General Data Protection Regulation and Medical Practice

Table of Contents

Foreword 3

Acknowledgements 4

1. Introduction 5

2. Important Definitions in the GDPR 7

3. Aspects of the GDPR of Particular Relevance to Healthcare 8

3.1 Transparency 8

3.2 Legal Basis for Processing of Special Categories of Personal Data 8

3.3 Data Subjects' Rights 9

4. Data Controller Obligations 10

4.1 Privacy Policy 10

4.2 Records of Processing Activities 10

4.3 Data Processing Contracts 11

4.4 Data Protection Officer 11

4.5 Security Obligations 12

4.6 Data Breach Notifications 12

5. Sharing Personal Health Data 13

5.1 Sharing Patient Data with Third Parties for Provision of Health Care 13

5.2 Sharing Patient Data with Insurance Companies and Solicitors 14

5.3 Special Considerations when Sharing Patient Data 14

6. Overview of Data Protection Legislation as it Relates to Audit, Service Evaluation & Research 16

Appendix (i) – Frequently Asked Questions 17

1. What are the implications of the Data Protection Legislation on Audit? 17

2. What are the implications of the Data Protection Legislation on Health Research? 18

3. Is it always necessary to obtain consent to use Personal Data when providing medical care? 19

4. What is the impact of the GDPR on transfer of patient samples to international laboratories? 20

5. Are there particular requirements under the GDPR for the transfer children's personal data? 20

6. What precautions can be taken to ensure email communication is GDPR compliant? 21

7. How much technical due diligence must a sole practitioner exercise in selecting a vendor? 21

8. Does the GDPR allow info about conferences to be shared with a network of professionals? 22

Appendix (ii) – Useful References 23

Foreword

"As you will be aware, the General Data Protection Regulation came into force in May 2018. The GDPR is the legal framework that now regulates the collection and use of personal data within the EU.

As doctors, we have always kept privacy as well as patient safety and well-being to the forefront of what we do. Although, to some extent, we are still coming to grips with the implications of these new regulations, it is good to know that the GDPR, with the backing of the regulator and the support of employers, will further enshrine patient privacy in all aspects of the delivery of care.

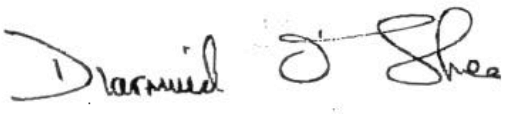
RCPI established the Professional Policy Group for GDPR, with representation from various faculties and trainees, to consider the implications of the legislation for us as practitioners.

The group aims, with appropriate legal input, to establish clarity on doctors' obligations under GDPR, to provide practical guidance for ensuring compliance with the GDPR and to address some of the unintended consequences of the GDPR on medical practice.

The discussion about balancing the patient's right to privacy with the importance of sharing case information will continue for some time. With that in mind, it is intended that this document will be iterative in nature to reflect this reality and the group will continue to meet periodically. Interpretation of the Data Protection Legislation is ongoing and in this regard RCPI would welcome input, feedback and comments so as to facilitate learning, development of training and understanding regarding application of the Data Protection Legislation in the healthcare sector.

If you have any contributions you would like to make to us, please get in touch at dataprotectionofficer@rcpi.ie"

Diarmuid O'Shea, Registrar of RCPI and Chair of the RCPI Professional Policy Group for GDPR



Acknowledgements

Chair	Dr Diarmuid O'Shea (Registrar of RCPI)
Special Advisor	Mr David Byrne (Lay Council Member, former Attorney General of Ireland and former EU Commissioner for Health and Consumer Protection)
Legal Advisor	Mr Colin Rooney (Partner, Arthur Cox)
Project Manager	Ms Yvette Fitzgerald (Data Protection Officer, RCPI)

Group Membership

Dr Anna Clarke (former RCPI Vice President and Censor, Consultant in Public Health Medicine)

Dr Ellen Crushell (Dean of Faculty of Paediatrics, Consultant Paediatrician)

Dr Conor McCarthy (RCPI Censor, Consultant in Rheumatology)

Dr Aine Carroll (RCPI Council Member, Consultant in Rehab Medicine)

Dr Una Fallon (Chair of RCPI Ethics Committee, Consultant in Public Health Medicine)

Dr Mary Keogan (Clinical Lead, National Clinical Programme for Pathology, Consultant Immunologist)

Dr Joan Power (Board Member of Faculty of Pathology, Consultant Haematologist)

Dr Ana Rakovac (RCPI Fellow in Familial Hypercholesterolaemia, Chemical Pathologist)

Dr Louise Hendrick (RCPI Trainee Committee Member, SpR in Public Health)

Dr Sinead O'Donnell (RCPI Trainee Committee Member, SpR in Pathology)

Dr John Gillan (Consultant Pathologist)

Dr Peter Kelehan (Consultant Perinatal Pathologist)

1. Introduction

The General Data Protection Regulation (EU) 2016/679, the Data Protection Act 2018 and the Health Research Regulations 2018 are known collectively as the Data Protection Legislation.

In summary, the GDPR requires the implementation of effective controls across the six privacy principles of:

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

The GDPR is designed to ensure individuals have more control over their personal data and gives them the following rights:

- to be informed about how their personal data will be processed
- access to their personal data and details of how it is processed
- rectification of inaccuracy in a timely manner
- erasure of their personal data ('right to be forgotten')
- to restrict processing of their personal data
- to obtain their personal data and reuse it for their own purposes ('data portability')
- to object to the processing of their personal data
- not to be subject to automated decision making and profiling

The healthcare sector is significantly impacted by the Data Protection Legislation because of the volume of sensitive personal data which is used for the purposes of patient care, related institutional management and scientific research.

This document highlights some areas of the Data Protection Legislation that are of particular relevance to clinicians and aims to be a useful supplement to the information you receive from your employer and the regulator.

In 2017, the Data Commissioner produced the report, *"Data Protection Investigation in the Hospitals Sector"*. A number of the DPC Report's practical recommendations are worth noting and we highlight these recommendations, where relevant, in these Guidelines.

These Guidelines have been published by the Royal College of Physicians of Ireland as general guidance for RCPI Trainees, Members and Fellows on the application of the Data Protection Legislation to the use of patient data in the course of medical practice.

This information is purely for guidance, and does not constitute legal advice or legal analysis. These Guidelines will be reviewed and updated regularly.

2. Important Definitions in the GDPR

Personal Data – means information concerning a living individual who can be identified whether directly or indirectly.

Data Concerning Health – means personal data related to the physical or mental health of an individual which reveal information about his or her health status. This definition includes genetic data, biometric data and information regarding the provision of health care services. The GDPR defines data concerning health as 'Special Category Data' (SCD) and it is, therefore, subject to a higher level of protection.

Data Processing – means any use whatsoever of personal data. This includes collection, organisation, storage, alteration, combining, retrieval, consultation, disclosure, restriction, erasure or destruction of personal data. All processing of personal data requires a legal basis under the Data Protection Legislation (Refer to section 3.2 of this document).

Data Controller – means the party that determines how and why the personal data is processed (i.e. the purposes and means of the processing). For doctors working in a public or private hospital, the hospital is likely to be the controller. The obligations under the Data Protection Legislation apply primarily to Data Controllers.

Data Processor – means an entity that processes personal data on behalf of, and to the instruction of, the controller e.g. a contract lab or a software service provider.

3. Aspects of the GDPR of Particular Relevance to Healthcare

3.1 Transparency

Transparency is a key principle of the GDPR and requires that any information about the processing of a patient's personal data must be easily accessible and easy for them to understand. Data subjects (i.e. patients) must be provided with certain information in relation to the processing of their personal data and it must be provided at the point of data collection.

In addition to the purpose and the legal basis for processing personal data, there are a number of generic points which are best captured in the organisation's Privacy Policy (Refer to section 4.1 of this document).

The DPC recommends that this information can be made available to patients in the form of summary leaflets and posters in the admissions areas of the hospitals. Such notices should also inform patients of the use of their personal data for the purposes such as training, service evaluation and clinical audit as well as letting them know how they can access the Privacy Policy in full and who to contact about any queries relating to personal data (i.e. the DPO)

3.2 Legal Basis for Processing of Special Categories of Personal Data

Under the Data Protection Legislation, you must have a Legal Basis in order to process personal data. Additional conditions are included in the GDPR which allow for the processing of data concerning health:

- preventive or occupational medicine
- medical diagnosis
- provision of health care
- management of health care systems and services
- contract with a health professional
- Public Health
- ensuring high standards of quality of health care
- protection of the vital interests of the data subject i.e. to protect someone's life, where they are not capable of giving consent and it cannot be done is a less intrusive way

Where these legal bases are relied upon, *'suitable and specific measures'* must be taken to safeguard the fundamental rights and freedoms of the patient. The Data Protection Act contains a non-exhaustive list of such suitable and specific measures which, in summary, are:

- limitations on access to personal data
- strict time limits for erasure of personal data
- specific targeted training for those involved
- logging and verification mechanisms that are proportionate to the likelihood and severity of risk to the patients right to privacy
- processing is undertaken by a health practitioner, or someone equally bound by a duty of confidentiality to the patient
- pseudonymisation
- encryption
- explicit consent of the patient

As regards consent, it must be freely given, informed and an unambiguous indication of an individual's wishes. Failure to object does not constitute consent and controllers are required to ensure that they are able to demonstrate that valid consent was obtained. Furthermore, Individuals must be able to withdraw their consent easily and they must be informed of this right to withdraw consent.

Personal data must be kept in a form which permits identification of data subjects for no longer than is absolutely necessary.

3.3 Data Subjects' Rights

Data subjects are provided with enhanced rights under the GDPR. Of particular note to medical professionals are the patient's:

- right of access to information concerning the processing of their personal data and to a copy of any personal data processed (i.e. any personal data in the possession of the Data Controller). The controller must provide the information requested by data subject within one month. That period may be extended by two further months where necessary e.g. due to the complexity of the data gathering exercise.
- right of rectification of any genuinely inaccurate personal data without undue delay.
- right to be forgotten means the right to have any personal data in the possession of the Data Controller deleted. It is not an absolute right and applies only if certain conditions such as the withdrawal of consent or unlawful processing are met.

4. Data Controller Obligations

The obligations of the GDPR rest mainly with the Data Controller. Where a doctor is in private practice, they are the Data Controller. Where a doctor is employed in a hospital, the employer is the Data Controller. The Data Controller is obliged to ensure that there are appropriate technical and security measures implemented within the organisation. While your hospital or organisation will have a duty in helping you to meet these obligations, as a clinician you will still have responsibility for your actions.

4.1 Privacy Policy

Many of the transparency obligations to your patients can be met in the form of a Privacy Policy.

The Privacy Policy must be easy to read and concise while including the following information:

- types of personal data that are collected and stored
- ways in which the personal data will be used (in a medical context this may include the use of data for training, service evaluation and clinical audit as well as the primary purpose of the provision of care)
- any potential categories of third parties with whom personal data may be shared
- the criteria used to determine the data retention period
- the legal basis for the processing
- the data subjects' rights under GDPR
- contact details of the Data Controller
- name and contact details of the Data Protection Officer
- the right to lodge a complaint with the Data Protection Commission

Corresponding to the GDPR transparency obligations, the DPC Report recommends that the Privacy Policy should be freely available to patients in short format e.g. posters or leaflets in waiting rooms and a section on the hospital website. The short format should include basic information and how to access the full Privacy Policy as well as the name and contact details of the Data Protection Officer.

4.2 Records of Processing Activities

Data Controllers in healthcare settings must keep Records of Processing Activities which include:

- name and contact details of the Data Controller and the Data Protection Officer
- categories of data subjects

- categories of personal data
- purposes of the processing
- categories of recipients to whom the personal data have been or will be disclosed
- details of personal data sent to any third country and the documentation of suitable safeguards
- a general description of the technical and organisational security measures

4.3 Data Processing Contracts

Where a Data Processor is used to support the activities of healthcare provision, there must be a contract between the Data Controller and the service provider which includes the following:

- subject-matter and duration of the processing
- nature and purpose of the processing
- type of personal data and categories of data subjects
- obligations and rights of the controller

4.4 Data Protection Officer

Since the core activities of healthcare organisations involve processing data concerning health, they must have a Data Protection Officer (DPO) who has the appropriate skills, expert knowledge of data protection law and due regard to the level of risk associated with processing activities. The role of the DPO is to:

- monitor internal compliance
- ensure staff are trained on Data Protection
- support Data Protection Impact Assessments
- advise on data protection obligations (including obligations as regards health research)
- act as a contact point for Data Subjects and the DPC

The DPO is bound by secrecy and, therefore, should be allowed access to personal data and be properly involved in all issues relating to data protection.

4.5 Security Obligations

Data Controllers and Data Processors are under an obligation to implement appropriate technical and organisational measures to ensure a level of security that is appropriate to the risk. Of particular relevance to healthcare organisations, the DPC recommends the implementation of measures such as:

- pseudonymisation
- encryption
- secure door access to restricted areas
- reviewing swipe care access every six months
- changing key codes periodically
- setting computers to lock automatically
- prohibiting the sharing of user accounts to access personal data
- securely locking filing cabinets used to store personal data

It is prudent to undertake regular information security audits to ensure that appropriate measures to secure patient personal data are in place and that they are effective.

4.6 Data Breach Notifications

A personal data breach means a breach of security that has led to the accidental or unlawful disclosure, alteration, loss or destruction of personal data. If the data breach poses any risk to the patient(s) right to privacy, it must be reported to the DPC. If it poses a high risk to their right to privacy and there are not implementable measures to eliminate the risk, the patient(s) must be promptly informed. In the medical context the level of risk attached to a breach should be carefully reviewed on the basis that a breach is likely to involve data concerning health which is Special Category Data. The Data Controller must maintain a log of all personal data breaches, whether or not they need to be reported.

In line with the GDPR's data breach reporting obligations, the DPC Report recommends that healthcare organisations have a protocol to handle personal data breaches and that all staff are trained accordingly.

5. Sharing Personal Health Data

Before sharing any personal data, ensure that there is clarity with regard to:

- the purpose of the disclosure
- the Legal Basis for the disclosure
- the patient's right to transparency
- the duty of confidentiality to the recipient

5.1 Sharing Patient Data with Third Parties for Provision of Health Care

Medical Diagnostics (e.g. Laboratory)

Internal Laboratory:
When a patient has a consultation with a doctor for the purposes of medical diagnosis or treatment, there is an implied agreement to their personal data being processed because it would not be possible to complete the consultation without the use of patient personal data. This includes laboratory consultation and the use of a referral laboratory where necessary. Of course, patients should be informed of this type of sharing in advance, for example, through the Privacy Policy as described in sections 3.1 and 4.1 of this document.

External Laboratory:
In addition to providing patients with the appropriate level of detail on the use of their personal data, the Data Controller (i.e. the hospital or private practitioner) must ensure that all services are provided on the basis of a written contract and that there is a Data Sharing Agreement in place.

Taking account of the nature of the data processing, the controller must ensure that the processor (i.e. the external lab) has the appropriate technical and organisational measures so as to keep data safe and secure (e.g. the ability to ensure the ongoing confidentiality, integrity and availability of processing services, the ability to restore the access to personal data in a timely manner and a process for evaluating the effectiveness these measures).

International Laboratory:
An additional consideration if the laboratory is in a country outside the EEA is that the controller must ensure that the country in question provides an adequate level of protection e.g. the US Privacy Shield. If the country does not provide the required level of protection, then the Irish controller must use a 'Model Contract' with standard contractual clauses.

Other Medical Professionals

Allowing personal data to be processed (i.e. reviewed) by another health professional who owes a duty of confidentiality to the patient is permissible. However, such data sharing must be transparent and the Privacy Policy should outline the potential for personal data pertaining to health to be

shared in this way. You must ensure that the disclosure is limited to the minimum number of recipients.

Other Hospitals

Sharing patient data with other hospitals is considered processing personal data. Patients should be made aware their health data may be shared with other Hospitals and the general purposes for doing so (e.g. when a patient is being transferred, laboratory services). To the extent the other Hospital is a data controller of the patient data, meaning they hold the patient data for their own reasons, not on behalf of the original hospital, it is prudent to have a Data Sharing Agreement in place that Clearly states that when they share patient data, each will abide by their obligations as data controller, for example in relation to informing the patient of how their data is used.

5.2 Sharing Patient Data with Insurance Companies and Solicitors

While most doctors request consent to share patient data with insurance companies and solicitors as good professional practice, the GDPR does not require that consent for this type of sharing be sought. The GDPR does stipulate however, that only the information that is required by the insurance company or the solicitor to handle the claim or provide the advice is shared and no more. The GDPR also requires that patients are informed of the possibility that their data may be shared with insurances companies and solicitors in the Privacy Policy.

5.3 Special Considerations when Sharing Patient Data

Children's Data

Children's personal data for the provision of a medical service may be shared on the same legal basis as adult personal health data. The GDPR, however, gives specific protection with regard to children's personal data as they may be less aware of the risks, consequences, safeguards concerned and their personal rights. Therefore, as far as reasonably possible, individual patients must be helped to understand that their data shall be transferred.

Email Communication and Data Transfer

As with any processing of data, it is necessary to confirm that appropriate technical and organisational measures, proportionate to the risk to the privacy of the patient are in place.

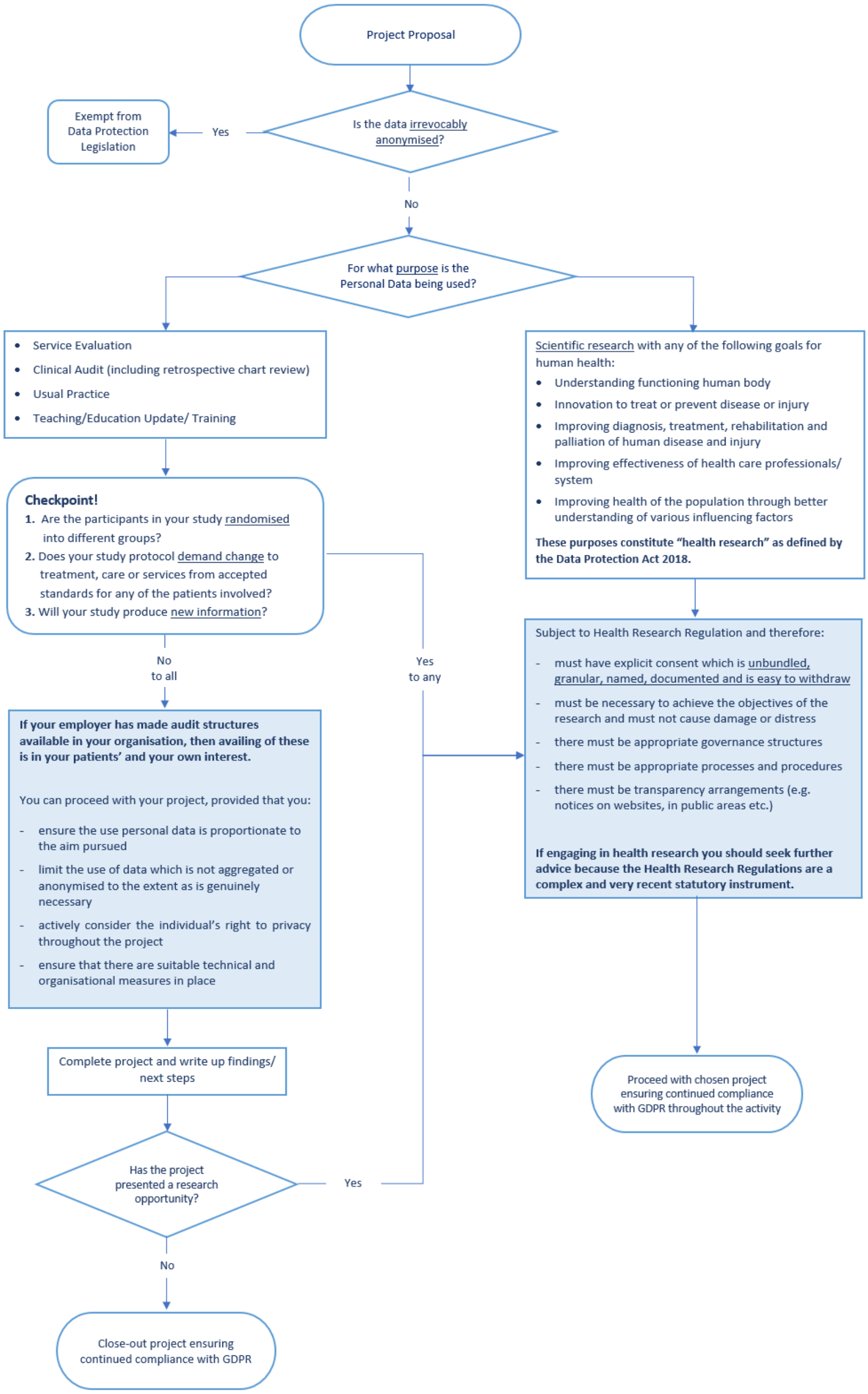
It is recommended that you use the healthmail.ie service provided by the HSE to allow clinical information to be shared between health professionals.

Where the use of healthmail.ie is not feasible, you should encrypt and password-protect your email attachments and send the password separately, preferably via a different communications channel.

A common problem is sending emails to the wrong address, usually arising from human error. Sending personal data to the wrong recipient is a data breach and it is therefore worth minimising the risk of this human error e.g. disabling the auto-complete of e-mail addresses.

If communicating with a patient by email, the authenticity of the email address must be verified by means other than the given email address.

6. Overview of the Data Protection Legislation as it Relates to Audit, Service Evaluation & Research



Appendix (i) – Frequently Asked Questions

1. What are the implications of the Data Protection Legislation on Audit?

Article 9(2) of the GDPR provides that processing of special categories of personal data (to include data concerning health) is permitted where:

> *(h) 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; and*
>
> *(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.*

Section 52 of the 2018 Act provides:

> *(1) Subject to subsection (2) and to suitable and specific measures being taken to safeguard the fundamental rights and freedoms of data subjects, the processing of special categories of personal data shall be lawful where it is necessary— (d) for the provision of medical care, treatment or social care, (e) for the management of health or social care systems and services, or (f) pursuant to a contract with a health practitioner.*
>
> *(2) Processing shall be lawful in accordance with subsection (1) where it is undertaken by or under the responsibility of— (a) a health practitioner, or (b) a person who in the circumstances owes a duty of confidentiality to the data subject that is equivalent to that which would exist if that person was a health practitioner. (3) In this section, "health practitioner" has the same meaning as it has in the Health Identifiers Act 2014.*

Therefore, in accordance with the above mentioned Article 9 and Section 52, it is permissible for patient information to be used for clinical audit and for clinician training to the extent use of such personal data (as opposed to anonymised or aggregated data) is genuinely necessary, whether to improve medical services and standards of practice or for medical educational purposes. Personal data should also be used in such audits only to the extent reasonably necessary.

To the extent reasonably possible, where information is used for audit purposes, the information should be anonymised (i.e. such that a living individual cannot be identified or re-identified). If personal data is used (and even if such data is pseudonymised) the Data Protection Legislation will apply.

From a clinician perspective if your employer has made audit structures available in your organisation, then availing of these is in your patient and your own interest. Availing of the supports provided by your employer will strengthen the design, process and publication of your audit.

Note: If the audit involves or in any way develops into "health research" (as defined in response to Question 2 below), additional and significantly more onerous provisions apply.

2. What are the implications of the Data Protection Legislation on Health Research?

Controllers conducting "Health Research" must take account of the Data Protection Act 2018 (Section 36(2)) (Health Research) Regulations 2018 (S.I. No. 314/2018), as they introduce material changes to the rules governing health research. These Regulations set out mandatory suitable and specific safeguards that apply to the processing of personal data for the purposes of health research and for related matters. These safeguards which arise under the General Data Protection Regulation (GDPR) are separate from the requirements in the GDPR to have a ground in Article 6 and to meet a condition in Article 9.

The term "Health Research" is defined as any of the following scientific research for the purpose of human health:

- Research with the goal of understanding the normal and abnormal functioning of the human body;
- Research specifically concerned with developing innovative strategies, products or services to diagnose, treat or prevent disease or injury;
- Research with the goal of improving the diagnosis, treatment, rehabilitation and palliation of human disease and injury and of improving the health and quality of life of individuals;
- Research with the goal of improving the efficiency and effectiveness of health professionals and the health care system; and
- Research with the goal of improving the health of the population as a whole or any part of the population through better understanding of social, cultural, environmental, occupational and economic factors on determining health status.

Where scientific research involves the processing of SCD (such as data relating to health), Article 9(2)(j) of the GDPR requires that such processing must:

- be proportionate to the aim pursued;
- respect the essence of the right to data protection; and
- provide again for "suitable and specific measures" to safeguard the fundamental rights and interests of the data subject.

The GDPR does not define "suitable and specific measures" but Section 36(1) of the 2018 Act partially does. It provides a non-exhaustive list of suitable and specific measures that may be adopted by controllers where personal data is being processed for research purposes. Section 36(2) also provides for further regulations to be made identifying further suitable and specific measures to those listed in Section 36(1) and/or to specify that certain suitable and specific measures be mandatory in some cases.

If engaging in health research further advice should be sought as S.I. No. 314/2018 is a complex and recent statutory instrument.

3. Is it always necessary to obtain consent to use Personal Data when providing medical care?

In order to process the personal data of a patient you must have a legal basis under the Data Protection Legislation.

Consent is one such legal basis but it is not the only legal basis available for the use of patient personal data. Processing personal data for the provision of medical care is often not based on consent.

The legal basis for processing of data of patients is provided by the following Articles 6 and 9 which work together in the GDPR.

Article 6 provides the grounds for the processing of 'normal' personal data:

> *Article 6.1(b) - processing is necessary for the performance of a contract*
>
> *Article 6.1(c) - processing is necessary for compliance with a legal obligation.*
>
> *Article 6.1(d) - processing is necessary in order to protect the vital interests of the data subject or of another natural person.*
>
> *Article 6.1(e) - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.*

Article 9 provides particular grounds for processing Special Category Data (including health data)

> *Article 9.2(h) - 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.*
>
> *Article 9.2(i) - processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.*

4. What is the impact of the GDPR on the transfer of patient samples and personal data to international laboratories?

The Data Protection Acts Legislation specifies conditions that must be met before personal data may be transferred to third countries (i.e. countries outside the European Economic Area ("EEA")). Organisations that transfer personal data from Ireland to places outside of the EEA will need to ensure that the country in question provides an adequate level of data protection. If the country does not provide an adequate standard of data protection, then the Irish controller must rely on use of approved contractual provisions ("model clauses") or one of the other alternative measures provided for in the Data Protection Legislation.

5. Are there particular requirements under the GDPR for the transfer children's personal data?

Children are provided a specific protection under the GDPR.

Recital 38 of the GDPR states that:

> *"Children require specific protection with regard to their personal data as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data."*

If you rely on consent as your lawful basis for processing personal data when offering an online service ("ISS") directly to children, only children aged 16 or over are able provide their own consent. For use of children personal data outside of ISS the age of consent in Ireland is 18 years. Prior to the child reaching the age of consent, permission for processing of personal data may be given by the parent or guardian (to the extent consent is being relied upon as the legal basis for such processing).

Hence when transferring patient lists from children's hospitals to adult hospitals when the patient turns eighteen, such a transfer must have a legal basis for processing (which may be consent or perhaps one of the other justifications set out in the response to Question 3 above) and the data must be transferred in a secure fashion. Furthermore, it is important that to the extent reasonably possible individual patients understand and are informed that their data shall be so transferred.

6. What precautions can be taken to ensure email communication is GDPR compliant?

The GDPR does not set out specific measures that must be taking when using email to share personal data. However, Article 32 of the GDPR does provide some guidance on the required security considerations when processing personal data and these considerations can be applied to the use of email systems (see also, the response to Question 6).

A common problem is sending emails to the wrong address, usually arising from human error. Sending personal data to the wrong recipient is a data breach that might have to be reported.

To the extent possible you should:

- encrypt and password-protect your email attachments; and

- if using password protection, send the password separately, preferably via a different communications channel.

7. How much technical due diligence must a sole practitioner exercise in selecting a vendor?

Such a vendor is termed a 'processor' under the Data Protection Legislation. Where the clinician engages the vendor it will be doing so as a Data Controller engaging the services of a processor.

The controller must take certain steps to ensure that the data protection standards are maintained. For example, a controller can do business with a processor only on the basis of a written contract which includes appropriate security and other data protection safeguards. The key points that must be set out in the contract in writing between are set out in Article 28 of the GDPR.

Amongst other things Article 28(3) provides that the controller must take into account the "nature of the processing", and ensure the processor has in place "appropriate technical and organisational measures" so as to keep the data being processed safe and secure.

Article 32 of the GDPR set out on more detail what is meant by "security of processing" and therefore what a clinician must consider when engaging a vendor (with our underline emphasis):

> *"(1)Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; 4.5.2016 L 119/51 Official Journal of the European Union EN (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process*

for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

(2) In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed."

It is prudent to undertake regular information security audits on vendors to ensure that appropriate measures are in place to secure patient personal data.

Further guidance from the DPC Report on data security (albeit based on the old law) is set out here:

https://www.dataprotection.ie/docs/Data_security_guidance/1091.htm

8. Does the GDPR allow information about conferences to be shared with a network of similar professionals?

Individuals have a right to object at any time to processing of personal data for direct marketing purposes, in which case the personal data shall no longer be processed for such purposes. The key point in relation to this kind of communication is to respect the preferences of the recipients within the network. It is important to include an opt-out from future such messages in each such communication and it is vital to respect any opt-out or similar preferences expressed by recipients of such messages.

Appendix (ii) – Useful References

"A Data Protection Investigation in the Hospitals Sector" ODPC, 2018.

"Defining Research" Health Research Authority (UK), 2017.

"Is my study research?" MRC Regulatory Support Centre (UK), 2017. www.hra-decisiontools.org.uk/research/