communicating with others who have responsibility for other aspects of care.

c) Categories of Personal Data

Examples of the catgories of data that might be collected include

Administrative data which is necessary to support the administration of patient care e.g. name, address, contact details (phone, mobile, email), dates of appointment

Medical Record data which is necessary to provide surgical care e.g. Individual Health identifier, Other record numbers (MRN) date of birth, family history, contact details of next of kin, medication details, allergy details, current and past medical and surgical history, laboratory test results, imaging test results, ECGs, images, and other data required to provide medical care.

Account Details which is required for providing a service and billing and/or for submission of reimbursement claims to insurers e.g. record of billable services provided, patient name, address, contact details, billing and payment records, private insurer and/or record number.

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

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 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 you will rely upon a combination of Article 6 to process non sensitive data and Article 9 conditions to process special categories of data.

The processing of personal data in medical practice is necessary in order to protect the vital interests of the patient and for the provision of health care and, in some cases, public health. The lawfulness of processing data for the provision of medical care based on the provisions in these articles rather than explicit patient consent.

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

d) Categories of Recipients to Whom Personal Data may be disclosed

These are broken down into four categories:

- sharing data in relation to the provision of medical care
- sharing data with data processors where a contract is required
- sharing data under legal arrangements
- sharing data for public health purposes.

Recipients with whom we may share personal data:

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

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 between doctors this referral is discussed and agreed between the patient and the doctor. As part of this decision, there is an understanding to be open and transparent, with all relevant medical information being shared between doctors 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 doctor open to regulatory sanction or a medical negligence action. The transmission of personal data concerning health is part of the referral process and part of the practice of medicine. It does not need a separate signed patient consent form.

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

e) Transfers to a Third Country

During standard operating procedures, patient records shall not be transferred outside of the European Economic Area (EEA). Where patient data is to be transferred, explicit consent is required which must include informing the patient of the risks of such transfers of the personal data outside of the EEA (Art 49.1(a)). In emergency situations where, for example, a patient has a medical event in the USA and transfer of medical records is required to support their care and they are physically or legally incapable of giving consent, such transfer is permitted (Art 49.1(f)). However, where possible, patients should explicitly consent to such a transfer of medical records and evidence of this consent should be retained.

f) Time Limits

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

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

Type of Healthcare Record	Retention Period
General (adult)	8 years after last contact, unless in the interest of the Data Subject to retain *
Deceased persons	8 years after death
Children and young people (all types of records relating to children and young people)	Retain until the patient's 25th birthday or 26th if young person was 17 at the conclusion of treatment, or 8 years after death. If the illness or death could have potential relevance to adultconditions 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

*At all times the interest of the patient must be to the forefront and records should not be deleted where it is not in the best interests of the data subject (patient). For example, a 25-year- old man has treatment for a malignant melanoma and after recovery is discharged and not seen again for 8 years. 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 data controller must commission regular information security audits to ensure that appropriate measures are in place to secure patient data in the practice. Such an audit should cover:

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

3. COMPLIANCE WITH DATA PROTECTION PRINCIPLES

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

- Lawfulness, Fairness and Transparency
- Purpose Limitation
- Data Minimisation
- Accuracy
- Integrity and Confidentiality
- Accountability

a) Lawfulness, Fairness and Transparency

Doctors must ensure the lawful, fair and transparent processing of personal data. Section 2 of this Guideline describes Records of Processing Activities detailing the purpose of processing, lawfulness of processing, categories of recipients to whom the personal data will be disclosed, and envisaged time period for retention. Any processing activities outside of the areas detailed in Section 2 requires the data controller 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

The **practice privacy statement** must be made available to data subjects when they register with you for care. Where possible, this notice should also be displayed in general waiting areas in the practice. You should refer to Articles 12, 13 and 14 of GDPR in relation to what needs to be included in a privacy notice. A **sample practice privacy statement** is provided in the Appendices.

The primary processing of patient personal data in clinical 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 surgery is defined in Section 2 (lawfulness of processing) and is generally not based on consent.

However, there are specific processing conditions where consent is required, particularly when disclosing of personal data to recipients unrelated to the provision of medical or social care. You must 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. You 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. You 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 within undue delay.

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

b) Purpose Limitation

Doctors are only permitted to collect and process information for an explicit purpose. If your practice is carrying out any additional processing beyond what is normal practice, then it must be included in your 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. Doctors are only permitted to collect and process appropriate information to the extent needed for the provision of medical care and to comply with all applicable statutory, regulatory, contractual and/or professional duties.

d) Accuracy

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

You must take all reasonable efforts to ensure the accuracy of the patient data. For example, if a patient has moved house, a record showing that he is currently living at his old address is obviously inaccurate. But a record showing his former address remains accurate, even though he no longer lives there.

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

e) Integrity and Confidentiality

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

f) Accountability

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

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

Once the Irish Data Protection Act 2018 is enacted, doctors will no longer be 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 or records to be kept.

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

4. Compliance with Individual Rights

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

The request or authorisation form to satisfy these individual rights should be in writing or by email and should be signed by the Data Subject or legal guardian. **An example of a request form for access to a medical record** is shown in the Appendices. It is important for the practice to verify the identity of a patient making an access request in order to ensure the personal data is only provided to the data subject

a) Right to Access

Under Article 15 of GDPR, the patient has a right to access a copy of their medical record. The doctor shall provide a copy of the patient's medical record on receipt of a signed request or authorisation form. The access request should be carried out as soon as possible, and no later than 30 days after the access request. No fee is chargeable for providing a copy of the medical record. It is important for the practice to verify the identity of the person making an access request or providing an access authorisation.

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

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

The right to access may be restricted, as per Section 54 of the Data Protection Bill 2018, if the disclosure of the record to the patient 'would be likely to cause serious harm to the physical or mental health of the data subject'. In any situation where access is denied, the doctor must advise the patient of the reason invoked for the restriction either at the time access is denied or as soon as is practical thereafter. In addition, only the part of the medical record likely to cause harm can be withheld, the rest of the medical record should be released in the usual way. The patient has a right to appeal the restriction to the Data Protection Commissioner.

b) Right to Rectification

Under Article 16 of GDPR, the patient has the right to obtain rectification of records which are factually inaccurate. However, this is not an unqualified right and depends on the circumstances of each case. Where there is disagreement between the doctor and the patient as to the inaccuracy of the record, such a dispute may be resolved by the addition of a supplementary statement in the patient record. Inaccurate patient data should be noted as such.

c) Right to Erasure

Article 17 of GDPR deals with the right to erasure. Because the doctor has a requirement under Medical Council rules (Section 33 of Guide to Professional Conduct and Ethics for Registered Medical Practitioners, 8th Edition 2016) to keep medical records and also has a right to defend medico-legal claims (under Article 23.1(g)), the right to erasure of medical records is not an absolute right and restrictions may apply. This would need to be examined on a case-by-case basis and it might be appropriate to seek independent legal advice or the opinion of your indemnifiers. You should keep a record of this advice.

d) Right to Restriction of Processing

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

e) Right to Data Portability

The right to data portability, under Article 20 of GDPR, relates to circumstances where the processing is based on consent or a contract. Although this is not the case in medical 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. You should facilitate patients moving to another doctor by providing their medical record in an electronic format where technically feasible or in a format which could be used by other doctors.

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

f) Right to Object

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

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:

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

a) Notifying the Data Protection Commission

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

b) Notifying the Data Subject

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

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

c) Data Breach Flow Chart and Examples

The Article 29 Data Protection Working Group has produced 'Guidelines on Personal data breach notification under Regulation 2016/679' This is available at https://iapp.org/media/pdf/resource_center/WP29-Breach-notification_02-2018.pdf and you are referred to pages 30 to 33 for a flowchart on notification requirements and examples of personal data breaches and who to notify.

6. Miscellaneous Provisions

a) Data Protection Impact Assessment (DPIA)

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

A doctor carrying out normal medical care for his or her patients and using an established practice software management system may not be required to carry out a DPIA. Medcial practice does not typically involve "large-scale processing". In summary, DPIAs in medical practice might be a useful tool but are not mandatory.

Where a commercial organisation or company (or a private hospital or clinic) manages a number of different practices, there may be a requirement for that organisation to undertake a Data Protection Impact Assessment.

b) Data Protection Officers (DPO)

Article 37 of GDPR deals with the designation of a data protection officer (DPO). Recital 97 discusses the need to appoint a DPO 'where the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data'. Typically, medical practice is not processing data on a "large scale" and there is no requirement to appoint a DPO in this setting.

Where a commercial organisation or company (or a private hospital or clinic) manages a number of different practices, there may be a requirement for that organisation to appoint a DPO.

However, even though GDPR do not specifically require the appointment of a DPO, it may be useful to designate a DPO on a voluntary basis. The Article 29 Data Protection Working Party ('WP29') encourages these voluntary efforts.

c) Data Protection and Cyber Security Awareness and Training Details

All practice clinicians and support staff need regular training in data protection and cyber security. A log of training activities should be maintained. Signed confirmation of training completed per employee should be retained. RCSI is exploring the possibility of providing access to suitable online training for practice staff.

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. Staff leaving the practice should have their access revoked, both to local and online applications and services, including backup services.

7. Bibliography

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

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

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

Working Party 29 Guidelines, http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360

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

Irish Data Protection Bill 2018, http://www.oireachtas.ie/viewdoc.asp?DocID=37646&&CatID=59&StartDate=01%20January%202018&OrderAscending=0

National Hospitals Office, Code of Practice for Healthcare Records Management, https://www.hse.ie/eng/about/Who/qualityandpatientsafety/safepatientcare/healthrecord smgt/Healthcare Records Management.html

Frequently Asked Questions

Retirement or Death

Q I am retiring shortly. What should I do with my private patient records?

It cannot be assumed that private patients will attend your (public) replacement and records should be forwarded to other doctors only with explicit consent from the patient. You should maintain the patient medical records accumulated at that time for an adequate period consistent with meeting legal and other professional responsibilities. During that period, the provisions of the Data Protection Acts continue to apply to that information.

Transfer of individual records

Q I have received an email from a woman requesting that I forward the medical records of herself and her husband and son who also attended me for treatment. How should I proceed?

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

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

Solicitor requests

Q 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. Am I ok to do this?

Under Data Protection legislation the patient has an entitlement to this information. However, before releasing to the solicitor, you should confirm with the patient that they do indeed want all medical information to be released. You should ensure that it contains nothing that might be injurious to the patient's wellbeing, or that would breach confidentiality with another patient or colleague. It may be reasonable in some circumstances to notify a colleague that a particular letter or result is being released, however you should not withhold it.

Email Communication

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

If there is a specific request by email from a patient to send their results back by that format, then it is reasonable to acquiesce to that request. However, if you are contemplating a standardised process of returning results, you should restrict the content of any message, and consider the potential for a data breach. You should keep the information exchanged to a minimum. An explicit and informed request from the patient should be recorded. The Patient should be informed that usual personal email providers are not secure e.g. gmail, ymail. If the patient wants their details sent by mail consider using password protected attachments.

Incidental access to information

Q 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, and IT support staff. How do we handle this?

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

Data Access Request

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

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 you are satisfied that the person was genuinely acting on behalf of, and in the best interests of, the child whose data was being requested. Revealing of medical information of a child who is capable of making decisions themselves will in most situations constitute a breach of the Data Protection Acts if undertaken without the consent of the child capable of making their own decisions.

Personal Public Service number (PPS number)

Q Can I ask for a patient's PPS number?

It is an offence for any person or body to request or hold a record of a PPS number unless they are permitted by law (the Social Welfare Acts) to do so.

Consultants are not specified bodies under the Social Welfare Acts, but you may ask patients for their PPSN as part of specified HSE schemes such as the Mother and Child scheme, Childhood Immunisations and Cervical Screening or Sickness Certification for the Department of Social Protection. The Data Protection Commissioner acknowledges that entities such as the Department of Social Protection (DSP) or the HSE are legally permitted to seek the PPSN in the context of the provision of a service. In each case, the requests must be justifiable and the capture of the PPSN must not be made on a "just-in-case" basis or be used as a practice identifier. This latter point is of particular importance, as any use of the PPSN by a doctor that is beyond that required by the HSE or DSP may leave you open to legal action under the provisions of the Social Welfare Acts.

Research Projects

Q Do I need a patient's consent to use their records in research projects?

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 obtained and documented in the patient record. Where the data is anonymised, it is no longer personal data and data protection regulations do not apply. It will be a matter to consider each project in this regard and to review that assessment periodically to ensure that the data remain anonymous or unlikely to be re-identified. Normally, the Research Ethic Committee approval will address this issue.

In general the concept of data minimisation and anonymisation 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.

Faxes

Q Is it OK to use Faxes for communicating patient data?

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

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

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

SMS Texts

Q Is it OK to use SMS texts to communicate with patients?

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. You might find the article for general practitioners useful - 'Patient texting – let's be careful out there', Forum, the Journal of the Irish College of General Practitioners, (December 2017)

Use of Healthmail

Q Can I use email to send patient identifiable clinical information?

Documents sent by normal email are not secure and can be accessed inappropriately by others before reaching their intended recipients. Secure clinical email (Healthmail) allows exchange of patient identifiable clinical information between doctor and HSE clinicians and between doctor and voluntary, maternity and children's hospitals. Healthmail is suitable for the electronic exchange of patient identifiable clinical information, including attachments.

Access to Clinical Records by Secretarial and Administrative Staff

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

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

- Identifying and printing repeat prescriptions for patients.
- Typing referral letters to GPs, other consultants or allied health professionals such as physiotherapists, occupational therapists, psychologists and dieticians.
- Opening and scanning of referral letters from GPs and other consultants
- Scanning other clinical letters, radiology reports and any other documents not available in electronic format.
- Downloading laboratory results and integration of these results into the electronic patient record.
- Photocopying or printing documents for referral to other consultants
- Handling, printing, photocopying and postage of medico legal and life assurance reports, and of associated documents.
- And other activities related to the support of medical care appropriate for practice support staff.

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

If you use a practice management software package, this 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.

Freedom of Information Requests

Q. A private patient has submitted a Freedom of Information Request for their medical record. How should I proceed?

While the records in a public hospital are subject to FOI, this may not be the case in private hospitals or clinics. However, you should provide a copy of the patients records on request (under other legislation).

APPENDICES

Appendix A: Data Protection Check List

It is good practice to review this check list annually. The completed 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 Surgeons'?		
2. Have you commissioned an information security audit of your practice computers and network?		
3. Have you identified a person in the practice with responsibility for data protection?		
4. Have you reviewed your records of processing activities to ensure all your data processing and data outflows are documented?		
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?		
6. Are you using secure clinical email 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 Practice Software Vendor, your online backup service, 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?		
10. Do you have a protocol in place to manage a Data Breach?		
11. Have you identified the person or legal authority that is the data controller in your practice?		
12. Do you have a practice privacy statement on display in the waiting room and available to patients?		

Check List Reviewer: _____

Date of Review: _____

Appendix B: Sample Request for Transfer of patient records

Mr Joseph Bloggs
Private Clinic,
Phone: 01 123456

<Date>

To: <Dr Name>
<Dr. Address>

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

Dear <Dr Name>

The above has decided to transfer their specialist care to me. I would be grateful if you could send me a copy of the medical records you hold regarding this patient. Signed patient consent in accordance with Data Protection Regulations has been provided below.

Yours Sincerely

_____
Mr Joseph Bloggs FRCSI

PATIENT SECTION

<Date>

I _____ (PRINT NAME)
consent to the release of my medical records to Mr 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 Doctor	
Address of practice	

Patient

First Name	
Family Name	
Date of Birth	
Address	
Signature	
Date	

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

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

Appendix D: Waiting Room Notice

Data Protection Regulations

Medical Records

A surgeon's 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 the RCSI 'Processing of Patient Personal Data: A Guideline for Surgeons.

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

Thank you.

Appendix E: Practice Privacy Statement

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

Practice Privacy Statement

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

Legal Basis for Processing Your Data

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

Managing Your Information

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

- We retain your information securely.
- We will only ask for and keep information that is necessary. We will attempt to keep it as accurate and up to-date as possible. We will explain the need for any information we ask for if you are not sure why it is needed.

- We ask you to inform us about any relevant changes that we should know about. This would include such things as any new treatments or investigations being carried out that we are not aware of. Please also inform us of change of address and phone numbers.
- All persons in the practice (not already covered by a professional confidentiality code) sign a confidentiality agreement that explicitly makes clear their duties in relation to personal health information and the consequences of breaching that duty.

- Access to patient records is regulated to ensure that they are used only to the extent necessary to
  - enable the secretary or manager to perform their tasks for the proper functioning of the practice. In this regard, patients should understand that practice staff may have access to their records for:
    - » Identifying and printing repeat prescriptions for patients.
    - » Typing referral letters to GPs, other consultants or allied health professionals such as physiotherapists, occupational therapists, psychologists and dieticians.
    - » Opening and scanning of referral letters from GPs and other consultants
    - » Scanning other clinical letters, radiology reports and any other documents not available in electronic format.
    - » Downloading laboratory results and integration of these results into the electronic patient record.
    - » Photocopying or printing documents for referral to other consultants
    - » Handling, printing, photocopying and postage of medico legal and life assurance reports, and of associated documents.
    - » And other activities related to the support of medical care appropriate for practice support staff.

Disclosure of Information to Other Health and Social Care Professionals

We may need to pass some of this information to other health and social care professionals in order to provide you with the treatment and services you need. Only the relevant part of your record will be released. These other professionals are also legally bound to treat your information with the same duty of care and confidentiality that we do. We will regularly communicate with your general practitioner of other referring doctors to appease them of your clinical progress.

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 will only provide a confirmation that you are unfit for work with an indication of when you will be fit to resume work. Where it is considered necessary to provide additional information we will discuss that with you.
- In the case of disclosures to insurance companies or requests made by solicitors for your records we will only release the information with your signed consent.

Use of Information for Training, Teaching and Quality Assurance

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

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

Use of Information for Research and Audit

It is usual for patient information to be used for research and audit in order to improve services and standards of practice. Information used for such purposes is done in an anonymised or pseudonymised manner with all personal identifying information removed.

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

Your Right of Access to Your Health Information

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

Transferring to Another Doctor

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

Other Rights

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

Questions

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

Appendix F: Data Protection Accountability Log

Overview

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

Accountability Log

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

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

Date	Event	Description
18/11/2017	RCSI Charter Day	Attendance at information session on GDPR
08/01/2018	Audit Meeting	All consultants staff meeting to review data protection guidelines
01/04/2018	Security Audit	Information Security audit by Secure Systems Ltd
26/05/2018	RCSI training day	Attendance by practice manager at workshop on GDPR

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 Practice Software Vendors and any other data processors;
- Where processing on basis of consent, records of this consent;

Accountability Log for General Data Protection Regulation (GDPR)

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

Date	Event	Description

Appendix H: Staff Confidentiality Agreement

Surgeon 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 surgeon or data controller.
- Not to access records belonging to me, members of my family or those known to me without advance authorisation from the data controller.
- 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

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

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

Category of Personal Data	Purpose of Processing	Lawfulness of Processing
Administrative: name, address, contact, details(phone, mobile, email), dates of appointment, etc	Necessary to support the administration of patient care	Article 6.1(d): processing is necessary in order to protect the vital interests of the data subject or of another natural person. Special Categories are processed under the derogations in Articles derogations in Articles 9.2(h) and 9.2(i). Please see the notes under this table
Medical Record: Individual Health identifier, date of birth, religion, sexual orientation, gender, family history, contact details of next of kin, medication details, allergy details, current and past medical and surgical history, genetic data, laboratory test results, imaging test results, other data required to provide medical care.	Necessary to provide patient care	Article 6.1(d): processing is necessary in order to protect the vital interests of the data subject or of another natural person. Special Categories are processed under the derogations in Articles derogations in Articles 9.2(h) and 9.2(i). Please see the notes under this table

Account Details: record of billable services, provided, patient name, address, contact details, billing and payment records	Required for providing a service and billing	Article 6.1(c): processing is necessary for compliance with a legal obligation to which the controller is subject (Revenue, Medical and Legal Obligations), and Article 6.1(b) in relation to getting paid for providing a service to private patients necessary for compliance

Recipients with whom we share personal data

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

RCSI Royal College of Surgeons in Ireland
Coláiste Ríoga na Máinleá in Éirinn
123 St Stephen's Green, Dublin 2
Tel: +353 1 402 8594
Email: pcs@rcsi.ie
rcsi.ie

EDUCATIONAL AND RESEARCH EXCELLENCE IN SURGERY MEDICINE PHARMACY PHYSIOTHERAPY NURSING & MIDWIFERY LEADERSHIP POSTGRADUATE STUDIES RADIOLOGY DENTISTRY SPORTS & EXERCISE MEDICINE