General Data Protection Regulation (GDPR)

Guideline and Action Points for Hospital Consultants

IRISH HOSPITAL CONSULTANTS ASSOCIATION

HERITAGE HOUSE

DUNDRUM OFFICE PARK

DUBLIN 14

TELEPHONE: 298 9123

FAX: 298 9395

e-mail: **info@ihca.ie**

website: **www.ihca.ie**

Disclaimer

The IHCA is not licensed or regulated to provide legal advice. The information contained in this document is intended as general guidance only. If you are unsure about any aspect of your data protection obligations, you should consider obtaining specific legal advice separately before taking action based solely on the information provided in this Guideline.

Summary List of Action Points

As you read this Guideline you will note that there are a number of Action Points included throughout the document. For ease of reference, the full list of Action Points is set out below.

ACTION POINT 1: If, having reviewed Section 2.2, you have determined that you are a Data Controller then you should take steps to follow and implement this Guideline and all other Action Points in full. If you are a Processor, you have less onerous obligations under GDPR but should refer to Section 4 of this Guideline and the relevant Action Points identified therein.

ACTION POINT 2: Review and complete the template *Records of Processing Activity* in Appendix A. This template allows you to consolidate information on categories of personal data held and the parties involved in the sharing of personal data.

ACTION POINT 3: Review section 3.1.1 and consider whether you need to enter into a *Processor/Controller Agreement* as set out in Appendix B or rely on the template *Data Sharing Arrangements* as set out in Appendix C.

ACTION POINT 4: Ensure that you and your staff, if any, are familiar with and adhere to the retention periods outlined in Section 3.2. Put in place procedures so that files are reviewed periodically and disposed of securely where required.

ACTION POINT 5: Review the template *Practice Privacy Statement* in Appendix D and the template *Privacy Notice* in Appendix E and adapt them according to your practice.

ACTION POINT 6: In circumstances where you require explicit patient consent, review the template *Patient Consent Form* included in Appendix F and adapt it according to your practice.

ACTION POINT 7: Review and complete the template *Data Protection Accountability Log* included in Appendix G. The log should be updated periodically.

ACTION POINT 8: Circulate this Guideline document to all staff having particular regard to the *IT Guidance Document* as included in Appendix J. Ensure that all staff are familiar with and adhere to this Guideline.

ACTION POINT 9: Ensure that all relevant personnel who may have access to areas or systems where personal data is stored enter into a *Confidentiality Agreement* using the template included in Appendix H.

ACTION POINT 10: An outline process for dealing with Subject Access Requests is included in Appendix I. The template should be adapted according to your practice.

ACTION POINT 11: Appendix I includes a template policy for Subject Access Requests and how you deal with rectification, erasure, restrictions on processing and data portability. The template should be adapted according to your practice.

ACTION POINT 12: Review the IT guidance document included in Appendix J. If you have specific concerns regarding the security and integrity of your IT systems, seek advice and commission a regular information security audit from your IT provider or an appropriately qualified service provider.

ACTION POINT 13: Review the template *Data Breach Response Plan* in Appendix K and adapt it according to your practice.

CONTENTS

1 INTRODUCTION

1.1 OBJECTIVE OF THIS GUIDELINE

The General Data Protection Regulation (GDPR) is an EU regulation that is intended to strengthen data protection and privacy rights for European Citizens.[1] It is supported by updated Irish legislation in the form of the Data Protection Act 2018.[2] This Guideline is intended to outline the requirements for Consultants to achieve compliance with their data protection obligations in both regards.

The GDPR has major implications for the way in which Consultants and their staff process and manage patients' personal data**. Consultants who satisfy the GDPR definition of a 'Controller' or 'Processor' (see Section 2.2 below) should note that GDPR compliance is not discretionary**. Enforcement actions for non-compliance include the imposition of fines which may be as high as €20m or 4% of annual turnover, whichever is the greater. In addition, failure to comply could result in significant reputational damage for a Consultant and his or her practice, for example in the case of a data breach, given the sensitive nature of the data that is generally processed in respect of patients.

This Guideline is comprised as follows:

- An overview of the legal basis for processing by Consultants
- A series of practical action points
- Frequently asked questions
- A suite of template policies and procedures

Please note that all of the template policies and procedures in the appendices are available and have been circulated separately in MS Word format so that you can amend and adapt them as necessary.

1.2 SCOPE AND APPLICATION OF THE GUIDELINE

It is beyond the scope of this document to provide an exhaustive list of the issues and appropriate actions that Consultants need to consider in the context of their GDPR obligations. Rather, the aim of this Guideline is to give Consultants a solid base from which they can progress with a view towards reaching GDPR compliance.

This Guideline considers data protection issues for Consultants practising in public and/or private settings. It applies to personal data processed in all forms of media including paper records, electronic records and documents, images, videos, emails, SMS text, and any other electronic message format.

Please note that the IHCA is not regulated or licensed to provide legal advice. Accordingly, adhering to this Guideline and adopting the Actions Points outlined herein will not guarantee that your practice achieves GDPR compliance. Due to the variability and the specific nature of the services delivered across different Consultant practices, each Consultant together with his or her staff will need to spend some time and effort to ensure that they become GDPR compliant. The Association's Guideline will assist in this process but it

[1] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[2] Available at: http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html

may, in some instances, be necessary to obtain independent, specialist advice, depending on the nature of your practice.

Requirements under GDPR and relevant domestic data protection legislation are subject to change and will evolve over time. Consultants are advised to review their practice and procedures on a periodic basis taking account of emerging legislation.

1.3 Establishing the Legal Basis for Processing of Data

Articles 6 and 9 of the GDPR provide the legal basis for processing of patients' personal data by Consultants.[3]

Article 6(1)(b) provides a legal basis for processing where "*processing is necessary for the performance of a contract to which the data subject is party …*"[4]

However, given that health data is a special category of personal data, Consultants cannot rely solely upon Article 6(1)(b) and must also rely upon one or more of the exemptions set out in Article 9.

There are two exemptions in Article 9 that are relevant in this context. Article 9(2)(a) applies where the patient has given explicit consent and Article 9(2)(h) applies where processing is necessary for the purposes of (with emphasis):

> *"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;"*

The legal basis for processing of data by Consultants is therefore derived from the necessity for the performance of a contract to which the patient is a party and where either (a) the patient has provided explicit consent or (b) where the processing is necessary for the purpose of medical diagnosis, the provision of health or social care or treatment.

For most patients therefore, it is generally not necessary to obtain explicit consent to process their personal data.[5] However, there are some exceptions. Explicit and informed consent is required for some defined data outflows, for example to health insurance companies, solicitors and for research or clinical audit purposes. Please refer to Sections 3.1.2, 3.1.3, 3.1.4 and 3.3.2 for further details in this regard.

---

[3] Article 6 and Article 9 work in conjunction with one another. For instance, a Consultant will rely upon a combination of Article 6 to process non-sensitive data and Article 9 to process special categories of data. The legal underpinning for the processing in many of these cases is contained in relevant national legislation.

[4] Article 6(1)(d) relating to "vital interests" and Article 6(1)(f) relating to "legitimate interests" apply in very limited circumstances as a legal basis for processing, for example in emergency situations or where a patient is incapacitated, etc. They cannot be relied upon to provide a legal basis for the more general processing of personal data by Consultants in private practice.

[5] However, as a matter of common law and basic medical ethics, patient consent must be obtained for medical examination, treatment, service or investigation.

2 AM I A DATA CONTROLLER?

2.1 RELEVANT DEFINITIONS

Before you consider your status under GDPR, whether as a Controller or Processor, you should familiarise yourself with the following GDPR definitions:[6]

'**anonymisation'** means transforming personal data in a manner that makes it impossible to identify individuals. This should be irreversible and the resulting data should not be capable of being linked to other data about an individual, or being used to deduce an individual's identity.

'**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";

> Please note that this refers to the issue of consent for the processing of personal data and not the issue of consent for medical treatment. Informed patient consent for medical treatment continues to be a requirement and it should be documented accordingly.[7]

'**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";

'**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";

'joint controller' is a concept introduced by GDPR, where two or more controllers jointly determine the means and purposes of processing. The controllers must set out a clear description of their respective responsibilities for compliance with GDPR obligations, with particular regard to the rights of the data subject. This can arise where controllers share data between them as peers in a collaborative way.

'**personal data**' means any information relating to an identified or identifiable natural person, where 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". It is important to be aware of one's obligations regarding breach notifications in accordance with the law (see Section 3.6 below).

'**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

---

[6] Article 4 GDPR.

[7] For specific guidance on patient consent for medical procedures, please refer to the Medical Council's Guide to Professional Conduct and Ethics (8th Edition) available at https://www.medicalcouncil.ie/News-and-Publications/Reports/Guide-to-Professional-Conduct-and-Ethics-8th-Edition-2016-.pdf.

otherwise making available, alignment or combination, restriction, erasure or destruction. So every operation on personal data is effectively in the scope of the new Regulation. Transmitting, backing up a file or record, viewing and even destruction of data all count as processing, even if the data you process is encrypted.

'**processor**' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, for example in an outsourcing arrangement. However, an employee of the controller is not a processor acting on its behalf because, as an employee, he or she is not an independent party. This is particularly relevant for a Consultant who is employed under a public hospital contract, i.e. he or she is not considered to be a processor of the data controller hospital when dealing with or handling the personal data of public patients.

> Processors in relation to a Consultant's practice will include practice management providers, practice software system vendors, providers of online data backup services, etc. It is worth noting that Consultants may also act as processors for other Data Controllers. See Sections 3.1.1 and 4 below for guidance regarding processors generally.

'**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.

2.2 WHAT DOES THIS MEAN IN PRACTICE?

In this section, references to a Consultant should be interpreted to include an individual Consultant or a group of Consultants who operate in a group practice or partnership.

When a Consultant collects or processes data in respect of a public patient in a public hospital/facility, they generally do so in their capacity as an employee of the public hospital/facility. In that case, the Consultant is neither a Controller nor a Processor, as the Consultant is not considered to be an independent party to the hospital/facility employer which is the Data Controller in this instance.[8]

However, the situation is different where a Consultant processes personal data in respect of a patient, whether in a public or private hospital/facility, and where they are doing so as an independent party engaged in private practice, rather than as an employee of the hospital/facility.

In those circumstances, the following questions need to be considered:

- Do you keep or process any information about your private patients?
- Do you decide the kind of personal information that is going to be kept?
- Do you decide the use to which the information will be put?

[8] However, the Consultant still has certain obligations as an employee to ensure the security and confidentiality of personal data over which the employer is Controller. The HSE has issued guidance for its employees in this regard. See: https://www.hse.ie/eng/gdpr/hse-data-protection-policy/hse-data-protection-policy.pdf and https://www.hse.ie/eng/services/yourhealthservice/info/dp/dpstaffguide.pdf.

You are a Data Controller if you "*determine the purposes and means of the processing of personal data*" and, in that event, you should take steps to follow and implement this Guideline and Action Points in full.[9]

Personal data in respect of private patients in public and private hospitals is typically stored or recorded in hard copy form on a patient chart as maintained by the hospital, e.g. in the hospital's medical records library, or in soft copy form on the hospital's IT system, e.g. PIMs, NIMIS, etc. However, in some cases, personal data in respect of private patients may also be stored on a separate patient file and/or IT system as maintained by a Consultant or group practice/partnership, particularly where patients are seen and reviewed in private rooms or private outpatient clinics.[10] **Where a Consultant maintains a separate patient file for a private patient as distinct from that of the hospital/facility, the Consultant is considered to be a Data Controller in respect of the patient's personal data contained therein, whether in electronic or hard copy form.**

Most Consultants who work in full-time private practice will have practice rights or admitting privileges in a private hospital or clinic. Consultants who hold public hospital contracts that permit off-site private practice may also have similar arrangements. The very nature of the relationship between a private hospital or clinic and a Consultant means that personal data must be shared to enable appropriate medical care for patients. You may be requested by a private hospital or clinic to enter into a data sharing or data processing agreement in this context. It is beyond the scope of this Guideline to include comprehensive guidance in this regard. The IHCA is not licensed or regulated to provide legal advice. If you are requested to enter into a data sharing agreement, you should consider obtaining independent legal advice, in particular, on the issue of joint liability for data breaches and the possibility that you would be requested to provide an indemnity related to same.

Finally, there are some limited circumstances in which a Consultant may be considered to be a Processor rather than a Controller, for example, where he or she undertakes medico-legal work which entails processing patient data on behalf of another party. Examples include the provision of a medico-legal report to the State Claims Agency, Mental Health Commission, solicitors or an insurance company. Consultants who engage in this kind of work or any other processing on behalf of a Controller should refer to Section 3.1.1 and Section 4 below. It should be noted that a Consultant who is commissioned to prepare a report in respect of a patient for occupational health purposes is likely to be considered a Data Controller regardless of the fact that the report may have been requested by the patient's employer.

ACTION POINT 1: If, having reviewed Section 2.2 above, you have determined that you are a Controller then you should take steps to follow and implement this Guideline and all other Action Points in full. If you are a Processor, you have less onerous obligations under GDPR but should refer to Section 4 of this Guideline and implement the relevant Action Points identified therein.

[9] Definition of a Data Controller under the EU General Data Protection Regulation

[10] It is also possible that some data in respect of private patients will be duplicated as between the records maintained by the hospital/facility and those maintained by the Consultant. Equally, it is possible that some data will be recorded on the hospital/facility system only but not on the Consultant's, and vice versa.

3 WHAT ACTIONS DO I NEED TO TAKE AS A CONTROLLER?

3.1 CREATE AND MAINTAIN RECORDS OF PROCESSING ACTIVITIES

Under GDPR, a Controller is required to maintain *Records of Processing Activities*.[11] In order to create and maintain your records, you must first establish the categories of personal data that you collect or process. Table A shows the categories of personal data typically collected, generated or processed by Consultants.

Table A: Categories of personal data typically collected, generated or processed by Consultants

Category of Personal Data	Purpose of Processing	Lawfulness of Processing	Retention Period
Administrative: • Name • Address • Contact details (phone, mobile, email) • Dates of appointment	Necessary to support the administration of patient care.	Article 6(1)(b) provides a legal basis for processing where "*processing is necessary for the performance of a contract to which the data subject is party …*"	Linked to financial records, retention as per Revenue requirements. Revenue requires individuals/organisations to retain financial records for 7 years.
Medical Record: • Individual health identifier • GMS number • 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 • Imaging test results • Photographs • Near patient test results • ECGs	Necessary to provide patient care.	Article 9(2)(h) applies where 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;"*	For adults: 8 years after last contact, unless in the interest of the Data Subject to retain. For Children (under 18 years of age): Retain until the patient's 25th birthday or 26th if young person was 17 at the conclusion of treatment, or 8 years after death. If the illness or death could have potential relevance to adult conditions or have genetic implications, consider whether it is appropriate to retain the records for a longer period. Deceased Persons: 8 years after death. Maternity: 25 years after birth of last child.

[11] Article 30 of GDPR

• Ultrasound scan images • Other data required to provide medical care			
Account Details: • Record of billable services provided • Patient name • Address • Contact details • Billing and payment records for private patients • Private health insurance details	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 securing payment for providing a service to private patients.	Revenue requires organisations to retain financial records for 7 years. The retention period for financial records is provided for in the Companies Act 2014. In particular, Chapter 2, Accounting Records, comprises the following Sections: 281. Obligation to keep adequate accounting records 282. Basic requirements for accounting records 283. Where accounting records are to be kept 284. Access to accounting records 285. Retention of accounting records 286. Accounting records: offences Specifically Section 285 states: "An accounting record required to be kept by section 281 or information or a return referred to in section 283 (2) shall be preserved by the company concerned for a period of at least 6 years after the end of the financial year containing the latest date to which the record, information or return relates."

The *Records of Processing Activities* must contain:

a) The name and contact details of the data 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 has 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

Please note that the obligation applies when the processing is of a 'high-risk' nature, including processing of special categories of personal data such as health information.

Note: This information is also required for compliance with other obligations set out in the GDPR such as:

- Demonstrating transparency and providing information to data subjects
- Integrity and confidentiality, i.e. establishing the relevant technical and organisational measures including security measures for personal data and the implementation of data protection policies

- Accountability for compliance with the principles
- Undertaking data protection impact assessments
- Ensuring data protection by design and by default
- Demonstrating compliance to the Data Protection Commission
- Reporting data breaches

Having established the categories of personal data that you collect or process, you need to identify the categories of parties involved in the sharing of that personal data, i.e. transferors and recipients. These are shown in Table B below.

Table B: Sharing of Data - Categories of Transferors and Recipients

Categories of Transferors and Recipients	Description
Healthcare Providers, Social Care Providers	Other Consultants, General Practitioners, Public Hospitals, Private Hospitals and Clinics, Health Service Executive, Occupational Therapists, Occupational Health Physicians, Opticians, Palliative Care Services, Pharmacies, Psychologists, Physiotherapists, Speech and Language Therapists, Social Workers, Nursing Homes, Counselling Services, Diagnostic Imaging Services, Hospital Laboratories, Practice Support Staff, GP Locums, Acute Hospital and Community Services clinical staff, Prison Service clinical staff, Mental Health Commission, and other healthcare providers.
Data Processors (contractual)	Practice Software Vendors, Online Data Backup Companies, Practice Management Services, Debt Collection Agencies, Dictation Service Providers
Legal Proceedings or Legal Affairs	Coroner, HIQA, Medical Council, Medical Indemnifier/Insurer, Revenue Commissioners, Social Protection, Tusla, Solicitors in Regulatory Bodies in relation to legal cases, Office of Ward of Courts regarding capacity cases, Gardaí or authorised offices in relation to Mental Health legislation.
Public Health Entities	Infectious disease notifications, influenza surveillance, National Cancer Registry and other National Registries, International Databases for benchmarking patient outcomes.
Third Parties (under explicit patient consent)	Health Insurance Companies, Solicitors, Banks, Insurance Companies, etc.

ACTION POINT 2: Review and complete the template *Records of Processing Activity* in Appendix A. This template allows you to consolidate information on categories of personal data held and the parties involved in the sharing of personal data.

3.1.1 A Note on Data Sharing Arrangements and Controller/Processor Agreements

If you transfer personal data to another third party for processing under an agreement or contract, for example a billing agent, then you need to ensure that all parties to the agreement are aware of and compliant with their respective obligations. Similarly, if you are receiving data from another controller and processing it on their behalf, you may be requested to enter into an agreement with that party.

Most third parties will include data protection provisions within their respective agreements or contracts with you. You need to review these carefully. It is beyond the scope of this document to provide definitive guidance with regard to such provisions as they will vary on a case by case basis. Having reviewed any such agreements, you should consider whether you need to obtain independent legal advice.

If there is no such agreement or contract already in place, then you should consider the nature of your relationship with the third party and act accordingly as follows:

(a) **Controller/Processor**: If a third party is acting as a processor on your behalf where you are the Controller, you can adapt and use the template Processor/Controller agreement in Appendix B, for example, where you transfer personal data to a dictation service provider.

(b) **Controller/Controller**: If you, as a Controller, are transferring to or receiving personal data from another Controller, you can furnish a copy of the template Data Sharing Arrangements in Appendix C.

ACTION POINT 3: Review section 3.1.1 above and consider whether you need to enter into a *Processor/Controller agreement* as set out in Appendix B or rely on the template *Data Sharing Arrangements* as set out in Appendix C.

3.1.2 A Note on Referrals between Consultants and/or GPs

The healthcare community is one that operates on the basis of trust. All Consultants and GPs are subject to rules and ethical obligations relating to privacy and patient confidentiality which are overseen by the Medical Council. When a patient is referred to a Consultant by a GP or Consultant colleague, this referral is generally discussed and agreed between the patient and the referring doctor. As part of this discussion, it is understood that all relevant medical information will be shared with the Consultant in order to provide medical treatment. In fact, to omit any relevant information would leave the referring doctor exposed from a medico-legal perspective. The transfer of personal data concerning health is necessitated by the referral process and it is integral to the practice of medicine. **It does not require explicit consent from the patient.** The same principles apply with regard to referrals from one Consultant to another Consultant colleague.

When sharing patients' personal data with other parties who are data controllers in their own right, such as a public or private hospital, the responsibility for compliance with data protection regulations, including subject rights, falls to that party. It is important in these circumstances that each entity understands their respective responsibilities. See Sections 2.2 and 3.1.1 above.

3.1.3 A Note on Transferring Personal Data to Private Health Insurers

There are certain processing activities associated with the provision of healthcare and medical services which do not require explicit consent, such as referral of the patient to another doctor or processing of personal data for administration purposes, for example by a Consultant's dictation service provider, subject to appropriate safeguards and a data processing agreement being in place.

However, submitting a patient's personal data to his or her health insurer for the purpose of claims processing requires the patient's explicit consent. Consultants can rely upon the patient consent that is included in the health insurance claim form as signed by the patient for the purpose of submitting a claim to the patient's health insurer and for the purpose of dealing with subsequent queries and processing of the claim generally. It is not necessary to obtain separate explicit consent from the patient if the health insurance claim form is in order and signed by the patient.

Consultants generally have access to the medical records and patients' personal data that are in the custody of the public or private hospital where the Consultant delivers patient care. These records and data may only

be accessed and used for the purpose of delivering medical care or for the purpose of claims submission to a health insurer where the patient has signed and provided his or her explicit consent on the form.

Regardless of the purpose for which a patient's personal data is provided to a health insurer and regardless of whether the data is stored or recorded by a hospital/facility or Consultant, it remains at all times the patient's personal data. It is not appropriate to comply with a request from a health insurer for the entirety of the patient's chart or medical history. For example, if a health insurer has requested additional personal data for the purpose of processing a specific claim, then the personal data provided should be confined only to that data which is necessary for the processing of the claim, consistent with the principle of data minimisation.

Consultants will be aware that health insurers often request medical records or personal data for audit purposes, for example in the context of a review of billing practices, utilisation review, pre-payment checking, post payment audit of claims, etc. **In such circumstances, a Consultant cannot rely upon the consent provided by the patient on the health insurance claim form as a legal basis for the transfer of such records or data.** There is a concern that the current data protection and consent provisions in the relevant health insurance claim forms either (i) do not address or authorise this kind of additional processing or (ii) include general consent provisions that are too wide ranging and do not satisfy GDPR requirements regarding informed consent. A separate explicit confirmation of consent is therefore required from the patient in these circumstances and the health insurer should demonstrate to the Consultant that the patient has so consented.

Finally, it has been noted that health insurers have adopted a practice of requesting medical records or patients' personal data for audit purposes to be transferred to them by way of registered post. This practice may potentially create risks in terms of data minimisation, retention, purpose limitation, etc. The Data Protection Commission has advised that both parties, health insurers and Consultants, as Data Controllers have an obligation to implement technical and organisational measures to ensure the security, integrity and confidentiality of personal data. The transfer of patient files off-site for audit purposes can create risks which would be mitigated by conducting audits on-site. Accordingly, insofar as possible, any such audits should be conducted on the basis that the relevant personnel from the health insurer will attend physically on the premises of the Consultant's suite or rooms with the Consultant's permission, and that medical records and personal data are not copied or removed from the premises. Any access given to a third party auditor to systems or data should be strictly under observation and, where appropriate, revoked afterwards. Access should not include transfer of personal data to removable media.

3.1.4 A Note on the Use of Personal Data for Research and Audit, Quality Improvement and Surveillance

Consultants engaged in the processing of personal data for the purposes of health research must have regard to the requirements set out in the Health Research Regulations made pursuant to the Data Protection Act 2018.[12] The regulations require mandatory, suitable and specific safeguards to be implemented for the processing of personal data for health research. If you are engaged in health research activity, you should review the regulations in detail as the information included in this section is provided only by way of general guidance.

The collection and distribution of personal data for research purposes should be conducted on an anonymised basis as distinct from pseudonymisation (see definition in Section 2.1). There are certain exceptions to this where legislation permits analysis and research on patient identifiable clinical information, for example the Infectious Disease regulations and the National Cancer Registry. If research entails the utilisation of identifiable

[12] Data Protection Act 2018 (Section 36(2)) (Health Research) Regulations 2018, available at: http://www.irishstatutebook.ie/eli/2018/si/314/made/en/pdf

patient clinical information, then explicit patient consent must be sought and documented in your records. (See Section 3.3.2 and Action Point 6 below). Where the data is anonymised, it no longer constitutes personal data and data protection restrictions do not apply. Assessments should be carried out periodically to ensure that the data remains anonymous and is unlikely to be re-identified.

The concept of data minimisation and anonymisation should be maintained at all times for health research. Where informed patient consent is used as the legal basis for research in circumstances where identification is required and consented to, the data controller must be able to demonstrate that consent has been provided and must facilitate the right of the patient to withdraw consent at any time. (See Section 3.3.2 below.)

It is normal for patients' personal data to be used for research, audit, and surveillance in order to improve services and standards of practice. Information used for such purposes must be processed either with the patient's consent or in an anonymised manner with all personal identifying information removed. It is perfectly reasonable to carry out these activities in the interest of maintaining and improving a high quality of service to your patients as long as appropriate data protection safeguards are in place.

Generally, in the context of processing personal data for health research purposes, the default position is that the patient's explicit consent is required unless the personal data is wholly anonymised or there is specific legal provision authorising the health research in question. The institution you are working for will have arrangements in place for research implementation by the Research Ethics Committee.

Regulations made pursuant to the Data Protection Act 2018 provide for the establishment of a Health Research Consent Declaration Committee which can make consent declarations that would allow researchers to collect and use personal data without the explicit consent of the data subject only in very specific circumstances. To protect the individual, consent declarations may only be given by the Committee where obtaining consent is not possible and where the public interest in carrying out the research concerned significantly outweighs the need for consent. In such circumstances, a data controller carrying out health research using personal data may apply for a consent declaration which means that the consent of the individual is not required for the obtaining and use of his or her personal data for the health research concerned. For further information see www.hrcdc.ie.

3.2 ADHERE TO RECOMMENDED DATA RETENTION PERIODS

Personal data in a form that permits identification of data subjects should not be retained for a period longer than is absolutely necessary and should only be utilised or processed for specified purposes. The principles of storage and purpose limitation apply to medical records. In the process of determining a reasonable and justifiable time frame, the applicable legal and operational requirements should be taken into consideration (Table C). Furthermore, when personal data is processed solely for health or scientific research it may be stored for longer periods. However, in both cases, appropriate technical and organisational safeguards have to be adopted.

The retention periods for medical records in Table C are adopted from the HSE's '*National Hospitals Office, Code of Practice for Healthcare Records Management'.* [13] These periods are also in line with the recommendations of medical indemnity providers and the Health Information and Quality Authority (HIQA). In addition, the HSE published a policy document in 2013 which sets out a range of differing retention periods

[13] Further information can be found at: https://www.hse.ie/eng/services/publications/hospitals/nho-code-of-practice-for-healthcare-records-management-version-2-0.pdf

for different types of healthcare records. Basic records in the form of hospitals charts are assigned a retention period of "*8 years after conclusion of treatment or death*".[14]

Table C: Recommended Retention Periods

Type of Healthcare Record	Recommended Retention Period
General (Adult)	8 years after date of last contact
Deceased Persons	8 years after death
Children and Young Persons	Retain until the patient's 25th birthday or 26th if young person was 17 at the conclusion of treatment, or 8 years after death of patient if sooner. If the illness or death could be potentially relevant to adult conditions or have genetic implications, consider whether it is appropriate to retain the records for a longer period.
Mentally disordered persons (within the meaning of the Mental Health Acts)	20 years after the date of last contact between the patient and any healthcare professional involved in the patient's care, or 8 years after the death of the patient if sooner
Death - Cause of, Certificate counterfoils	2 years
Maternity (all obstetric and midwifery records, including those related to episodes of maternity care that end in stillbirth or where the child later dies)	25 years after the birth of the last child
Records/documents related to any litigation	Review 10 years after the file is closed
Suicide – Records of patients having committed suicide	10 years

There are circumstances where it may not be in the interest of the patient to delete his or her medical records. For example, there are certain patients who may present with a recurrence or require a revision procedure outside of the recommended time frames set out above. If you propose to exceed the recommended retention periods, it is important that you have justification or a valid reason for doing so and you should consider archiving all such personal data securely (see paragraph 6 in Appendix J) so that you can demonstrate that it is not subject to ongoing or unnecessary processing.

The Data Protection Commission also advises that workable processes are required to provide for the safe destruction, on an annual basis at a minimum, of personal data that has reached or exceeded its recommended retention period. If you are disposing of medical records or personal data that is held in hard copy format, secure shredding can be implemented in-house, but can also be carried out by a third party certified vendor.

Finally, there may be instances where you will need to retain employees' personal data for financial, taxation or employment law purposes. You are entitled to do this under GDPR Article 8(2)(b) where processing is "*necessary in the context of employment law*" and Article 9(2)(b) where processing is "*necessary in the context of employment law, or laws relating to social security and social protection*". Under current legislation, payroll data should be retained for seven years. Staff personnel files should be retained for the duration of employment plus seven years thereafter as you may need this information if any matters are subsequently litigated or pursued by a former employee under employment legislation.

[14] Further details are available at https://www.hse.ie/eng/services/yourhealthservice/info/dp/recordretpolicy.pdf

ACTION POINT 4: Ensure that you and your staff, if any, are familiar with and adhere to the retention periods outlined above. Put in place procedures so that files are reviewed periodically and disposed of securely where required.

3.3 ENSURE THAT YOU ARE COMPLIANT WITH GENERAL DATA PROTECTION PRINCIPLES

The GDPR places a requirement on Data Controllers to be able to demonstrate their compliance in line with GDPR principles and good data protection practices.

3.3.1 Lawfulness, Fairness and Transparency

Consultants who process data must do so lawfully, fairly and transparently. Appendix A of this Guideline provides a template for the creation of *Records of Processing Activities* detailing the purpose of processing, lawfulness of processing, categories of recipients and transferors involved in data sharing, and the appropriate time period for retention (see Section 3.2 above). If you are engaged in any processing activities outside of the areas detailed in Section 3.1, you should document the processing activity extensions in a similar form to Appendix A.

In addition, a *Practice Privacy Statement* (Appendix D) should be made available to patients when they register with your practice or attend for treatment. It should provide details to the patient in a concise, transparent, intelligible and easily accessible form to include[15]:

- The identity and contact details of the Controller
- The identity of the staff member with responsibility for data protection
- The information that is being collected
- Processing purposes
- Recipients or categories of recipients to whom their data will be disclosed
- Period of processing
- Information about their GDPR rights
- Lawful basis for the processing

In addition to providing a *Practice Privacy Statement* (Appendix D) to the patient, it is recommended that a *Privacy Notice* (Appendix E) is also displayed in waiting areas, Consultant rooms or some other suitable location where patients will see it.

ACTION POINT 5: Review the template *Practice Privacy Statement* in Appendix D and the template *Privacy Notice* in Appendix E and adapt them according to your practice.

3.3.2 A Note on the Circumstances in which the Explicit Consent of the Patient is Required for Processing

The legal basis for processing of data by Consultants is derived from the necessity for the performance of a contract to which the patient is a party and where the patient has either provided explicit consent or where the processing is necessary for the purpose of medical diagnosis or the provision of health or social care or treatment. These are the main grounds that provide a basis for the lawfulness of such processing by a

[15] See Articles 12, 13 and 14 of GDPR

Consultant as defined in Section 1.3 above. It is worth noting that the lawfulness of such processing is generally not based on consent.

However, there are circumstances in which the patient's explicit consent *will* be required where you are disclosing personal data to recipients unrelated directly to the provision of medical care. Consultants must obtain specific, explicit consent for these disclosures. An example of this would be sharing personal data with a health insurance company or solicitor, i.e. for any purposes that might not be immediately obvious to the patient. See section 3.1.3 above regarding private health insurance claims. If you are engaged in any research activity that involves identifiable patient clinical information, then explicit patient consent must be sought and documented in your patient records (see section 3.1.4 above).

Where consent is required for processing, the Consultant must be able to demonstrate that the patient has consented to this processing, and that the consent is informed, freely given, and provided in a clear and transparent manner. Specifically, where the lawfulness of processing requires explicit consent, there should be a process for obtaining this consent. It is worth noting that patients may also withdraw their consent in which case the Controller should document this fact in the patient record and ensure that any such withdrawal is acted upon without delay. See Action Point 6 and Appendix F.

Processing of personal data must be conducted in a fair, lawful and transparent manner. **In summary, the patient should be informed of any disclosures that you intend to make to any other party that is not directly related to the diagnosis or provision of medical care or treatment.**

3.3.3 A Note on Children and Parental Consent

The GDPR contains provisions that are intended to enhance the protection of children's personal data and to ensure that children are addressed appropriately in a way that they can understand.

> *"Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand."*[16]

Transparency and accountability are important where children's data is concerned. However, in all circumstances you need to carefully consider the level of protection you are giving that data. **It is considered good practice to obtain parental consent for the processing of children's personal data.** It is understood that the Data Protection Commission intends to issue guidance later in 2019 that deals specifically with the processing of children's data. An addendum to this Guideline will be circulated as necessary. Preliminary reports arising from the DPC's consultation exercise can be accessed at https://www.dataprotection.ie/en/news-media/consultations.

3.3.4 A Note on the meaning of 'Explicit Consent'

Despite the specific references to the requirement for 'explicit consent' in the GDPR, this term is not separately defined. **In considering and assessing whether a patient has given 'explicit consent', you should satisfy yourself that the consent as provided leaves no room for misinterpretation.**

Explicit consent should specifically refer to:

- The particular data set that is to be processed
- The precise purpose of processing (including any automated decision-making)

[16] Recital 58 of GDPR

- Identification of any risks and/or implications that might arise for the data subject as a result of the data processing, and
- The provision of any other relevant and specific information that might influence the decision of a data subject to give or withhold their consent

If you are unsure about whether you need to obtain explicit consent from a patient, consider the following questions:

- Is the personal data being shared in a manner that is unexpected or objectionable?
- Will the data being shared have a significant effect on the patient?
- Is the data sharing widespread or does it involve entities that the patient might not expect?
- Is the sharing being carried out for a range of different purposes?
- Is the patient likely to suffer any detriment as a result of any data sharing?

If you can answer yes to one or more of these questions, you should consider obtaining explicit consent.

Article 7 of the GDPR sets out what is meant by consent:

- Data controllers must be able to demonstrate that consent was given.
- Where consent is given in a written declaration which also concerns other matters, e.g. a contract, the request for consent must be clearly distinguishable, intelligible and easily accessible.
- If this requirement is not complied with, the consent will not be binding.
- Data subjects need to be informed of their right to withdraw consent at any time and it must be as easy to withdraw consent as give it.
- When assessing if consent has been freely given 'utmost' account should be taken of the fact that performance of a contract is conditional on the provision of consent to processing personal data that is not necessary for the performance of a contract.
- Where consent is being used, you will need to retain a record of that consent.

ACTION POINT 6: In circumstances where you require explicit patient consent, review the template *Patient Consent Form* included in Appendix F and adapt it according to your practice.

3.3.5 Processing for a Specific and Lawful Purpose

Consultants can collect personal data "*for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*".[17] If you process personal data for any other purposes, then it must be included in your *Records of Processing Activities* (see Section 3.1 and Appendix A). There must also be a legal basis for such additional processing and it must be transparent to the patient. You can only do this if (i) the new purpose is compatible with the original purpose, and (ii) you also obtain the individual's specific consent for the new purpose or you can point to a clear legal provision requiring or allowing the new processing in the public interest. See Section 1.3 above generally with regard to the legal basis for processing of data by Consultants.

[17] Article 5 GDPR

3.3.6 Data Minimisation

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Consultants must only collect and process the personal data that they need to achieve their processing purposes, e.g. the provision of medical care, compliance with statutory, regulatory, contractual or professional duties. Doing so has two major benefits. First, in the event of a data breach, the unauthorised individual will only have access to a limited amount of data. Second, data minimisation makes it easier to keep data accurate and up to date.

3.3.7 Accuracy

The accuracy of personal data is integral to data protection. The GDPR states that "*every reasonable step must be taken*" to erase or rectify data that is inaccurate or incomplete. It is important to note that individuals have the right to request that inaccurate or incomplete data be erased or rectified within 30 days. Maintaining accurate data is a key element in demonstrating compliance.

With regard to misdiagnoses, errors or changes in one's initial opinion, it is acceptable to keep records in this regard for future reference provided those records are not misleading about the facts. In any such situation, a note should be added by the Consultant to clarify this within the patient record.

3.3.8 Integrity and Confidentiality

Appropriate technical and organisational measures must be implemented to ensure a level of security appropriate to the volume and format of the data, its sensitivity and associated risks. A Consultant must consider appropriate measures to protect personal data they process. A regular information security audit will ensure that appropriate measures are in place to secure personal data that is held. An audit should address both technical and organisational aspects of information security. The audit results and the resulting actions to address any issues identified should be maintained in the data protection accountability log (see Section 3.3.9, Section 3.5, Action Point 7 and Action Point 12 below).

3.3.9 Accountability

To demonstrate one's compliance and accountability under GDPR, there is a requirement to keep certain records. These include:

- Regular Information Security Audits (See Action Point 12)
- Records of Processing Activities (See Action Point 2)
- Staff Training and Awareness Records (See Section 3.3.10)
- Confidentiality Agreements with your staff (See Action Point 9)
- Agreements with Practice Software Vendors and any other Processors (See Action Point 3)
- Where processing on basis of consent, records of consent (See Action Point 6)

The Irish Data Protection Act 2018 is now enacted and Consultants who are Data Controllers are no longer required to register with the Data Protection Commission. [18] While the principle of accountability has previously been an implicit requirement of data protection law, it is now mandatory. The onus is on Data Controllers to demonstrate all aspects of their compliance to fulfil their accountability requirements. The

[18] The requirement that existed under the previous legislative regime for organisations to register their data processing activities with the DPC no longer applies under GDPR. Accordingly, as of 25th May 2018 organisations are no longer obliged to submit an application for registration of their data processing activities to the DPC and pay the applicable fee. Also, GDPR removes the requirement for the DPC to maintain a public register of such processing activities.

records listed above will assist you but you should consider whether any additional action or documentation is required having specific regard to the circumstances of your practice.

Consultants engaged in private practice should display information on data protection regulations in their waiting room (see Action Point 5 above). Consultants should also nominate themselves or a named individual to carry out a data protection role, to answer any data protection queries and process Subject Access Requests. (see Section 3.4.1 below).

ACTION POINT 7: Review and complete the template *Data Protection Accountability Log* included in Appendix G. The log should be updated periodically.

3.3.10 Data Protection and Cyber Security Awareness and Training Details

All Consultants 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.

ACTION POINT 8: Circulate this Guideline document to all staff having particular regard to the *IT Guidance Document* as included in Appendix J. Ensure that all staff are familiar with and adhere to this Guideline.

3.3.11 Employee / Office Workers Confidentiality Agreements

Support staff, such as managers, secretaries, receptionists and any associated health professionals must sign confidentiality agreements as part of their contract of employment. Keep records of staff joining or leaving employment. Any staff who cease their employment should have all access removed including remote access privileges. Change passwords and access cards as appropriate. Also make sure that access to local and online applications and services (Office 365, Google, Dropbox, etc.) and backup services are restricted.

ACTION POINT 9: Ensure that all relevant personnel who may have access to areas or systems where personal data is stored enter into a *Confidentiality Agreement* using the template included in Appendix H.

3.4 Ensure that you are compliant with Individual Rights

Patients have certain rights with regard to their personal data and you should implement procedures to support those rights as outlined below.

3.4.1 Right of Access

GDPR gives all patients the right to access their medical records. A Consultant must provide a copy of the patient's medical record and personal data on receipt of a written request. The request (or authorisation form) to satisfy these individual rights should be in writing and should be signed by the patient or legal guardian as appropriate. Requests can also be accepted via email where it has previously been verified that the email address belongs to the patient concerned. The simplest way to verify an email address is to call your patient on their verified phone number. You should verify the identity of a patient making an access request to ensure the personal data is only provided to him or her. The requested records should be provided to the patient 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. However, Consultants should note the following guidance regarding costs from the Data Protection Commission:

> *"where requests from a data subject are considered 'manifestly unfounded or excessive' (for example where an individual continues to make unnecessary repeat requests or the problems associated with identifying one individual from a collection of data are too great) the data controller may:*
>
> 1. *Charge a reasonable fee, taking into account the administrative costs of providing the information/ taking the action requested; or*
> 2. *Refuse to act on [the] request.*
>
> *In cases where this is used as a reason to refuse an access request or to charge a fee, it is up to the organisation to prove why they believe the request is manifestly unfounded or excessive."*[19]

The right of access is one of the most important data protection rights because it allows individuals to find out whether their personal data is being held and to obtain a copy of their personal data. Like all other data protection rights, the GDPR does not say when, or in what circumstances, a parent or guardian can make an access request for their child's personal data, or when or in what circumstances a child can make their own access request.

It is worth noting that once a child is capable of understanding their rights to privacy and data protection, then 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. A Consultant who receives a request from a legal guardian should be satisfied that the person is genuinely acting on behalf, and in the best interests, of the child whose data has been requested.

Disclosing to another third party the medical information of a child who is capable of making decisions themselves will in most situations constitute a data protection breach if conducted without the consent of the child.

The right to access may be restricted if the disclosure of the data to the patient would be likely to cause serious harm to his or her physical or mental health.[20] In any situation where access is denied, the Consultant must advise the patient of the reason, either at the time access is denied or as soon as practicable 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. The patient has a right to appeal the restriction or refusal as the case may be to the Data Protection Commission.

With regard to requests by An Garda Síochána or a law enforcement agency for access to personal data from records in relation to the prevention, detection or prosecution of offences, any such requests should:

- Be made in writing (this includes email) with some detail provided in relation to the data required.
- Confirm the purpose or reason for which it is required.
- The Gardaí or law enforcement agency should quote relevant legislation which might apply to their request for data.
- The request for data should be signed by a person at a suitably senior level.

---

[19] https://www.dataprotection.ie/en/individuals/know-your-rights/what-will-it-cost

[20] Section 54 of the Data Protection Bill 2018

Subject Access Requests should be complied with without undue delay and within one month of receipt of the request. Where reasonable additional information is required to substantiate the request, the time frame for responding runs from receipt of the additional information. That period may be extended by a further two months where necessary, taking into account the complexity and number of the requests. The designated contact shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

Finally, where a Consultant who is a data controller receives a subject access request, he or she can comply with that request only insofar as it relates to data that the Consultant has in his or her custody. Where the request also relates to data that is held by another data controller, e.g. a public or private hospital, then the data subject should be informed that a separate access request is required to be submitted to that other data controller.

ACTION POINT 10: An outline process for dealing with Subject Access Requests is included in Appendix I. The template should be adapted according to your practice.

3.4.2 Right to Rectification

Your patients have the right to request that their data is rectified if it is inaccurate or incomplete. You must respond within one month in this regard although a longer period of two months is allowed if the request is complex. If the request is declined, you must provide an explanation to the individual, informing them of their right to complain to the Data Protection Commission and potentially to a judicial remedy. Under GDPR, the patient has the right to obtain rectification of inaccurate personal data which is factually inaccurate. However, this is not an unqualified right and depends on the circumstances of each case.[21] Your records should reflect any disputes, for example in the event of a patient disagreeing with a diagnosis. A note reflecting this can be added to their record. See also Section 3.3.7.

3.4.3 Right to Erasure

GDPR gives Data Subjects the right to request the deletion of personal data. However, the Consultant has an obligation under Medical Council rules to maintain medical records[22]. In addition, a Consultant is entitled to retain records for medicolegal purposes, for example in the context of raising a defence to a clinical negligence claim or proceedings that might subsequently arise. The right to erasure of medical records is not absolute and restrictions may apply.[23] Requests for erasure should be dealt with on a case-by-case basis.

3.4.4 Right to Restriction of Processing

In certain circumstances, a patient may request the Consultant to restrict processing either permanently or temporarily. This could be requested by a patient where:

- accuracy is contested, pending resolution;
- where a patient objects to processing, pending verification of legitimate grounds;

---

[21] Irish Data Protection Commissioner case study 1 of 2007

[22] Section 33 of Guide to Professional Conduct and Ethics for Registered Medical Practitioners, 8th Edition 2016 available at: https://www.medicalcouncil.ie/News-and-Publications/Reports/Guide-to-Professional-Conduct-and-Ethics-8th-Edition-2016-.pdf

[23] Article 23.1(g) of GDPR

- where the Consultant no longer needs the data, but the data is required to be maintained for legal reasons;
- where processing is unlawful but the patient opposes erasure.

Where a patient is in a disagreement or dispute with a Consultant, they may request that their medical records are marked restricted for processing. The patient must be informed of implications for his or her medical care and treatment while medical records are assigned with 'restricted processing' status. Restriction of processing requests from patients must be in writing and signed.

3.4.5 Right to Data Portability

The right to data portability arises when a patient moves from one healthcare provider to another. On request, the patient should be provided with a copy of their medical records in a transferable format that allows them to transmit the data to another Consultant or doctor. This should be facilitated using electronic or other standard messaging formats.

You should ensure that appropriate signed consent forms are obtained from the patient authorising the transfer. The records should be transferred securely by using security features such as encryption. For example, if you use Gmail (these features can be enabled in most web-based mail services):

1. Compose a message.
2. Add recipients to the "To" field.
3. To the right of your recipients, you will see a lock icon that shows the level of encryption that is supported by your message's recipients. If there are multiple users with various encryption levels, the icon will show the lowest encryption status.
4. To change your S/MIME (Secure/Multipurpose Internet Mail Extensions) settings or learn more about your recipient's level of encryption, click the lock, then view details.

3.4.6 Right to Object

Individuals can object to the processing of their data, for example, in relation to direct marketing, profiling, scientific and historical research.

3.4.7 Automated Individual Decision-making, Including Profiling

Profiling is any form of automated processing of personal data to evaluate certain personal aspects relating to an individual. This is not permitted under GDPR, but it is unlikely to arise in a healthcare setting.

ACTION POINT 11: Appendix I includes a template policy for Subject Access Requests and how you deal with rectification, erasure, restrictions on processing and data portability. The template should be adapted according to your practice.

3.5 ADOPT APPROPRIATE SECURITY MEASURES

It is beyond the scope of this document to provide comprehensive guidance with regard to IT systems and IT security generally. If you have concerns in this regard you should seek advice from your service provider.[24]

[24] In this Guideline, references to Information Technology (IT) Systems should also be taken to mean Information and Communications Technology (ICT) Systems

A key principle of the GDPR is that you process personal data securely by means of 'appropriate technical and organisational measures'. This is referred to as the 'security principle'.

This means that you must have appropriate security measures to prevent the personal data you hold being accidentally or deliberately compromised. You should remember that information security extends beyond cybersecurity (the protection of your networks and information systems from attack). It also covers other issues like physical and organisational security measures.

Simple, common sense security practices can go a long way towards ensuring that the data you process is stored, maintained and transferred in a secure manner. These are outlined in Appendix J.

The security principle goes beyond the way you store or transmit information. Every aspect of your processing of personal data is covered, not just cybersecurity. This means the security measures you put in place should seek to ensure that:

- the data can be accessed, altered, disclosed or deleted only by individuals authorised by you and that those individuals only act within the scope of the authority you give them.
- the data you hold is accurate and complete in relation to the purpose for which you are processing it.
- the data remains accessible and usable, i.e. if personal data is accidentally lost, altered or destroyed, you should be able to recover it and therefore prevent any damage or distress to the individuals concerned.

These are known as "confidentiality, integrity and accountability" under the GDPR and they form part of your obligations.

Before deciding what measures are appropriate, you need to assess your information risk. You should review the personal data you hold and the way you use it in order to assess how valuable, sensitive or confidential it is – as well as the damage or distress that may be caused if the data was compromised. You should also take account of factors such as:

- The nature and extent of your premises and computer systems;
- The number of staff you have, if any, and the extent of their access to personal data; and
- Any personal data held or used by a data processor acting on your behalf.

As a minimum, for compliance purposes you must commission regular IT security audits to ensure that appropriate measures are in place to secure personal 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

In the event that you or any of your staff need to have access to data at home, or transport it in your car, the same precautions should be taken. If you or your staff are accessing data at home on your own device, appropriate Malware and Anti-Virus software should be installed and if using a private Gmail or other email address, the appropriate common sense measures outlined above should also be used. It is advisable to

implement a Bring Your Own Device (BYOD) Policy in these circumstances. A BYOD policy template is included in Appendix J.

ACTION POINT 12: Review the IT guidance document included in Appendix J. If you have specific concerns regarding the security and integrity of your IT systems, seek advice and commission a regular information security audit from your IT provider or an appropriately qualified service provider.

3.6 ADOPT A POLICY ON DATA BREACH HANDLING

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It may be accidental or deliberate.

Data breaches can be categorised as follows:

- **Confidentiality breach** – unauthorised or accidental disclosure of, or access to, personal data;
- **Integrity Breach** – where there is an unauthorised or accidental *alteration* of personal data;
- **Availability breach** – where there is an accidental or unauthorised *loss* of access to, or *destruction* of, personal data.

Under the GDPR, breach notification is mandatory where there has been a data breach that is likely to "*result in a risk to the rights and freedoms of individuals*". The GDPR does not lay down a specific threshold as to when a breach causes a "high risk" to individuals and their rights, but it is important to understand what constitutes a breach.

Examples include:

- Computers or devices holding personal data being lost or stolen
- Documents or files lost or stolen
- Fire or flooding resulting in destruction of information or data loss
- Inappropriate access controls allowing unauthorised use
- Cyber-attack, ransomware
- Obtaining information by deception, for example a Subject Access Request with unconfirmed identity
- Incorrectly addressed emails, other human errors (reports sent to wrong recipients)
- Access by an unauthorised third party
- Sending personal data to an incorrect recipient
- Alteration of personal data without permission of the Data Controller

As outlined above, breaches also include the accidental loss of personal data, for example a fire on one's premises that results in the loss of hard copy paper files. Most breaches are internal in nature and often arise from non-malicious user behaviour, for example, the loss of an unencrypted laptop or USB stick, etc. Breaches can also occur by not correctly verifying the identity of patients in communications. Training and awareness of staff is an important element in preventing such data breaches.

In the event of a data breach, you will need to:

- Notify the Data Protection Commission
- Notify the Data Subject

The processes you should follow to notify the Data Protection Commission and Data Subject are outlined in Appendix K, together with examples of Personal Data Breaches and your obligations as a Controller.

ACTION POINT 13: Review the template *Data Breach Response Plan* in Appendix K and adapt it according to your practice.

4 DATA PROCESSOR OBLIGATIONS

Under GDPR a 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of a controller. A Consultant acting as a Data Processor has specific obligations under GDPR. The Data Protection Acts 1998 to 2018 contain provisions that a written contract should be entered into between Controllers and Processors when processing of personal data is carried out by a Processor on the instruction of a Controller. Similarly, the GDPR requires that when a Controller engages a Processor to process personal data on its behalf, the Controller and Processor must enter into a legally binding contract governing this processing of personal data (see Section 3.1.1 above). The following list highlights the main responsibilities of a Processor that you need to be aware of:

- You must have adequate information security in place (See Section 3.5 and Action Point 12)
- You should not engage sub-processors without the prior consent of the Controller (See Section 3.1.1 and Action Point 3)
- You must cooperate with the authorities in the event of an inquiry
- You must report data breaches to the Controller as soon as you become aware of them, without undue delay (See Section 3.6 and Action Point 13)
- You must give the Controller the opportunity to carry out audits examining your GDPR compliance
- You must keep records of all processing activities (See Section 3.1 and Action Point 3)
- You must comply with EU cross border data transfer rules (if applicable)
- You must help the Controller to comply with data subjects' rights (including the processing of data subject requests) (See Section 3.4.1 and Action Point 10)
- You must assist the Controller in managing the consequences of data breaches (See Section 3.6 and Action Point 13)
- You must delete or return all personal data at the end of the contract at the choice of the Controller, and
- You must inform the Controller if the processing instructions infringe GDPR

5 DATA PROTECTION IMPACT ASSESSMENTS AND THE ROLE OF DATA PROTECTION OFFICER

5.1 DATA PROTECTION IMPACT ASSESSMENTS (DPIAS)

A Data Protection Impact Assessment (DPIA) is a process that helps identify risks to the privacy of data subjects and ensure that best practice is followed when a new project or service is planned, or when changes are made to an already existing product or service. A DPIA serves to ensure that privacy related risks that arise during data collection, use and disclosure are mitigated using appropriate plans and measures, while allowing the objectives, outputs or deliverables of a project which involves the use of personal data to be met.

A privacy risk can be defined as the probability that the fundamental rights and freedom of a data subject may be put at risk through one's data processing activities. Recital 4 of the GDPR defines the fundamental rights of a data subject as:

- respect for private and family life
- respect for home and communications
- protection of personal data
- freedom of thought, conscience and religion
- freedom of expression and information

Privacy related risks can include one or all of the following:

- Risks to patients, research participants, staff or other third parties, for example ill-use or overuse of research participant data, loss of anonymity, intrusion into privacy through monitoring activities, lack of transparency, lack of fairness and lawfulness of data processing activities, etc.
- Compliance risks, for example breach of the GDPR or other health related legislation including the Health Research Regulations 2018.[25]
- Inherent or residual risks to your practice, for example project failure and associated costs, legal penalties or claims, damage to the Consultant's reputation, loss of trust of patients or the public.

The carrying out of a DPIA is <u>only</u> mandatory where a processing is "*likely to result in a high risk to the rights and freedoms of natural persons*".[26] It is particularly relevant when a new data processing technology is being introduced. In cases where it is not clear whether a DPIA is required, the Article 29 Data Protection Working Party ('WP29') recommends that a DPIA is carried out nonetheless as a DPIA is a useful tool to help data controllers comply with data protection law.

A Consultant carrying out normal medical care for his or her patients and using an established and accredited medical practice software management system is <u>not</u> required to carry out a DPIA. The processing of personal data by an individual Consultant or group practice would not generally be considered to constitute large-scale processing. In summary, DPIAs are a useful tool and are recommended, but they are not mandatory.

[25] Data Protection Act 2018 (Section 36(2)) (Health Research) Regulations 2018, available at: http://www.irishstatutebook.ie/eli/2018/si/314/made/en/pdf

[26] Article 35(1) of GDPR

5.2 DATA PROTECTION OFFICER (DPO)

Under the GDPR, a Data Protection Officer must be appointed where one of the following criteria applies:

- where the organisation processes data in a manner which requires "*regular and systematic monitoring of Data Subjects on a large scale*". Note that 'large scale is not defined.
- where the data processing activities "*consist of processing on a large scale of special categories of data*"; or
- where the organisation is a public body or has statutory authority, or processes personal data on behalf of such an organisation.

The processing of personal data by an individual Consultant or group practice would therefore not generally be considered to warrant or require the appointment of a DPO. However, you should identify and nominate a named individual to act as a Data Protection lead for the purpose of co-ordinating your data protection arrangements.

6 FREQUENTLY ASKED QUESTIONS

1. **Is it acceptable to communicate with patients using text message or voicemail and what information can be included in such messages?**

While it is not recommended to send sensitive personal data via text message, sending appointment reminders via SMS text is permitted as long as you have consent to do so. You can include the patient's name, the hospital department or location of clinic, the appointment date and time, but you should also include an opt-out in every text message. 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.

The subject matter of the conversation with your patients may dictate what type of voicemail if any you should leave if you do not get through to them. As a general rule, voice messages should only be left on the patient's personal phone and not on an office or work phone. Leaving your contact details and a request for the patient to call you back is a prudent approach to take.

2. **Can Consultants use personal email addresses when sending personal data, e.g. Gmail, Yahoo, G Suite or equivalent email providers? Can they email personal data to patients' own Gmail (or other unsecure server) addresses? Can Consultants use their own personal websites to communicate with patients and transfer personal data?**

If a Consultant is using an email address that does not support encryption, e.g. Gmail, any sensitive data should be sent in a password protected document. This is best practice when sending any documents containing sensitive personal data. You should not send the document password by email, but rather use an alternative delivery method, e.g. via text message. Make sure you record the patent's consent allowing you to contact them via email.

It is not recommended to use personal websites to transfer personal data due to security concerns, although if this is absolutely necessary then the appropriate technical safeguards must be in place to ensure that personal data is processed in a secure manner.

If another doctor requests you to send data or images in an unsecure manner prior to accepting referral, you should inform them that all personal data must be processed in a secure manner to comply with GDPR.

3. **Is it acceptable to use fax or electronic fax to transmit patients' personal data?**

The use of fax machines is not recommended and does not represent best practice due to security concerns around unauthorised disclosure of personal data. If the use of a fax machine is unavoidable, then appropriate data protection safeguards must be in place. These should include: ensuring that the fax number is correct; confirming that transmission is received; placing the fax machine in an area not accessible to the public; and making sure only those authorised to access faxed documents have physical access to the machine.

Best practice also requires a notice placed in close proximity to the fax machine which details the procedures for sending transmissions in a safe manner, and the procedures to follow in the event of a fax being sent to an unintended recipient. If required, a Controller/Processor agreement should be in place to ensure that the recipient of the facsimile handles transmissions in accordance with appropriate data handling procedures. 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, with suggested wording 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.*"

Many eFax servers are located outside the European Economic Area, for example, in the US, and as there is a general prohibition on transfers of personal data outside the EU, their use may be in breach of the GDPR.

4. **Is it acceptable to send sensitive information or data to patients by post?**

When sending sensitive personal data via the postal service, all post should be registered to ensure secure delivery and traceability. You must also use an accurate postal address that has been verified and confirmed by the patient.

5. **Is it acceptable to use WhatsApp or similar messaging apps to send patient data to colleagues?**

Consultants should not use WhatsApp or other messaging apps to transmit personal data as this could lead to the disclosure of sensitive personal data into the public domain. It is understood that the HSE is considering tendering for the provision of a messaging service for staff that would be fully encrypted end-to-end and where messages would not be readable by anyone, including the vendor of the application. You should make local enquiries with hospital management to determine if this facility is available.

In particular WhatsApp should not be used to send special category health data. Even though there is end to end encryption of WhatsApp messaging, all messages are backed up on servers which are potentially not secure. If you are sharing information over WhatsApp you are likely doing so from a personal handheld device which could be easily lost or stolen.

6. **Is it acceptable to transfer information from a Consultant's mobile device to a colleague's mobile device in circumstances where existing hospital infrastructure does not support timely transfer of patient information?**

Storing or transferring personal data using a mobile device is not recommended due to the security risks involved. It is important to be extremely vigilant with mobile devices. While not recommended, if it is absolutely necessary to transfer information to avoid compromising a patient's care, then it should be conveyed only using devices that are secured using passwords and encryption. Any patient related personal data should be deleted subsequently.

7. **If MDT requests to other hospitals within the hospital group are conveyed by sending messages to other colleagues and submitting consultation requests via phone messages, should I use a HSE or hospital phone instead of a personal phone?**

Please refer to the response to question 6 above. It is also important to note that regardless of the ownership of the phone, best practice as outlined above should be followed.

8. **What special measures are required regarding a Consultant's relationship with health insurers?**

Please refer to Section 3.1.3 in the main Guideline

Any personal data sent to Medserv or similar billing agent for billing purposes should be encrypted and password protected. Again, passwords should not be sent via email to the same recipient, but rather sent by text message or via a phone call.

9. Are Consultants Data Processors or Data Controllers?

The GDPR applies to 'Controllers' and 'Processors' of data. Data Controllers determine the purposes and means of processing personal data. Data Processors process data on behalf of a Data Controller. Please refer to Section 2.2 for detailed guidance.

10. What should I do if a patient wants to exercise his or her right to have information erased or corrected?

Consultants who are Data Controllers must ensure that there is a data subject request procedure in place to deal with requests from patients to correct or erase personal data (see Appendix I). All access requests from patients must also follow this same procedure. If a patient seeks a correction to their personal data, the personal data must be updated in line with procedures outlined in the policy and this must be documented. See Section 3.4 in the Guideline and Appendix I.

While patients now have a right to erasure, this is not an absolute right as Consultants have an ethical and legal duty to keep medical records for varying lengths of time. This time frame must be identified before any medical data can be erased and should be included as part of a documented procedure for a data erasure request. There are also legal requirements to keep details of personal medical records for a specified time frame (see Section 3.2) which would supersede the request from the data subject to erase the data.

11. Is it appropriate for secretarial and administrative staff to have access to patient records?

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 your practice. In that regard, patients should understand that staff may have access to their records for: typing referral letters to other hospital consultants or allied health professionals; opening letters from hospitals and other consultants; scanning clinical letters, diagnostic reports and any other documents not available in electronic format; downloading laboratory results; photocopying or printing documents for further referral; handling, printing, photocopying and posting of medico-legal reports, and of associated documents; sending and receiving information via secure email; and other activities related to the support of medical care appropriate for practice support staff.

All such staff, 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. See Section 3.3.11 in the Guideline and Appendix H.

Practice Software Management systems should provide an audit log of when patient information has been accessed, and by whom. Such an audit log makes it possible to detect any unauthorised access to personal health information.

12. What physical or technical measures should I take to ensure the security of my patients' sensitive personal data?

Consideration should be given to the need for speech privacy at any front desk or reception area where patients are required to register or check in. When planning the location of new consultation areas where sensitive personal data will be discussed and disclosed, it may be advisable that a Data Protection Impact Assessment (DPIA) is undertaken which should include facilitating the privacy of the data subject and to mitigate the risk of personal data being overheard by unauthorised persons or the public.

If you are physically carrying charts between locations, ensure that there is a tracking system in place to show where a chart is at any given time, and who has control of the chart. Barcode scanning software is an option to track paper records while in transit.

Do not leave the chart unattended in any area where there is a risk of access to the chart by unauthorised personnel.

It is not recommended to leave sensitive personal records unattended in a car or in any public area. Files should be placed in a securely locked carrying case, out of sight while in a vehicle.

If any patient files are kept at home, consider using a fire-resistant safe or securely locked, structurally sound cabinet as a minimum.

If certain non-medical staff have access to areas where patient records are stored (e.g. students, IT support staff, cleaners, etc.) you should take precautions to ensure that patient information is protected from unintended or unauthorised use. In the circumstances mentioned above, it is reasonable to ask those individuals to sign a confidentiality agreement (see Section 3.3.11 in the Guideline and Appendix H).

The use of encryption software is best practice in order to ensure that personal data stored electronically is secure. General security software packages such as Norton or McAfee are sufficient to provide anti-virus protection to your PCs, but they may not cover other threats such as password stealers, rootkits or other forms of malware. If you have concerns in this area you should seek the advice of your IT provider.

If you need to access patient information remotely, use a Virtual Private Network (VPN) to protect from unauthorised snooping or interference. Using a VPN will allow you to browse freely from Wi-Fi hotspots with the reassurance of knowing that you cannot be tracked or monitored.

Refer to Appendix J for more detailed guidance on good IT practice.

13. What do I need to consider to ensure the secure storage of personal data under my control?

A Consultant who is a Data Controller is responsible for ensuring the safe storage of personal data under his or her control. Remember, the GDPR covers paper records as well as electronic health data, so the principles of data security should apply equally to paper records as to personal medical data in a digital format. If you have hard copy files stored in a commercial warehousing or storage facility, a Controller/Processor agreement compliant with GDPR regulation must be in place to ensure the Processor implements technical and organisational measures to ensure the confidentiality and integrity of the personal data.

It is not recommended to use Dropbox or similar cloud storage providers for storing sensitive data. However, if this is unavoidable, documents must be password protected. Any memory sticks used must also be encrypted as a security precaution.

If you are considering keeping an Excel spreadsheet on a hospital server with private patient details, you should keep this file on an encrypted drive, or password protect the document as a minimum precaution. You should also ensure that backup images of the server data are also encrypted.

If you are disposing of medical records or personal data that is held in hard copy format, secure shredding can be implemented in-house, but can also be carried out by a third party certified vendor.

14. Is it acceptable to store data with iMedDoc and Medserv?

Yes. iMedDoc vendors are certified to ISO27001:2013 and have adequate privacy in place that ensures integrity and confidentiality of information. It is understood that Medserv have been audited by the Data Protection Commission and by PricewaterhouseCoopers and also have appropriate controls.

15. Do the new regulations apply to my hard copy medical files?

The GDPR covers hard copy paper records as well as electronic health data, so the principles of data security apply equally to paper records as to personal data in a digital format.

16. What arrangements should I have in place for patients' photographic images, e.g. skin conditions, scarring, etc.?

Medical photographs should only be taken using an office camera designated for that purpose. The camera should be stored in a secure locked cabinet. Photographs should not be taken on a mobile phone where there is a risk that the device could be lost or stolen. All images should be stored securely.

17. Do I have to erase or destroy my private patient data billing information after a certain period?

Private patient billing data should be retained for seven years as per Revenue requirements.

18. What is best practice for handling historical patient data in terms of retention, deletion, and length of time records should be kept? Do you need a private company to destroy records?

There may be legal requirements to retain personal data for patients for specified periods and the period may be different for different categories of data. See Section 3.2.

Although not necessary, best practice is to have record deletion carried out by a professional vendor.

19. Are there specific requirements regarding transmitting information, such as digital dictation files, by email, backup storage or on home PC, and to third party companies?

Data such as digital dictation files should be transmitted on an encrypted channel and saved on an encrypted storage device. They should also be password protected while in transit. Any personal data stored on home devices must conform to the same technical and organisational measures that are in place for all workplace technologies. See Appendix J which includes a template *Bring Your Own Device* (BYOD) policy.

20. Does GDPR restrict the ability of one hospital to transfer personal data to another hospital that is providing care to the same patient?

No, GDPR does not prevent this transfer if the processing is necessary for "*medical diagnosis, the provision of health or social care or treatment*".

21. If a solicitor acting for a patient sends a letter to a Consultant, with patient consent attached, requesting the entire patient record including third party correspondence, is it appropriate to comply with this request?

Under Data Protection legislation the patient has an entitlement to this information. However, before releasing to the patient's solicitor, you should confirm with the patient that they 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. It may also be appropriate to redact personal data that relates to or identifies a third party but provide the data subject with a summary of the personal data that, insofar as possible, permits the data subject to exercise his or her access rights without revealing the identity of the third party.

22. Is it acceptable to supply further information or documentation on request to a private health insurer regarding a patient's treatment?

See Section 3.1.3 in the Guideline.

23. Are there specific requirements in respect of reporting data outside of the country for example to the British Paediatric Surveillance Unit or National Study of HIV in Pregnancy and Childhood in UK?

EU data protection rules apply to the European Economic Area (EEA), which includes all EU countries and non-EU countries Iceland, Liechtenstein and Norway, along with a third country that may also be declared as offering an adequate level of protection. A transfer can take place outside the EU through the provision of appropriate safeguards and on condition that enforceable rights and effective legal remedies are available for individuals, such as binding corporate rules, contractual arrangements with the recipient of the personal data, adherence to a code of conduct or certification mechanism together with obtaining binding and enforceable commitments from the recipient to apply the appropriate safeguards to protect the transferred data. The above applies when using a provider from outside the EU, e.g. ProtonMail encryption system.

This advice will be updated in the event that the United Kingdom leaves the European Union and assumes third country status.

24. How should patients be informed about GDPR?

In general, patients should be informed about GDPR via notices at the usual contact points where personal data is collected, for example at reception, in waiting rooms, in website policy notices, or in emails where necessary and appropriate. See Section 3.3.1 in the Guideline and Appendices D and E.

25. Is there a short guide on GDPR available for staff with a declaration for them to sign to indicate that they are aware of the requirements?

The Data Protection Commission website (www.dataprotection.ie) has a range of guidance and information resources that will assist in the task of educating staff on the requirements under the new regulations.

Staff should sign a confidentiality agreement with you as the Data Controller outlining their duties and responsibilities in relation to the handling of personal data. How you deal with possible data breaches will also have to be documented and be available for inspection, along with other practice policies and

procedures. A bespoke staff declaration form should be drafted according to the needs of your practice. Please refer to Section 3.3.11 in the Guideline and Appendix H in this regard.

If staff or secretaries are working from home, a policy should exist for users working remotely. On a technical level, all devices, laptops, USB drives, phones etc. should be encrypted, and appropriate anti-virus, anti-malware programs installed. A secure Virtual Private Network (VPN) should also be utilised to connect to an organisation's network for transfer of personal data. See Appendix J for more detailed guidance.

26. What is required to ensure GDPR compliant contracts with third-party vendors? Will my dictation or cloud back-up services be affected by GDPR?

See Section 3.1.1 in the Guideline and Appendices B and C. At a minimum, the following is required to be stated to ensure GDPR-compliant contracts with third parties:

- The Controller organisation name, address, contact name
- Vendor organisation, address, contact name
- The obligations and rights of the controller
- The subject matter of the processing
- The duration of the processing
- The nature of the processing
- The purpose of the processing
- The type of personal data processed
- The categories of data subject
- The details of any risk mitigation measures.

Contracts with all third-party providers, for example, dictation service providers, billing agencies, software providers, back-up cloud storage, etc. should be reviewed so that they comply with GDPR. This has to be documented to ensure compliance. Contracts of this nature should also include arrangements to deal with circumstances where there is a change of provider or a party to the agreement ceases practice or closes down.

27. Do I need to check anything else with my practice software provider?

Apart from reviewing your agreement with your software provider to ensure GDPR compliance, practice management software systems should have the capacity to provide a log of when patient information has been accessed and by whom.

28. Do I need to employ a Data Protection Officer?

Consultants generally will not require the services of a Data Protection Officer as the GDPR only requires this where there is large scale processing of data.

APPENDICES

Note: All Appendices are available and have been circulated separately in MS Word format so that you can amend and adapt them as necessary.

APPENDIX A: TEMPLATE FOR RECORDS OF PROCESSING ACTIVITY

Consultant or Group Practice Name	
Consultant or Group Practice Address	
Telephone Number	
Data Controller	
Lead for Data Protection	

The following Table applies in respect of Private Patients and shows the categories of personal data that we process.

[Note: The data elements listed below should be amended, deleted or expanded according to your practice.]

Category of Personal Data	**Purpose of Processing**	**Lawfulness of Processing**	**Retention Period**
Administrative: • Name • Address • Contact details (phone, mobile, email) • Dates of appointment	Necessary to support the administration of patient care.	Article 6(1)(b) provides a legal basis for processing where "*processing is necessary for the performance of a contract to which the data subject is party …*"	Linked to financial records, retention as per Revenue requirements. Revenue requires individuals/organisations to retain financial records for 7 years.
Medical Record: • Individual health identifier • GMS number • 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	Necessary to provide patient care.	Article 9(2)(h) applies where 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*	For adults: 8 years after last contact, unless in the interest of the Data Subject to retain. For Children (under 18 years of age): Retain until the patient's 25th birthday or 26th if young person was 17 at the conclusion of treatment, or 8 years after death. If the illness or death could have potential relevance to adult conditions or have genetic implications, consider whether it is appropriate to retain the records for a longer period. Deceased Persons: 8 years after death.

• Allergy details • Current and past medical and surgical history • Genetic data • Laboratory test results • Imaging • Imaging test results • Photographs • Near patient test results • ECGs • Ultrasound scan images • Other data required to provide medical care		*law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;"*	Maternity: 25 years after birth of last child.
Account Details: • Record of billable services provided • Patient name • Address • Contact details • Billing and payment records for private patients • Private Health Insurance details	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 securing payment for providing a service to private patients.	Revenue requires organisations to retain financial records for 7 years. The retention period for financial records is provided for in the Companies Act 2014. In particular, Chapter 2, Accounting Records, comprises the following Sections: 281. Obligation to keep adequate accounting records 282. Basic requirements for accounting records 283. Where accounting records are to be kept 284. Access to accounting records 285. Retention of accounting records 286. Accounting records: offences Specifically Section 285 states "An accounting record required to be kept by section 281 or information or a return referred to in section 283 (2) shall be preserved by the company concerned for a period of at least 6 years after the end of the financial year containing the latest date to which the record, information or return relates."

Categories of Transferors and Recipients involved in sharing of personal data

[Note: The parties listed below should be amended, deleted or expanded according to your practice.]

Categories of Transferors and Recipients	**Description**
Healthcare Providers, Social Care Providers	Other Consultants, General Practitioners, Public Hospitals, Private Hospitals and Clinics, Health Service Executive, Occupational Therapists, Occupational Health Physicians, Opticians, Palliative Care Services, Pharmacies, Psychologists, Physiotherapists, Speech and Language Therapists, Social Workers, Nursing Homes, Counselling Services, Diagnostic Imaging Services, Hospital Laboratories, Practice Support Staff, GP Locums, Acute Hospital and Community Services clinical staff, Prison Service clinical staff, Mental Health Commission, and other healthcare providers.
Data Processors (contractual)	Practice Software Vendors, Online Data Backup Companies, Practice Management Services, Debt Collection Agencies, Dictation Service Providers
Legal Proceedings or Legal Affairs	Coroner, HIQA, Medical Council, Medical Indemnifier/Insurer, Revenue Commissioners, Social Protection, Tusla, Solicitors in Regulatory Bodies in relation to legal cases, Office of Ward of Courts regarding capacity cases, Gardaí or authorised offices in relation to Mental Health legislation.
Public Health Entities	Infectious disease notifications, influenza surveillance, National Cancer Registry and other National Registries, International Databases for benchmarking patient outcomes.
Third Parties (under explicit patient consent)	Health Insurance Companies, Solicitors, Banks, Insurance Companies, etc.

We/I have implemented appropriate technical and organisational measures to ensure, and can demonstrate, that processing is performed in accordance with GDPR. These measures will be reviewed and updated where necessary.

APPENDIX B: TEMPLATE AGREEMENT BETWEEN DATA CONTROLLER AND DATA PROCESSOR

Agreement between Data Controller and Data Processor

Agreement between:

[Name, Registered Office]

(hereinafter referred to the as 'the Controller')

and

[Name, Registered Office]

(hereinafter referred to the as 'the Processor')

This agreement may operate as an agreement in its own right or as an Addendum to any existing contract. Its details and terms are determined by the General Data Protection Regulation. For definitions, refer to the GDPR text.

1. Compulsory details: (Amend as appropriate)

These details are required to protect against the possibility of changes being made to the scope of the processing over time, without taking into account any additional risks this poses to the Data Subjects.

1.1 State the Subject Matter of the processing: e.g. patients' personal data
1.2 State the Duration of the processing: e.g. Monthly via Contract Terms
1.3 State the Nature of the processing: e.g. Data Entry
1.4 State the Purpose of the processing: e.g. Dictation Services
1.5 State the Type of personal data: e.g. Patient name, policy no.
1.6 State the Categories of Data Subject: e.g. Patients
1.7 State the procedure in accordance with which a party may withdraw from the agreement, either by business closure, retirement, or termination for convenience.
1.8 State the requirements in relation to the retention of (i) the information to be disclosed, and (ii) the information resulting from the processing of that information, for the duration of the agreement and in the event that the agreement is terminated for any of the reasons specified in 1.7 above.

2. The obligations and rights of the Controller.

2.1 The Controller of the personal data must comply with the GDPR and must therefore require the Processor to recognise and agree to the Compulsory Terms. The Controller has the responsibility to ensure that the Processor is competent to process the personal data in accordance with all the requirements of the GDPR.

3. Compulsory Terms required by GDPR

3.1 The Processor must only act on the written instructions of the Controller (Article 29, unless required by law to act without such instructions);
3.2 The Processor must ensure that employees processing the data are subject to a duty of confidentiality;
3.3 The Processor must take appropriate measures to ensure the security of processing in accordance with Article 32;

3.4 The Processor maintains records of its processing activities in accordance with Article 30.2;
3.5 The Processor must only engage a Sub-processor with the prior consent of the Controller and subject to a written contract (Article 28.2);
3.6 The Processor must assist the Controller in providing subject access and allowing Data Subjects to exercise their rights under the GDPR;
3.7 The Processor must assist the Controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
3.8 The Processor must notify any personal data breaches to the Controller in accordance with Article 33;
3.9 The Processor must delete or return all personal data to the Controller as requested at the end of the contract;
3.10 The Processor must submit to audits and inspections, provide the Controller with whatever information it needs to ensure that they are meeting their Article 28 obligations;
3.11 The Processor must tell the Controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state;
3.12 The Processor must co-operate with supervisory authorities (such as the Data Protection Commission) in accordance with Article 31;
3.13 The Processor must employ a Data Protection Officer if required in accordance with Article 37;
3.14 The Processor must appoint (in writing) a representative within the European Union if required in accordance with Article 27;
3.15 The Processor may be subject to investigative and corrective powers of supervisory authorities (such as the Data Protection Commission) under Article 58 of the GDPR;
3.16 If the Processor fails to meet its GDPR obligations, it may have to pay compensation under Article 82 of the GDPR;
3.17 If the Processor fails to meet its GDPR obligations, it may be subject to an administrative fine under Article 83 of the GDPR;
3.18 If the Processor fails to meet its GDPR obligations, it may be subject to a penalty under Article 84 of the GDPR.
3.19 Nothing within the contract relieves the Processor of its own direct responsibilities and liabilities under the GDPR.

4. Risk Allocation:

4.1 State details of any risk mitigation measures. State details of any indemnity that has been agreed.

Signed at [location] on [date] in duplicate, each Party acknowledging having received its original copy.

For the Controller	**For Processor**
Name:	Name
Title:	Title:
Date:	Date:
Signature:	Signature:

APPENDIX C: DATA SHARING ARRANGEMENT

Data Sharing Arrangement (Consultant Controller with other Controllers)

This Data Sharing Arrangement sets out the framework for the sharing of Personal Data between a Consultant and another Data Controller to ensure that there is a clear attribution of data protection responsibilities between controllers, and that this information is made available to data subjects.

Controller Responsibility

Each Controller is responsible for:

- Compliance with all Data Protection obligations for personal data they hold.
- Making this arrangement known to data subject.
- Ensuring the data subject is fully informed, and understands, what is being transferred between Controllers, and for what purposes.
- Informing the Data Subject if the intention is to use the data for any other reasons other than those defined specifically on collection, in this case the controller must notify the data subject prior to that processing taking place.

Data Subjects Rights

Data Subjects have the right to obtain certain information about the processing of their Personal Data.

The Parties agree that the responsibility for complying with Subject Rights falls to the Party receiving a Subject Access Request in respect of the Personal Data held by that Party.

The Data Subject may exercise his or her rights under this Regulation in respect of and against each of the Parties as Controllers.

Resolution of Disputes with Data Subjects or the Data Protection Commission

In the event of a dispute or claim brought by a Data Subject or the Data Protection Commission concerning the processing of shared personal data against either or both Parties, the Parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely and efficient manner with the vital interests of the patient and the provision of their healthcare paramount.

Termination of Agreement

The Controllers will notify each other if they intend to terminate any sharing agreements and act appropriately in deleting personal data. This will include all Service Providers involved in processing of data such as Cloud Providers/Software Providers, etc.

APPENDIX D: PRACTICE PRIVACY STATEMENT

Consultant or Group Practice Name	
Consultant or Group Practice Address	
Telephone Number	
Data Controller	
Lead for Data Protection	

Practice Privacy Statement

We want to ensure the highest standard of medical care for our patients consistent with 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. This statement is intended to inform you of our policies and practices regarding the processing of your medical information.

Legal Basis for Processing Your Data

This practice complies with the IHCA Data Protection Guideline for Consultants. The processing of personal data in a Consultant practice is necessary for medical diagnosis and the provision of healthcare or social care or treatment. In most circumstances we hold your data for eight 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, we need to collect and keep personal data about you and your health on our records. This includes basic personal information, contact details, billing information, etc. which we will use for administrative purposes. We will also record data related to your physical or mental health, i.e. personal data which reveals information about your health status, including vaccination details, medication details, allergies and test results, etc.

- We retain your personal data 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 personal data we ask for if you are not sure why it is needed.
- We ask you to inform us of 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 any change of address and phone numbers.
- All employees 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 data 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 administrative staff 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 prescriptions for patients. These are then reviewed and signed by the Consultant.
- Generating a sickness certificate for the patient. This is then checked and signed by the Consultant
- Typing referral letters to other consultants or allied health professionals such as physiotherapists, occupational therapists, psychologists and dieticians.
- Opening letters from hospitals and other healthcare professionals. 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 reports and performing integration of these results into the electronic patient record.
- Photocopying or printing documents for referral to other healthcare professionals.
- Checking for a patient if a laboratory or radiology result has been returned.
- Handling, printing, photocopying and postage of medico-legal and life assurance reports, and of associated documents.
- Sending and receiving information via secure email.
- And other activities related to the support of the provision of medical care and treatment.

Disclosure of Information to your health insurer

We will need to share your personal data with your health insurer for the purpose of claims processing. The health insurance claim form that you sign will have certain data protection provisions which provide for your consent in this regard. If it is intended to share your data with your health insurer for any other purpose that is not directly related to the processing of your health insurance claim, a separate explicit declaration of consent will be required from you and your health insurer may contact you in this regard.

Disclosure of Information to Other Health and Social Care Professionals

We may need to pass some of your personal data 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 health and social care professionals are also legally bound to treat your personal data 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 data (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 Consultant will only provide a confirmation that you are unfit for work with an indication of when you will be fit to resume work. Where it is considered necessary to provide additional information we will discuss that with you. However, Department of Social Protection sickness certs for work must include the medical reason you are unfit to work.

In the case of disclosures to health insurance companies, other insurance companies or requests made by solicitors for your records we will only release the information with your explicit consent.

Use of Information for Training, Teaching and Quality Assurance

It is usual for Consultants to discuss patient case histories as part of their continuing medical education or for the purpose of training 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 Consultants 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

From time to time, patients' personal data may be used for research and audit in order to improve services and standards of practice. The National Quality and Risk Management Standard for the Health Service Executive means some Consultants may be subject to a clinical audit. Information used for such purposes is done in an anonymised or pseudonymised manner with all personal identifying information removed.

If it is proposed to use your information in a way where it would not be anonymous or if we are involved in external research, we would discuss this further with you before we proceed 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 personal data held about you by this practice. If you wish to see your records, you can discuss this with your Consultant who will review the information in the record with you. You can also make a formal written access request and receive a copy of your medical records. These will be provided to you within 30 days, without cost. However, it should be noted that there may be circumstances where access may be restricted or denied, for example, where disclosure would be likely to cause serious harm to the physical or mental health of a patient.

Transferring to Another Doctor

If you decide at any time and for whatever reason to transfer to another Consultant or doctor we will facilitate that decision by making available to your new Consultant or doctor a copy of your records on receipt of your signed consent from your new Consultant or 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 under certain specific circumstances, restriction of processing, objection to processing and data portability. You also have the right to lodge a complaint with the Data Protection Commission.

Questions

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

APPENDIX E: PRIVACY NOTICE

Data Protection Regulations

Medical Records

In order to provide for your care, we need to collect and keep personal data and information about you and your health in your personal medical record. This is underpinned by our commitment to respect the privacy and confidentiality of your personal data and information.

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

We have voluntarily adopted the recommendations of the '*GDPR Guideline and Action Points for Hospital Consultants'* as issued by the Irish Hospital Consultants Association.

For further details please request a copy of our Practice Privacy Statement.

Thank you.

APPENDIX F: PATIENT CONSENT FORM

I _____of_____
Hereby give my permission for (add Consultant Name or Group Practice) to share personal data with other health service providers and third parties in connection with my care, including accessing and sharing my medical and personal data. I understand that [***Consultant or Group Practice name***] may hold information gathered about me from various sources and as such, my rights under the Data Protection Act 2018 and the GDPR will not be affected.

Statement of Consent:

- I understand that personal data is held about me, including medical records.
- I have had the opportunity to discuss the implications of sharing or not sharing my personal data.
- **I agree that my personal data may be shared with and transfered from the following:**
  - The HSE and other health services, including my GP.
  - Health insurance providers for claims processing purposes, billing audits, utilisation review, etc.
  - Practice Management Companies (invoicing, etc.)
  - HSE, Voluntary and Private Hospitals
  - (*Add here insurance companies, solicitors, banks, etc. as the case may be*)

☐ I agree to my personal data being shared with and gathered from the parties identified above

☐ I agree to my personal data being used for health research purposes ***[delete as appropriate]***

Your consent to share personal information is entirely voluntary and you may withdraw your consent at any time. Should you have any questions about this process, or wish to withdraw your consent, please contact: [*Insert name of designated Data Protection Lead in the Practice*]

Name ……

Address ……

Date of Birth ………

Patient Signature ……

Date ……

Signature of professional ……

Print name ……

APPENDIX G: DATA PROTECTION ACCOUNTABILITY LOG

Overview

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

Accountability Log

To demonstrate that you are accountable, you need to keep a 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;

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 (See Appendix J)
- Records of Processing Activities (See Appendix A)
- Confidentiality agreements with staff (See Appendix H)
- Records of staff training and awareness
- Processor contracts with Practice Software Vendors and any other data processors (See Appendix B)
- Where processing on basis of consent, records of this consent (See Appendix F)

Accountability Log for General Data Protection Regulation (GDPR)

Consultant or Group Practice Name		
Consultant or Group Practice Address		
Telephone Number		
Data Controller		
Lead for Data Protection		
Practice Software System		
Date	**Event**	**Description**

APPENDIX H: STAFF CONFIDENTIALITY AGREEMENT

Consultant or Group Practice Name	
Consultant or Group Practice Address	
Telephone Number	
Data Controller	
Lead for Data Protection	
Name of Staff Member	
Role	

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

- To treat all patient information and personal data, 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.
- To only access medical records where it is necessary for the delivery of care to the patient or associated administration.
- Not to remove documents or digital records from the practice without the consent of the responsible Consultant.
- Not to access records belonging to me, members of my family or those known to me without advance authorisation from the responsible Consultant.
- Not to discuss confidential patient information outside of the practice.
- 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: POLICY FOR SUBJECT ACCESS REQUESTS, RECTIFICATION & ERASURE

Consultant or Group Practice Name	
Consultant or Group Practice Address	
Telephone Number	
Data Controller	
Lead for Data Protection	

This policy and procedure document has been written to ensure that good practice is adopted when dealing with requests for personal data from a Data Subject. All staff are responsible for adhering to the timescales highlighted in this policy and aiding with requests for access to or copies of requested information.

Under Article 15 of the General Data Protection Regulation (GDPR) Data Subjects *have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her is being processed, and, where that is the case, access to the personal data and the following information:*

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 Article 22(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.*

Subject Access Request (SAR) Procedure

Stage 1 – Request Received

A formal Subject Access Request must be made in writing and sent by email, fax or hard copy letter. There is no formal application form that is required to be completed by Data Subjects.

All requests are handled by [named individual] who is referred to in this document as the designated contact.

Where a request is received by any staff member it must be forwarded to the designated contact without delay and no later than 24 hours after the request has been received. An acknowledgment letter shall be forwarded to the applicant by the designated contact confirming receipt of the request (see SAR Template 1 attached).

If data subjects ask for advice on applying for access, staff should advise them that they will need to:

a) Put their request in writing
b) Provide any relevant information that is required to sufficiently confirm their identity
c) Provide any relevant information to help locate the information required

The GDPR does not prevent an individual making a Subject Access Request via a third party. Often, this will be a solicitor acting on behalf of a client, but it could simply be that an individual wants someone else to act for them. In these cases, we need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney.

If the designated contact does not take action on the request of the Data Subject, the designated contact shall inform the Data Subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and potentially seeking a judicial remedy.

Information provided as part of a Subject Access Request shall be free of charge. The designated contact may consider charging a reasonable fee where requests from a Data Subject are manifestly unfounded or excessive. More specifically Article 12 (5) of the GDPR states:

> *Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:*
>
> 1. *charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or*
>
> 2. *refuse to act on the request.*
>
> *The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.*

It is recommended that a Data Controller should document the decision-making process and keep a record any evidence that supports a conclusion that the request is excessive or unfounded.

Stage 2 – Identity Check

To comply with the law, information relating to the Data Subject must only be disclosed to that person or someone authorised to receive it on their behalf. For that reason, an identity check of the individual or the individual's representative must be completed.

The following individuals may apply for access to their records:

- The Data Subject to whom the personal data relates
- The Data Subject's representative, with the Data Subject's consent
- A person appointed by the Court
- Relevant professional bodies
- Law enforcement agencies

Adequate steps must be taken to establish the identity of the requesting party before proceeding to comply with the request.

Where there is any doubt, proof of identity will be required. Examples of suitable documentation include copies of:

- Valid Passport
- Driving Licence
- Birth Certificate along with some other proof of address (e.g. a named utility bill or a Medical Card)

The following table shows the documentation or identity checks that are required for the different requester types:

Requester	**Consent Required?**	**Identity Document Required**	**Any Other Documentation Required**
The Data Subject (the person to whom the personal data or information relates)	No. As the request is made by the individual then further consent is not required	Photo ID document such as Passport or Driving Licence. Proof of address	No
Law Enforcement	No, this is addressed by the Law Enforcement Directive	Law Enforcement ID Card must be checked prior to providing the information	Data Protection Access Request Form stating (i) the reason(s) for the request, and (ii) a crime reference number
Courts	No	N/A	No, this is addressed under the Data Protection Act 2018
Relatives, Next of Kin, Personal Representative	Yes (where applicable)	Photo ID document such as Passport or Driving Licence. Proof of address. Confirmation to show relationship with the Data Subject.	No
Solicitors	Yes	N/A	Signed consent form completed by the Data Subject

Third Parties (other organisations not listed)	Yes	N/A	Data Subject's consent is required to provide information to Third Parties.

The designated contact should not retain personal data for the sole purpose of being able to react to potential requests. Therefore, all identity documents provided to the designated contact as part of the identity check process shall be securely destroyed.

The identity of the Data Subject or his/her representative must be verified before any personal data is released.

Stage 3 – Record Located

The designated contact must comply with Subject Access Requests promptly and in any event within one month of the date on which the request was received or (if later) the day on which the designated contact received the necessary information and documentation requested to confirm the requester's identity.

Before responding to the Subject Access Request the designated contact may ask the requester for information reasonably required to retrieve the personal data covered by the request, such as:

- Additional details that will help locating the requested information
- Information about the context in which the requested information may have been processed
- Likely dates when processing occurred
- If personal data is in electronic form, information as to the type of electronic data being sought, e.g. application form, letter, email, etc.

Stage 4 – Copy Records

Once the Records Location exercise has been completed the designated contact will arrange to retrieve a copy of all records, manual and electronic, in relation to the request.

Hard copy manual records should be copied at the location they are held.

Stage 5 – Exemption Review

Restrictions under GDPR and the Data Protection Act 2018

The GDPR recognises that in some circumstances controllers might have a legitimate reason for not complying with a Subject Access Request, so it provides a number of restrictions and exemptions from the duty to do so, specifically:

> *Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:*
>
> *a) national security;*
>
> *b) defence;*
>
> *c) public security;*

d) *the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;*

e) *other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;*

f) *the protection of judicial independence and judicial proceedings;*

g) *the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;*

h) *a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);*

i) *the protection of the data subject or the rights and freedoms of others;*

j) *the enforcement of civil law claims.*

The Data Protection Act 2018 further expands on the restrictions applicable. In such cases, legal advice should be sought.

Exemptions review and Third Party information removal

In some cases, Subject Access Requests may cover information which relates to one or more people (Third Parties) other than the Data Subject. The information about the other third party may include personal data about that party to which the usual data protection rules apply.

There are generally two components to the meaning of third party:

- A person who has provided information (about the Data Subject)
- An organisation, other than the data controller or data processor that has provided information (about the Data Subject)

Section 91(7) of the Data Protection Act 2018 provides that where information that a controller would otherwise be required to provide to a data subject includes personal data relating to another individual that would reveal or be capable of revealing the identity of that individual, the controller shall not provide the data subject with the information and shall provide, instead, a summary of the personal data that, insofar as possible, permits the data subject to exercise his or her rights and does not reveal, or is not capable of revealing, the identity of the other individual. However, where the third party whose personal data is contained within the information the data subject is seeking consents to the provision of this information, the data controller can disclose it to the data subject. This legislative rule applies regardless of whether this third party is a health professional or not as the exemption from withholding or redacting the third party data of health professionals previously contained in Regulation 6 of the Data Protection (Access Modification) Health) Regulations (S.I. 82/1989) has been deleted.

Therefore, the only basis for justifying the disclosure of third party information in response to a Subject Access Request is that the third party has given their consent. The designated contact must write to them asking if the third party consents to the disclosure. Please see attached SAR Template 2 to be sent to third parties asking for consent. In some cases, it may be difficult to obtain third party consent, for example the third party might refuse consent, he/she might be difficult to locate or may not be capable of giving consent.

If consent is obtained, the designated contact shall acknowledge the receipt of consent from the third party. please see SAR Template 3 which is an email for acknowledgment of third party consent.

If consent is not obtained, the designated contact must assess if a summary of the personal data can be provided to the data subject which does not reveal the identity of the third party and which allows the data subject to exercise his/her relevant rights. If this is possible, there is a positive obligation on the data controller to provide this summary to the data subject.

Where it is agreed an exemption applies, the designated contact where information is located must review the record in its entirety and redact the exempt information to ensure that this cannot be read or interpreted by the remaining information. Where an exemption is applied this must be explained within the disclosure response.

If challenged, you must be prepared to defend to the Data Protection Commission's Office, or a court as the case may be, your decision to apply an exemption. It is therefore good practice to ensure that such a decision is taken by the Consultant in his or her own right and that the reasons for it are documented.

Stage 6 – Release Information

Once any queries around the information requested have been resolved, copies of the information in a permanent form will be sent to the Data Subject. The designated contact will make the information available to the individual or requester either by providing photocopies or, if the requester has made a Subject Access Request electronically, they may prefer to receive the response electronically. In the case of an electronic request, information will be provided via email in the form of a scanned copy. It is good practice to check with the data subject as to his or her preferred method of receiving the information. Alternatively, the designated contact may invite the Data Subject or his/her representative to attend a meeting to view the records. Each case will be considered on an individual basis as to whether there is a requirement for the provision of additional support for the interpretation of these records.

If information is copied from the records, it should preferably be handed to the individual. If that is not possible, and the information has to be posted, it must be sent via registered post as a minimum requirement.

No matter how the information is supplied to the Data Subject, all of it must be intelligible. At its most basic, this means the information should be understandable by the average person. If records contain codes, complex or technical terms, an understandable explanation must be provided, for example by including a relevant abbreviation list.

In accordance with Article 15 of the GDPR, the information sent to the Data Subject as part of the Subject Access Request should also include:

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 Article 22(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.*

The designated contact must reply to the Data Subject within the specified timelines, without delay or within one month of the receipt of a Subject Access Request. If no exceptions are applied, please see the attached letter in SAR Template 5 in response to a Subject Access Request providing the requested information. If exceptions are applied, please see the attached SAR Template 6.

A record of all access requests must be maintained with a full audit trail of actions completed and decisions taken.

Unfounded and excessive requests

In cases where an individual's Subject Access Request is "*manifestly unfounded or excessive*", the designated contact may be permitted to charge the individual for the administrative costs of retrieving the information. A Data Subject may be charged if a request is repetitive or if additional copies of data are requested.

In addition to being permitted to charge the individual if their request is unfounded and/or excessive, the designated contact may outright refuse to respond to the request. If the designated contact chooses to do this, however, reasons for the refusal must be given to the individual. See the attached letter in SAR Template 7 to be sent in the event of refusal. The individual will also need to be informed of their right to complain to the relevant supervisory authority and of their right to a judicial remedy. Both the reasons for refusal and the advising of the right to complain should be put to the individual without undue delay and, at the very latest, within one month of the request.

The designated contact is not obliged to comply with an identical or similar requests to ones already dealt with unless a reasonable interval has elapsed between the first request and any subsequent ones. When dealing with such requests, consideration should be given to the following:

- The nature of the data – this could include considering whether it is particularly sensitive.
- The purposes of the processing – this could include whether the processing is likely to cause detriment or harm to the requester.

The particular circumstances of each request should be evaluated, balancing any difficulties involved in complying with the request against the benefits the information might bring to the Data Subject, whilst bearing in mind the fundamental nature of the right of access. In order to apply any exceptions, the member shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request and be able to provide proof showing that all reasonable steps have been taken to comply with the Subject Access Request, and that it would be disproportionate in all the circumstances of the case for the designated contact to take further steps.

It is recommended that in the above circumstances the designated contact engages with the Data Subject about the information required and try to reduce the scope and therefore the costs, time and effort that would otherwise be incurred in searching for and retrieving the information.

SAR Template 1: Acknowledgment Letter

Dear *[Name]*

Thank you for your *[letter/email/fax]* of *[date]* requesting information about *[subject].* I am writing to let you know that we have received your request and will process it as soon as possible, and within one month of the day we received the request. You will hear back from us by *[calculate date by which you must have processed the request]* at the latest.

Yours etc.

SAR Template 2: Obtaining the Consent of a Third Party

Dear *[Name of third party]*

I am writing to seek your views on the disclosure to *[name of data subject]* of *[give brief description of document/s]*.

We have received a Subject Access Request from *[name of data subject]* under the Data Protection Act 2018. Under this Act *[name of data subject]* has a right to receive copies of the information we hold about *[him/her]* unless particular exemptions apply. These exemptions include information about third parties where the third parties' interest in the data remaining confidential is greater than *[name of data subject]* 's interest in receiving the data.

In our search we identified some records that involve you. Before disclosing substantive third party information it is our practice to seek the views of the third party concerned and to take these views into account when responding and, potentially, applying an exemption. *[Name of data subject]* has the right to challenge any non-disclosure decisions that we make. This means that we cannot guarantee that these records will not be disclosed. However, we will ensure that your views are taken into account in any discussion about their disclosure.

The items concerned are included in *[describe file]*. They are:

1. *[Itemise the documents concerned or for large quantities list the number of pages]*

I enclose copies of them for your information.

Please advise by return whether or not you have any objections to the disclosure to *[name of the data subject]* of your *[name of the document]*. If you do have any objections, please explain the nature of your objections so that we can take your views into account when considering whether to disclose.

The Data Protection legislation requires us to reply to *[name of data subject]* by *[date – one month after receipt of valid Subject Access Request],* so I would be grateful if you could reply to my letter by *[date – allow sufficient*

time to consider and assess the issues and to reply]. If you would like clarification of any of the points I have raised, please feel free to contact me.

Yours sincerely

SAR Template 3: Acknowledgment of the Third Party's Consent to Disclose the Information

Dear *[Name of referee]*

[Name of data subject]

Thank you for your letter dated *[date]* concerning the disclosure of *[name of the document]* in response to *[name of data subject]'s* Subject Access Request. As you have no objections to the release of the information, I will include it in the information that I supply to *[name of data subject]* in response to *[his/her]* Subject Access Request.

Thank you for taking the time to consider this matter.

Yours sincerely

SAR Template 4: Acknowledgment of the Consideration of the Third Party's Opinions

Dear *[Name of referee]*

[Name of data subject]

Thank you for your letter dated *[date]* concerning the disclosure of *[name of the document]* in response to *[name of data subject*]'s Subject Access Request. Following consideration of your views we have decided *[not to disclose the document(s) / to disclose an anonymised version of the document(s) / to disclose the document(s)].*

[Explain how you came to your decision.]

Thank you for taking the time to consider this matter.

Yours sincerely

SAR Template 5: Replying to a Subject Access Request Providing the Requested Information

Dear [Name of data subject]

Data Protection Act 2018 Subject Access Request

Thank you for your letter of *[date]* making a data Subject Access Request for *[subject]*. Having carried out a search of our *[systems/paper records etc.]* on the personal details supplied in your request we are pleased to enclose the information you requested.

Under Article 15 of the GDPR you have the right of rectification of inaccuracies in your personal data that we hold, the right of erasure, the right of restriction of processing of personal data and the right to object to such processing.

If you are unhappy with the level of service you have received in relation to your request and wish to make a complaint or request a review of my decision you have the right to lodge a complaint with the Data Protection Commission or potentially seek a judicial remedy.

Yours sincerely

SAR Template 6: Release of Part of Information, when the remainder is covered by an exemption

Dear *[Name of data subject]*

Data Protection Act 2018 Subject Access Request

Thank you for your letter of *[date]* making a data Subject Access Request for *[subject].* To answer your request, we asked the following areas to search their records for information relating to you:

- *[List the areas]*

I am pleased to enclose *[some/most]* of the information you requested. *[If any information has been removed]* We have removed any obvious duplicate information that we noticed as we processed your request, as well as any information that does not relate to you. You will notice that *[if the documentation is incomplete]* parts of the document(s) have been blacked out. *[OR if there are fewer documents enclosed]* I have not enclosed all of the information you requested. This is because *[explain why it is exempt]*.

Under Article 15 of the GDPR you have the right of rectification of inaccuracies in your personal data that we hold, the right of erasure, the right of restriction of processing of personal data and the right to object to such processing.

If you are unhappy with the levels of service that you have received in relation to your request and wish to make a complaint or request a review of my decision you have the right to lodge a complaint with the Data Protection Commission or potentially seek a judicial remedy.

Yours sincerely

SAR Template 7: Replying to a Subject Access Request Explaining Why You Cannot Provide Any of the Requested Information

Dear *[Name of data subject]*

Data Protection Act 2018 Subject Access Request

Thank you for your letter of *[date]* making a data Subject Access Request for *[subject].*

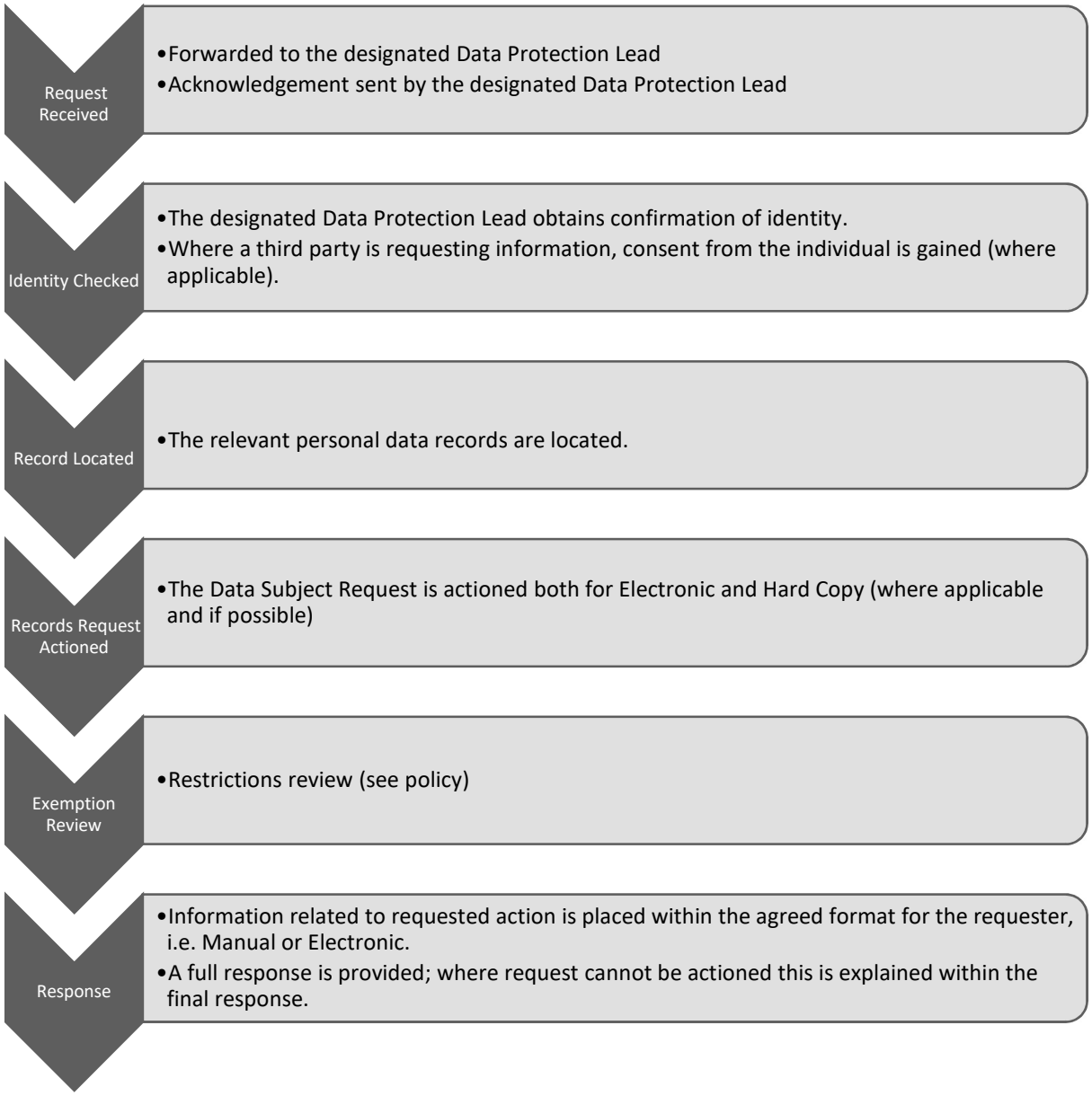
I regret that we cannot provide the information you requested. This is because *[explanation where appropriate].*

If you are unhappy with the level of service that you have received in relation to your request and wish to make a complaint or request a review of my decision you have the right to lodge a complaint with the Data Protection Commission or potentially seek a judicial remedy.

Yours sincerely

Data Subject Rights Process

This flow chart applies to Rights for: Access, Rectification, Erasure, Restriction, Portability and Objection



APPENDIX J: IT GUIDANCE: SYSTEMS AND COMMUNICATIONS – BEST PRACTICE

The following is a list of important best practices for healthcare data security in any practice, regardless of Vendor:

1. **Protect your Network**: When you connect to your practice software (Cloud/Mobile/Laptop/Office), make sure access is via use of a complex password, ONLY by authorised and properly trained staff.

2. **Train both yourself and your staff**: Make sure everyone is aware of what phishing and ransomware are, what a strong password should be, and why data protection is so important.

3. **Encrypt Mobile/Portable devices**: Data breaches often occur because a portable computing or storage device containing protected health information is lost or stolen. You can prevent this: Encrypt all devices that might hold personal data, including laptops, smartphones, tablets and portable USB drives, and most importantly, do not hold any personal data on an unencrypted portable device.

4. **Using a Fax:** Where possible, transmission of personal health information by fax should be avoided. If possible, use secure 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 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.

5. **If you have a wireless network, make sure it is secure**: many Consultants are increasingly relying on wireless routers for their network. Unfortunately, those wireless networks often introduce security vulnerabilities. Data can be stolen by hacking into those networks from an external location, for example, especially if the organisation relies on outdated technology such as “WEP”. To protect against attacks, you should make sure that routers and other components are kept up to date, network passwords are secure and changed frequently, and unauthorised devices are blocked from accessing the network.

6. **Implement Physical Security Controls**: Even as electronic health records become more common, many Consultants still keep sensitive data on paper. Therefore, you must make sure doors, filing cabinets are

locked, and that camera and other physical security controls are used. In addition, you should physically secure IT equipment by locking server rooms and using cable locks or other devices to keep laptop and desktop computers attached to office furniture.

7. **Have a Mobile device policy**: As employees increasingly use personal devices to do their work, it is important that every organisation create a mobile device policy that governs what data can be stored on those gadgets, what apps may be installed, etc. At the very least, make sure any mobiles used have a password lock screen enabled.

8. **Archive Data you do not need**: One lesson many data breach victims have learned is that the more data that is held, the more there is for hackers to steal. You should have a policy mandating the archiving of patient and other information that is no longer needed, but has a retention requirement. Most vendors can provide secure archiving.

9. **Vet/assess third party and vendor security**: Along with the mobile devices, the biggest IT trend in the past few years has likely been the rise of cloud computing. Cloud-based services have enabled smaller organisations to take advantage of many of the same technologies as large organisations by lowering the up-front costs necessary for deployment. However, putting information in the hands of third parties also creates a number of new risks. Therefore, it is important to vet the security of cloud computing vendors and other third parties with whom you contract.

10. **Make sure to install updates when prompted**: It is easy to ignore Windows and iOS updates as it can result in downtime. However these are very important for the security of your ICT systems. If at all possible allow them to take place when alerted by your system.

11. **Have a Data Breach Response Plan**: It is almost impossible to prevent every IT security incident so make sure you are familiar with the data breach response plan in the guide. (See Appendix K).

<u>Do you use Cloud Services? Here is what you need to know about Data:</u>

If you are using cloud services to store data you need to be aware of the following issues around Data Protection and how to address them:

The Data Protection Act and GDPR prohibits transfer of personal data to outside the EEA unless one of a number of conditions is satisfied:

- EC Model clauses are used
- Privacy Shield is used if Data is stored in US
- Data is only stored in Countries approved by EC

This applies in relation to all layers of the service, and as you need to inform your patient if data is transferred outside of the EEA the simple solution is to ensure you only use a provider that provides assurances that Data is not transferred outside the area.

The following are the main Data Protection risks associated with using Cloud based services, and should be considered when using a Cloud Provider to store Data:

- Liability for indirect loss, loss of profits and data is frequently excluded.
- Liability for direct loss should not be excluded, but sometimes it is.

- Customer is made responsible for back-up / security
- Data security is inadequate
- Not knowing where your data is located
- Does Cloud Provider guarantee region / location of data?
- Service terms do not include data processing clauses required by Data Protection Acts. Check that the service terms stipulate that the Cloud Provider will only process personal data on the instructions of the customer. In addition, check that the Cloud Provider is required to ensure that adequate technical and organisational security measures are in place.
- The National Standards Authority of Ireland (NSAI), in conjunction with the Irish Internet Association (IIA), has published "*Adopting the Cloud – Decision Support for Cloud Computing*". It provides useful information on the different models of cloud computing and the issues (including data protection and security) that need to be addressed by any organisation considering using a cloud provider. It is available from the NSAI at www.standards.ie.

Access Control (Systems and Data): Who has access in your practice?

Apply the least privilege access control – applying the least privilege rule is one of the best practices when setting up access control. In general terms, least privilege means that access should be granted only to persons who explicitly need to have it. Access control privileges should not be given out of convenience, and this applies to all forms of data wherever it is kept.

If possible, you should adopt the following for new members of staff with regard to the level of access and user rights/responsibilities they will receive:

- All staff or third parties will only be given access to specifically approved system groups.
- Only the Consultant can request and authorise changes in user accounts.
- For new employees, passwords must be provided to the user verbally (and in the office).
- If new employees have already read and accepted any employee handbook/policy, there is no need to sign off on the employee's responsibilities separately.
- New employees must be shown any security/data protection training for review.

And for staff who leave the practice:

- Remove/revoke all the user accounts.
- Repose/Disable users access card if applicable.
- Repose/Disable user's laptop and/or mobile phone if applicable.
- Make sure to retrieve/transfer relevant data back to the practice in case the laptop/mobile phone is owned by the employee
- Change all generic passwords if used on systems accessible from outside the your network (Practice systems/webmail, etc.)
- Send out a notification of termination to all other employees if not already sent by the employee himself or herself.
- Optional: If the employee was terminated by a practice management decision, it is advisable to send out an alert to all employees asking for details of those systems to which the terminated employee might have access (large practices).

Use of Email

Compromised email can result in several problems, such as:

- Intellectual property loss: this includes stolen medical information. These can be used for blackmail, or can even be sold on the internet to the highest bidder.
- Email contact loss: stolen address books mean your contacts and patients may be exposed to future spam and malware attacks.
- Also, depending on circumstances, data breaches might have to be publicly disclosed and practices may incur significant fines.

Attackers have a multitude of options at their disposal. Some individuals with malicious intent may run a simple Web search to obtain your webmail URL. Once they have this information, they can employ bots (automated programs) to guess a correct username and password. The most common attack is targeted phishing emails designed to deceive or mislead IT personnel. These messages employ various social engineering tactics to trick users into disclosing their password. Once the attackers have the passwords, they can login to the relevant webmail server and engage in additional malicious activity.

How can you stop this?

- Implement a two-factor authentication process with a hardware or software token. This will require a user to provide a second set of authentication credentials (in addition to username and password) to log into webmail. Most mail providers can facilitate this.
- Consider allowing only specific users access to webmail. This will reduce the attack surface area, which in turn reduces the probability of being targeted. In many instances, not all employees truly need webmail access outside of office hours.
- Avoid generic or webmail URLs that can be easily guessed or ascertained (such as webmail.domain.com or mail.domain.com).
- Enforce an effective password policy (such as requiring complex passwords) and force regular password changes.
- Train staff on Phishing/Malware and how to avoid these attacks.

Actions that you must take.

Be aware that your ICT Security needs to:

- Protect sensitive information
- Prevent theft of information
- Prevent Fraud
- Avoid damage to reputation
- Comply with laws and regulations
- Protect your Practice
- Protect your Patients

Implement a Password Policy:

Are your passwords complex enough? How many accounts do you have in a professional and personal life that need usernames and passwords? Now ask yourself, what percentage of these accounts have the same password? If the answer is more than one, please change this today.

Implement an Email Policy:

- Beware of attachments in unexpected e-mails.
- If a suspicious email is received log a call to your IT provider to investigate but don't forward the email.
- Never open an email attachment if it in the Junk or Spam folder.
- Never reveal personal or financial information in a response to an email request, no matter who appears to have sent it.
- Financial institutions NEVER include links to websites in email messages or request personal information by email.
- Do not access webmail services (e.g. Gmail, Hotmail or Yahoo etc.) from work computers unless you have secured them with all available security features.
- Check if the recipient address is correct before sending an email.

Implement Acceptable Use Policies:

Internet Use for you and your staff:

- Accessing or publishing illegal material
- Accessing or publishing offensive material
- Excessive personal use
- Use of chat rooms

Be careful about Social Media Use

- Do not bring the practice into disrepute
- Personally responsible for content you publish
- Do not post on behalf of the practice without permission
- Never post confidential information

Implement a Clear Desk Policy:

The main reasons for a clear desk/clear screen policy are:

- A clear desk/clear screen can produce a positive image when our patients visit the practice.
- It reduces the threat of a security incident, as confidential information will be locked away when unattended.
- Digital information cannot be taken from un-attended and locked machines.
- Sensitive documents left in the open can be stolen by a malicious entity.

You will need to:

- Consider your document classification.
- If you leave your desk for a prolonged period of time, ensure you clear away all information.
- Store anything confidential in a locked cabinet.
- Clear all meeting rooms at the end of meetings.

Clear Screen:

- Lock the screen when your computer is left unattended.
- Be wary of "shoulder surfing" from Visitors.
- Above all, use common sense!

- At known extended periods away from your desk, such as a lunch break, sensitive working papers are expected to be placed in locked drawers.
- At the end of the working day everyone is expected to tidy their desk and to put away all practice papers. The practice provides locking desks and filing cabinets for this purpose.
- Computers and laptops must not be left logged on when unattended. If staff have to leave their desks for any reason, they must lock the computer by using the 'Control, Alt, Del' keys simultaneously. Access to the computer/laptop must be protected by strong passwords; this is best practice.
- If sensitive or confidential information is being worked on, the screen must be closed, minimised or locked when unauthorised persons are in close proximity to the screen.
- If sensitive or confidential information is visible to an unauthorised person standing in close proximity to computer/laptop screen, they should be asked to move away to protect the confidentiality of this information.

Action

- Allocate time in your day to clear away your paperwork.
- Always clear your workspace before leaving for longer periods of time.
- If in doubt - throw it out. If you are unsure of whether a duplicate piece of sensitive documentation should be kept, it will probably be better to place it in the shred bin.
- Consider scanning paper items and filing them electronically on your computer.
- Use shredding for sensitive documents when they are no longer needed.
- Lock your desk and filing cabinets at the end of the day.
- Lock away portable computing devices such as laptops or any mobile devices.
- Treat mass storage devices such as CD-ROM, DVD or USB drives as sensitive and secure them in a locked drawer.
- Always lock your computer when it will be unattended.

Implement Mobile Device Policy:

- Applies to the use of mobile devices that can store data such as laptops, personal digital assistants (PDAs), iPADs, PADs and mobile (smart) phones which are particularly vulnerable to loss and theft.
- Portable media includes devices such as USB keys, CD/DVDs.
- Be cautious about inserting CDs or attaching USB sticks to practice computers. Always be sure of its source and content.
- Staff should ensure that no sensitive information is stored on mobile devices (USB, iPADs and mobile phones).
- Do not connect your phone to the practice computer.
- Passwords should not be written down (or stored e.g. in laptop cases).
- Always lock the screen if leaving your computer unattended.

And Just as important: Your Office

- Only authorised users allowed in secure areas.
- Consider visitor sign-in and escort to confidential areas (IT provider etc.).
- Challenge any person you don't know.
- Report any suspicious activity.
- Don't leave highly confidential information in printers or on computer screens.

Template Bring Your Own Device (BYOD) Policy

(*Use whichever statement is appropriate and amend/delete accordingly*)

We support widespread use of BYOD for work use – i.e. using such devices for the performance of work.

OR

We restrict the use of BYOD to a limited number of employees who would not be able to perform their work otherwise.

The rules in this policy apply to all BYOD, whether they are used for work or for private use, or whether they are used within or outside employment premises.

BYOD devices include all personally owned devices that have the ability to store, transfer or process any sensitive information related to work activities (e.g. laptops, smart phones, tablets, USB memory sticks, digital cameras, etc.).

For each BYOD, the following are mandatory (***Add and/or Delete where appropriate***)

- [*Describe how the backup of information must be conducted*]
- [*Describe which security software must be installed – e.g. anti-virus software, intrusion prevention, mobile device management software, etc*.]
- [*Describe the method of encryption that is to be used and the information/data it will be applied to*]
- [*Describe the method of authentication that is to be used e.g. Multi Factor (MFA)*]
- [*Describe the secure method of connection to the Practice network, e.g. VPN*]
- When using BYOD outside of the employment premises, it must not be left unattended and, if possible, should be physically locked away.
- When using BYOD in public places, the owner must take care that data cannot be read by unauthorised persons.
- Patches and updates must be installed regularly.
- Classified information must be additionally protected according to the Data Classifications and Handling Rules.
- Notify the designated Data Protection lead before BYOD is disposed of, sold, or handed to a third party for servicing.

It is not permitted to do the following in the context of BYOD:

- Allow access to anyone else except the employee who is the owner of the device.
- Install applications that are included in list of BYOD-prohibited applications.
- Store illegal materials on the device.
- Install unlicensed software.
- Connect via Bluetooth to any kind of device.
- Connect to unknown Wi-Fi networks.
- Locally store passwords, except when using the following applications: [*list allowed applications where passwords can be stored*]
- Locally store the following information: [*list sensitive information*]
- Transfer company data to other devices which are not permitted.

We retain the right to view, edit and perform full deletion of all data on BYOD if it is considered necessary for the protection of personal data, without the consent of the device owner.

All security breaches related to BYOD must be reported immediately to the designated Data Protection lead.

APPENDIX K: DATA BREACH RESPONSE PLAN

Consultant or Group Practice Name	
Consultant or Group Practice Address	
Telephone Number	
Data Controller	
Lead for Data Protection	

The following steps outline the different phases of a typical incident response procedure, and what is involved with each step.

Preparation

1. All staff and relevant parties must be aware of this data breach incident procedure and have had adequate data protection training so that they can, at a minimum, identify a breach and alert the designated Data Protection Lead.
2. Appropriate technical and organisational measures must be in place, both on the network and where hardcopy files are located or stored, to ensure that breaches can be detected.
3. The *Records of Processing Activities* (see Appendix A) must be kept up to date so that the extent of a breach can be quickly assessed.
4. Any third party processing data on your behalf must have a nominated contact for data protection queries/issues, and this list of contacts must be maintained and up to date.
5. Where an external expert is required, you shall:

    (a) Maintain up to date contact details in the event that a breach requires investigation and remediation that cannot be provided in-house;
    (b) Have a procedure for providing adequate access so that the external expert can fully investigate the suspected data breach;
    (c) Ensure appropriate Non Disclosure Agreements and Data Protection agreements are in place with the third party.

6. Ensure that a Practice Breach Log is available for recording all required information regarding the personal breach.

Identification and Classification

If an employee considers that a Personal Data security breach has occurred, this must be reported immediately to the designated Data Protection Lead. Once the designated Data Protection Lead has been alerted of the suspected breach, he/she must adopt the following procedures:

1. Request a formal personal data breach incident report from the processor, staff member, or team reporting the suspected personal data breach. A Personal Data Security Breach Report Form should be completed and returned to the designated Data Protection Lead immediately.
2. The designated Data Protection Lead will review Section 1 of the Report form in order to assess and determine:

(a) if a Personal Data security breach has taken place and if so:
(b) the nature of the Personal Data involved in the breach;
(c) the cause of the breach;
(d) the extent of the breach (how many individuals are affected);
(e) the harms to affected individuals that could potentially be caused by the breach;
(f) How the breach can be contained.

3. The designated Data Protection Lead will determine the severity of the incident and complete a Personal Data Security Breach Report Form.

4. Commence formal timeline documentation of the incident in the Practice Breach Log.

The designated Data Protection Lead should complete Section 1 of this form.

Section 1: Notification of Personal Data Security Breach	**To be completed by the designated Data Protection Lead**
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident or details of the information lost:	
Number of Data Subjects affected, if known:	
Has any Personal Data been placed at risk? If, so please provide details.	
Brief description of any action taken at the time of discovery:	
For Office Use	
Received by:	
On (date):	

Forward for action to:	
On (date):	

Section 2: Assessment of Severity	To be completed by the designated Data Protection Lead
Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial, legal liability or reputational consequences for the Consultant or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	
HIGH RISK Personal Data • Sensitive Personal Data (as defined in the Data Protection Acts) relating to a living, identifiable individual's a) racial or ethnic origin; b) political opinions or religious or philosophical beliefs; c) membership of a trade union; d) physical or mental health or condition or sexual life; e) commission or alleged commission of any offence, or f) proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.	
• Information that could be used to commit identity fraud such as personal bank account	

and other financial information and national identifiers, such as Personal Public Service Numbers (PPSNs) and copies of passports and visas;	
• Personal information relating to vulnerable adults and children;	
• Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;	
• Information about individual cases on employee disciplinary actions which could adversely affect individuals.	
• Security information that would compromise the safety of individuals if disclosed.	
Category of incident (……severity level……..):	
Reported to Data Protection Lead on:	

Section 3: Action taken	**To be completed by designated Data Protection Lead**
Incident number:	e.g. Ticket number etc.
Report received by:	
On (date):	
Action taken by responsible manager/s:	
Was incident reported to Gardaí:	YES/NO If YES, notified on (date):
Follow up action required/recommended:	
Reported to designated Data Protection Lead on (date):	
Reported to other internal stakeholders (details, dates):	
For use of designated Data Protection Lead	

Notification to Data Protection Commission	YES/NO If YES, notified on: Details:
Notification to data subjects	YES/NO If YES, notified on: Details:
Notification to other external, regulator/stakeholder	YES/NO If YES, notified on: Details:

Containment

Once it has been established that a data breach has occurred, the designated Data Protection Lead needs to take immediate and appropriate action to limit the breach. Containment involves limiting the scope and impact of the breach of Personal Data.

The following procedures should be adopted when a personal data breach incident is confirmed.

1. Preserve the scene and any devices, files, CCTV footage, etc. involved.
2. Preserve all logs. This could be digital log data or visitor log books, etc.
3. Preserve the memory on affected devices, where relevant and where possible.
4. Determine the most appropriate containment method if the breach is ongoing.
5. Where necessary, ensure all affected devices and applications are identified and isolated.
6. Where necessary, inform users of any systems or areas that containment is in effect. This will ensure that they do not continue to access systems and/or areas that designated Data Protection Lead is attempting to contain. Information provided should be on a need-to-know basis only.
7. If devices are removed from the premises for investigation, ensure a chain of evidence document is maintained, either separately, or recorded by the designated Data Protection Lead in the Breach Log.
8. Establish if it is appropriate to notify affected individuals immediately (e.g. where there is a high level of risk of serious harm to individuals).
9. Where appropriate (e.g. in cases involving theft or other criminal activity), inform the Gardaí.

Investigation & Assessment of Risk

The following procedures should be adopted when the personal data breach incident is being investigated:

1. As much evidence should be gathered as possible, with particular emphasis on the nature and extent of the personal data breach, and the personal data and data subjects involved.
2. Each action taken by the response team, and the results of those actions, should be documented.
3. Determine how and why the incident occurred.
4. Determine the likely consequences of the personal data breach as this information will be required by the Data Protection Commission as part of the breach notification.
5. Determine what measures can be taken to address the breach and, where possible, how the risks to data subjects could be mitigated.
6. Determine if any similar breach incidents occurred in the past.
7. Investigate how the personal data breach incident can be avoided or mitigated in the future.

In assessing the risk arising from a Personal Data security breach, the designated Data Protection Lead is required to consider the potential adverse consequences for individuals, i.e. how likely are adverse consequences to materialise and, if so, how serious or substantial are they likely to be. The information provided in the Data Security Breach Report Form will assist with this stage.

The Breach Response Team will review the Data Security Breach Report Form to:

- Assess the risks and consequences of the breach:

  - Risks for individuals:
    - What are the potential adverse consequences for individuals?
    - How serious or substantial are these consequences?
    - How likely are they to happen?

  - Risks for Practice:
    - Strategic & Operational
    - Compliance/Legal
    - Financial
    - Reputational
    - Continuity of Service Levels

- Determine, where appropriate, what further remedial action should be taken on the basis of the incident report to mitigate the impact of the breach and prevent repetition.

Notification

On the basis of the evaluation of risks and consequences, the designated Data Protection Lead, and others involved in the incident as appropriate, will determine whether it is necessary to notify the breach to others outside the practice. For example:

- the Gardaí;
- individuals (data subjects) affected by the breach;
- the Data Protection Commission;
- other bodies such as regulatory bodies;
- the press/media;
- trade unions;
- cybersecurity insurance providers (if applicable);
- External legal advisers.

Notification of Personal Data breach to the Data Protection Commission

After review of the breach by the designated Data Protection Lead, if the data breached likely affects the rights and freedoms of a data subject, the designated Data Protection Lead will inform the Data Protection Commission within an elapsed time of 72 hours of becoming aware of the breach. The details of the notification will include:

(a) Description of the nature of the Personal Data breach including, where possible, the categories and an approximate number of data subjects concerned and the categories and an approximate number of Personal Data records concerned.
(b) Description of the likely consequences of the Personal Data Breach.
(c) 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.
(d) The name and contact details of the designated Data Protection Lead or other point of contact where more information can be obtained.

If, at the time of making the notification, it is not possible for the designated Data Protection Lead to include in the notification all the information specified above, the designated Data Protection Lead shall nevertheless make the notification including such information as is possible to include at the time, and supply the outstanding information without undue delay.

Notification of Personal Data breach to data subjects

Where 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:

(a) Description of the nature of the breach
(b) Name and contact details of the designated Data Protection Lead
(c) Description of the likely consequences of the Personal Data Breach.
(d) 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.

Notification of Personal Data breach to controllers

Where the Consultant performs the role of processor, the designated Data Protection Lead will notify all controllers without undue delay after becoming aware of a Personal Data breach including:

(a) Description of the nature of the Personal Data breach including where possible, the categories and an approximate number of data subjects concerned and the categories and an approximate number of Personal Data records concerned.
(b) Description of the likely consequences of the Personal Data Breach.
(c) Description of the measures taken or proposed to be taken by the controller to address the Personal Data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Eradication

Once contained, the following procedures should be adopted to ensure that the effects of a personal data breach are not ongoing:

1. Where necessary, ensure that all affected devices and applications are cleared and operating properly. If a number of systems are affected, consider using a single system as proof the eradication procedures are working correctly before allowing full use.
2. Ensure that appropriate security measures are in place to prevent further unauthorised access. This would apply to both physical security, such as building access, and technical controls, such as ACLs (access control lists) on firewalls, servers, etc.

Recovery and Remediation

The following procedures should be implemented during the remediation phase:

1. Review the options previously determined for reducing or mitigating the risks to data subjects, and implement these where possible. For example, in the event of a hardware failure where data is lost, ensure that as much data as possible is recovered from available backups.
2. Conduct a review of the current technical and organisational measures in place to safeguard the personal data, and ensure that these are still appropriate. Where required, additional measures should be determined and implemented in order to prevent reoccurrence.
3. Where any issues in the handling of personal data or the response to the personal data breach were identified, ensure additional data protection training is conducted with all relevant staff and third parties.
4. Where necessary, monitor system logs more frequently over an initial period to highlight issues arising quickly and remediate where required.

Record and Follow up

The following procedures should be performed immediately after the incident:

1. The designated Data Protection Lead shall document a summary of the personal data breach and record this in the Data Breach Log. Each summary shall contain the facts relating to the personal data breach, its effects, and the remedial action taken. This is required to allow the Data Protection Commission to verify compliance with the GDPR.
2. Where similar data breach incidents have occurred previously, this shall be noted and a plan shall be developed to further assess the incidents, and how these may be remediated. For example, it may be determined that a Data Protection Impact Assessment (DPIA) is required for the processing affected.
3. The Data Breach Log shall be reviewed by senior staff to ensure that the designated Data Protection Lead continues to receive resourcing and support where required.
4. A 'lessons learned' approach should be used to update current incident handling procedures.

Personal Data Security Breach Report Link to Data Protection Commission

Please act promptly to report any data security breaches.

If you discover a data security breach, please follow the instructions at the following link:
https://forms.dataprotection.ie/report-a-breach-of-personal-data

Notes: