A Guide to Data Protection Legislation for Irish General Practice

Data Protection Working Group

April 2011

A Guide to Data Protection Legislation for Irish General Practice

Data Protection Working Group ~ *April 2011*

TABLE OF CONTENTS

Foreward

by Mr Pat O'Dowd, Chairperson of the National General Practice Information Technology (GPIT) Group

Practising medicine in the twenty first century is becoming increasingly complex. Not just in terms of the expanding knowledge base required by general practitioners and the need to keep up to date with clinical advances, but also with the regulatory environment in which general practitioners work. It is hard to be an expert in family practice and in data protection.

This Guide to Data Protection Legislation for Irish General Practice is intended to be a reference to GPs, something they download from the Internet or pull down from a bookshelf when a question related to information sharing or information access arises.

The aim of the National General Practice Information Technology (GPIT) Group is to support information technology in general practice and to promote interoperability between information systems in the health service. I am delighted that GPIT had the opportunity to work with the Irish College of General Practitioners and the Office of the Data Protection Commissioner to bring this Guide to fruition. I would particularly like to thank Dr Brian Meade who led the Data Protection Working Group to successful completion of its work.

This Guide contains a wealth of information. It is logically laid out, easy to read and will be an important reference document for general practice. I commend it to you.

Pat O'Dowd
Chairperson of the National General Practice Information Technology (GPIT) Group

1 Purpose of this guide

In November 2003, the Irish College of General Practitioners and the National General Practitioner Information Technology (GPIT) Group published a comprehensive guidance document *Managing and Protecting the Privacy of Personal Health Information in Irish General Practice – An information guide to Data Protection Acts for General Practitioners*. A Working Group was established in early 2010 following the discussions between the Office of the Data Protection Commissioner and the ICGP in response to the findings of the Office of the Data Protection Commissioner following audits it carried out on a number of GP practices. It was felt that it would be opportune to assist GPs in meeting their obligations under the Data Protection Acts while also updating the guide to take account of emerging issues.

This revised document therefore attempts to provide GPs with a straightforward and easy to use guide to Data Protection legislation. It has been structured to present data protection considerations in order of how information flows through a GP practice from the time it is first collected and how that should be undertaken. It then moves on to discuss the legal principles in relation to how information should be used within a practice and when it can be released to third parties as well as how it should be stored and retained. Advice as to access by patients to their own information is also provided. The document also draws on guidance from other sources such as the Irish Medical Council and medical protection agencies to assist GPs in making compliant decisions when faced with the many challenges regarding the use and sharing of medical records which GPs hold. A number of sample documents for use in GP Practices are also appended.

1.1 Members of the Data Protection Working Group

The members of the working group are

Dr Brian Meade	National GPIT Training Coordinator
Dr Brian O'Mahony	Health Informatics Specialist and GPIT Project Manager
Dr Anne Lynott	GPIT Facilitator
Mr Gary Davis	Deputy Data Protection Commissioner
Ms Ciara O'Sullivan	Office of the Data Protection Commissioner
Mr Dermot Folan	Chief Operating Officer Irish College of General Practitioners
Ms Margaret Cunnane	Administrator – ICGP Management in Practice Programme

2 Legislation governing the handling of patient information

The legal protection of an individual's private information is protected by a number of legal sources from the constitution down. In practice however the Data Protection Acts of 1988 and 2003 are the most relevant when it comes to General Practice records. The Freedom of Information Acts of 1997 and 2003 provide access to both personal and non-personal records and may also have relevance to some types of medical records as outlined in section 2.4 below.

2.1 Data Protection Legislation

Data protection is about a person's fundamental right to privacy. The Data Protection Acts 1988 and 2003 set out responsibilities for those who hold data about people (in both electronic and manual form) which they have to comply with and provides individuals with the right to access and correct data about themselves. The Acts set out the general principle that individuals should be in a position to control how data relating to them is used.

2.2 The Data Protection Commissioner

The Office of the Data Protection Commissioner is established under the 1988 Data Protection Act. The Data Protection Amendment Act, 2003, updated the legislation, implementing the provisions of EU Directive 95/46. The Data Protection Commissioner is responsible for upholding the rights of individuals as set out in the Acts, and enforcing the obligations upon data controllers. The Commissioner is appointed by Government and is independent in the exercise of his or her functions. Individuals who feel their rights are being infringed can complain to the Commissioner, who can investigate the matter, and take whatever steps may be necessary to resolve it. Further information on the specific legal powers of the Data Protection Commissioner to enforce compliance with the legislation is available on the Office's website, www.dataprotection.ie. Powers of the Commissioner include the power to audit organisations and the power to issue legal notices to ensure compliance with the provisions of the legislation.

The Data Protection Acts provides the following penalties for offences:

- on summary conviction, to a fine not exceeding €3,000, or
- on conviction on indictment to a fine not exceeding €100,000

The Court may also order that some or all of the information connected with offences under the Acts to be erased, forfeited or destroyed. Further, the Acts do not preclude an action at common law in relation to the mishandling of data, such as defamation, negligence, or breach of privacy.

2.3 Registration with the Data Protection Commissioner

Under the Data Protection Acts 1988 and 2003 certain categories of data controllers and data processors must register details with the Data Protection Commissioner. Registration must be renewed on an annual basis. Section 16 of the Data Protection Act 1988 requires persons to register if they record details on computer relating (in a health context) to the physical or mental health of identifiable individuals. Most GPs are covered under this category, to the extent that they record their patients' medical details on a computer. Any doctor who does not keep such computer records would not be required to register. Registration can be completed online on the website of the Office of the Data Protection Commissioner *www.dataprotection.ie*. Under Section 19(6) of the Data Protection Acts, it is an offence for a data controller to keep personal data unless they are registered. The requirement to register is one that lies with the legal entity responsible for patient data. In a single doctor practice it is that doctor or in a multiple doctor practice it would be the legal entity responsible for the practice.

2.4 The Freedom of Information Act 1997

The most important difference between Freedom of Information (FOI) legislation and the Data Protection acts is that freedom of information has no impact on GPs records of private patients. They do however cover records which are generated on behalf of a government body. For this reason the patient records of GMS patients are covered by the act as are immunisation and some maternity records. Requests for access to records under freedom of information also differs from the Data Protection Acts. In the case of FOI, the request for access must be made in writing to the head of the public body concerned which in the case of a GMS medical record is the HSE.

There are similar provisions under the two pieces of legislation where access to a medical record can be denied if it was felt that disclosure to the individual would result in harm to his or her physical or mental health. The threshold for refusal is generally considered to be lower in the case of Freedom of Information legislation.

3 Data Protection Principles

There are a number of key responsibilities in relation to the information which can be kept on computer or in a structured manual file about individuals. These may be summarised in terms of eight rules or principles. There is a legal obligation on Data controllers (in this case GPs or the practice) to adhere to these eight principles when dealing with patient information.

The principles state that the Data Controller must:

1. Obtain and process the information fairly
2. Keep it only for one or more specified and lawful purposes
3. Process it only in ways compatible with the purposes for which it was provided
4. Keep it safe and secure
5. Keep it accurate and up-to-date
6. Ensure that it is adequate, relevant and not excessive
7. Retain it no longer than is necessary for the specified purpose or purposes
8. Give a copy of his/her personal data to any individual, on request

These provisions are binding on every data controller. Any failure to observe them would be a breach of the Act.

To put these principles into the context of General Practice it is useful to look at each one individually and see how it impacts on the day to day running of a practice and how the principle can help guide the GP into making the correct decision in dealing with data protection problems.

4 Principle – Information should be obtained and processed fairly

4.1 Patient consent to collecting information

GPs are required to inform patients of what use will be made of their data including if it will be stored on computer. This can be covered in a patient information leaflet or patient privacy statement (see Appendix 2). In general, the patient should be aware of the following:

- What information is being collected?
- Why the information is being collected?
- Who within the practice will have access to the information?
- How the information will be used?
- The consequences of not providing the information
- What third party disclosures are contemplated, if any?
- That he or she can have access to the information, once collected

A good general question to for GPs to consider is "would my patients be surprised by any of the uses we are making of his/her information?"

Areas where patients may be surprised are:

1. The extent to which confidential information is passed on to insurance companies when completing a PMA.
2. Use of patient consultation notes in teaching medical students.

Both of these issues are addressed below.

Wherever it is reasonable and practicable to do so, personal health information about a patient should be collected directly from the patient rather than from third parties.

4.2 GPs acting as medical advisor or occupational health physicians

Sometimes GPs will interview and examine a patient where they are acting on behalf of an insurance company or an employer. It is important in these cases that the patient is fully aware of the nature and context of this type of consultation. In particular the patient should understand that the GP is acting on behalf of the company or employer and that the information gathered will be used to furnish a report. Misunderstandings can easily arise here if the patient also attends the same GP for ongoing care and records in the possession of the GP in such a context should not be consulted to prepare such a report.

5 Principle – Information should be kept for one or more specific and lawful purpose

In general this principle should hold no difficulty for GPs as information is collected for the purpose of providing medical care. If however the patients' names and addresses were used for a purpose which was unrelated to the provision of medical care, then this might be considered an illegitimate use of the patient information.

There are a number of areas in General Practice where use of the data could be considered in breach of this principle and therefore extra care is required. These include the following:

5.1 Provision of Private Medical Attendant Reports for Insurance Companies

The completion of private medical attendant reports for GPs on behalf of their patients has long been an area of concern. In many cases patients do not appear to be aware of the extent of information sought about their health by the insurance companies. Nor do they appear to be aware of the implications of adverse health information and that insurance companies are allowed to share "adverse" health information with each other. GPs can easily get caught up in a dispute between patients and their insurance companies and patients can feel angry that GPs have disclosed information to insurance companies even though they have provided consent. In order to protect the GP and the patient from the negative effects of this practice the GP should:

- Ensure written consent is provided with every request for a PMA report.
- Not send actual copies of recorded consultations.
- Not send specialist reports even if these are requested by the company. These can be sought together with an opinion on their relevance from the specialist separately if the company so wishes.
- Include in your patient information leaflet the fact that medical information is passed on to insurance companies (as is standard practice) on receipt of a signed consent form by the patient.

Some GPs offer patients the opportunity to review their PMA report before it is returned to the insurance company, particularly if it is likely to have a negative impact on their insurance risk. GPs may wish to consider

this action, where they have concerns that the patient has consented to what may be considered excessive disclosure of their information, to ensure the patient fully understands the nature of the consent provided.

In the completion of PMA reports it is important that GPs do not suppress or omit information in order to help patients avoid financial "loading" by the insurance company. To do so would make the policy invalid and could leave the GP exposed to legal action. If patients are unhappy with the terms offered based on medical information provided by the GP they should be referred to the chief medical officer of the insurance company in the first instance and failing this, the Financial Services Ombudsman *www.financialombudsman.ie* and\or the Equality Authority *www.equality.ie* who may be able to help.

5.2 Genetic Testing and Insurance Companies

The Disability Act 2005 prohibits the use of genetic test results by insurance companies to assess clients for a range of products including life assurance, permanent health insurance and pensions. Application forms for these products should not include any questions about genetic testing and GPs should not submit any information to insurance companies on the results of genetic tests even if these are favourable.

5.3 Medico-legal reports

General Practitioners can be asked to provide a copy of the patient's medical records to a Solicitor under section 4 of the Data Protection Acts where the patient is making a personal injury claim through that solicitor. Although the request for a copy of the records is usually accompanied by a signed consent form, it is good practice to confirm with the patient that they are aware this request has been made and that the entire medical record has been requested.

With the patient's consent, it should be possible to release only that portion of the record which is relevant to the legal claim.

5.4 Teaching of medical students

There is now a move towards the training of medical students in primary care rather than in a hospital setting. While this is a long overdue and worthwhile development, it may come as a surprise to patients attending their GP. For this reason it is important that the patients are informed by means of a patient information leaflet and\ or waiting room notice that the practice is involved in the teaching of medical students and that patients may be asked to allow students to sit in on their consultation with the GP.

In general medical schools in this country emphasise strongly the importance of patient confidentiality when training their medical students. In some cases, medical students will be asked to sign a patient confidentiality agreement with their medical school at the start of the clinical attachments which will cover their General Practice attachments also. Where there is no such confidentiality agreement in place, consideration should be given to a practice confidentiality agreement for medical students. A sample confidentiality agreement form is provided in Appendix 7.

5.5 Research

5.5.1 Legislative Position

The position in regard to the use of medical records is outlined in a document entitled *Data Protection Guidelines on research in the Health Sector* published by the Data Protection Commissioner in 2007. In the document, the Commissioner makes clear that data privacy legislation does permit the use of patient data by a data controller for

> *"medical purposes which include research where the processing is being undertaken by a health professional or other person owing a similar duty of confidentiality to that patient, providing this is done in a manner that protects the rights and freedoms of the patient. This can mean the data being anonymised or the patient giving an unambiguous consent to their data being used for specified research purposes"*

The Acts also provide an exemption for the use of patient data by their own GP or practice for the purpose of research or audit where there are no disclosures of personal data to outside third parties.

5.5.2 Consent and Research

GPs or practices who carry out internal audits on their own practice population can do so without seeking specific consent from the patient. The need for explicit consent can also be avoided during a research project if it is possible to anonymise the data so that individual patients can not be identified. In both cases however it is important to inform patients that the practice may

use data for internal audit or research and offering them the option of opting out of this use of their data. This can be included in a patient information leaflet or privacy statement (see Appendix 2). For all other forms of "external" research, explicit consent from the patient is required. It is not acceptable for external research staff to trawl through individual patient records without informed patient consent. It is also not acceptable to release the contact details of patients to researchers without informed patient consent. Further information on this area is available in a document entitled *Data Protection Guidelines on research in the Health Sector* which can be downloaded from the web site of the Data Protection Commissioner. Ethical approval from a relevant and authorised body should also be sought in the case of external research projects.

Care needs to be taken when rendering data anonymous, as depending on the nature of the illness and profile of the patient, there may be instances in which the individual can still be identified. This might occur for example with small groups of patients or those with rare conditions.

5.6 Continuing Professional Development

The use of case histories for discussion within a small group of GPs for the purpose of continuing education can be a very valuable educational tool. Where the patient cannot be identified, explicit consent is not required.

6 Principle – Information should be used and disclosed only in ways compatible with the reasons for which it was obtained.

6.1 Using and disclosing personal health information

As a general rule, personal health information should only be used for the purpose for which it was collected. In General Practice the patient's information is used for a variety of functions including identification of individuals for screening or prevention, generating referral letters, repeat prescribing etc. Most of these will be self evident to patients who come to the practice to avail of its services.

Additional uses or disclosures are permitted where:

- The patient concerned has explicitly consented to the proposed use or disclosure .
- The medical practitioner reasonably believes the use or disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's life, health or safety, or a serious threat to public health.
- The disclosure is required or authorised by law.
- The information concerns a patient who is incapable of giving consent, and is disclosed to a person responsible for the patient to enable appropriate care or treatment to be provided to the patient.

6.2 Access by secretarial and administrative staff

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

- Identifying and printing repeat prescriptions for patients. These are then reviewed and signed by the GP.
- Generating a social welfare certificate for the patient. This is then checked and signed by the GP.
- Typing referral letters to hospital consultants or allied health professionals such as physiotherapists, occupational therapists, psychologists and dieticians.
- Opening letters from hospitals and consultants. These could be clinic letters or discharge letters. The letters could be appended to a patient's paper file or scanned into their electronic patient record.

- Scanning clinical letters, radiology reports and any other documents not available in electronic format.
- Downloading laboratory results and Out of Hours Coop reports and performing integration of these results into the electronic patient record.
- Photocopying or printing documents for referral to consultants, attending an antenatal clinic or when a patient is changing GP.
- Checking for a patient if a hospital or consultant letter is back or if a laboratory or radiology result is back, in order to schedule a conversation with the GP.
- When a patient makes contact with a practice, checking if they are due for any preventative services, such as influenza vaccination, pneumococcal vaccination, ante natal visit, contraceptive pill check, cervical smear test, overdue childhood vaccination, etc.
- Handling, printing, photocopying and postage of medico legal and life assurance reports, and of associated documents.

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

In the future it is hoped that GP Management software will provide an audit log of when patient information has been accessed, and by whom. When such a log is available it will be possible for the data controller in a practice to detect any unauthorised access to personal health information.

6.3 Primary Care Teams

It is recognised that the development of primary care teams and other multi-disciplinary structures provide the opportunity for the provision of a wider range of, and more integrated, patient services either in a single healthcare centre or otherwise. The services of primary care teams may be delivered from a number of centres or locations, as local circumstances and needs dictate. Equally, group and partnership practices allow general practitioners to come together and pool clinical and administrative resources for enhanced patient care.

In order for the concept of integrated care involving a number of members of a primary care team to work effectively, the sharing of certain personal health information may well be necessary for proper patient treatment. The GP is often the source of key personal and medical information for other members of the primary care team and at team meetings. This creates a number of challenges for GPs because on the one hand the GP is anxious to seek the advice and assistance of other primary care team members but on the other has a duty to protect the patient's privacy.

A HSE working group consisting or GPs, primary care team members, experts in data privacy legislation and representatives from patient groups considered the issue of information sharing in 2009. They came up with an agreed set of guidelines to be followed by all primary care teams entitled *Interim Guidelines on Information Sharing in Primary Care Teams*. These guidelines include the following:

- **Consent:** The consent of the patient is required when there is a material change in the anticipated use or disclosure of confidential healthcare information. Sharing of such information among primary care teams would constitute a material change and therefore when a GP becomes part of a primary care team and intends sharing information among team members, consent is required. For consent to be valid it must be informed and freely given, therefore the type of information collected and held by all members of the primary care team should be made known to the patient and circumstances in which this information is shared within the team made known.
- **Information Sharing:** Information sharing is often related to the concept of "need to know". This is a concept that can be difficult to define. Information sharing within primary care teams is more appropriately linked to "duty of care" to the patient. If a team member is not providing care then he or she should not have access to healthcare records. Where both a role and a "duty of care" exist, then only relevant parts of the confidential healthcare record should be accessible.
- **Team meetings:** Whereas team meetings can be extremely valuable in formulating and implementing care plans for patients they can present risks to patient's privacy and confidentiality. Written patient consent should be in place prior to clinical team meeting and the patient should understand what information will be discussed and who will be present at the meeting. Notes of the team meeting should only be shared with colleagues who

have a duty of care arising from the meeting. No general clinical team meeting minutes containing confidential healthcare information should be circulated after the meeting. If minutes are required then the patient information should be anonymised.

- **Referral:** Where a GP is seeking the advice or support of another member of the primary care team regarding a patient the referral method used should be the same as that to a hospital colleague. The referral letter or form should contain selective abstracts of the patient record relevant to the other health care professional. Open access to a shared health record is not appropriate within a primary care team setting.
- Patients who refuse to allow their personal information to be discussed at multi-disciplinary team meetings will need to be made aware of the possible consequences of this decision and that it might affect the types and range of therapies that are provided to them.

6.4 Locums and GP Registrars

Making clinical records available to a locum GP, acting on behalf of the regular GP, so that they may provide medical care to patients, is compatible with the purpose for which the general practitioner keeps the patient record.

6.5 Staff provided by Pharmaceutical Companies

On occasions, staff provided by Pharmaceutical companies offer to help identify and interview patients at risk of particular illnesses. Even though the individual provided by the Pharmaceutical company may well be a qualified nurse or pharmacist, they are not part of the practice team and therefore do not have an automatic right of access to the patient records. As this would be considered a change of use of the medical records, explicit consent is required from the patients concerned in order to use the medical records in this way. This consent would need to be in place even to allow names of patients etc to be provided to such individuals acting on behalf of Pharmaceutical companies.

6.6 Patient transfer to another doctor

Where a patient decides to transfer to another doctor, the existing doctor should, in accordance with data protection law and ethical guidelines, facilitate that decision by making available to the patient's new doctor a copy of the patient's health records. This should only be done after signed consent from the patient is obtained. The existing doctor should, however, maintain a copy of the record for an adequate future period consistent with medico- legal and other professional responsibilities. During that period, the provisions of the Data Protection Acts continue to apply to that information. A sample request form for use when requesting notes for a new patient from the previous GP is provided in Appendix 8.

6.7 Change of GP within an existing practice

In cases where a medical practice is taken over by a new medical practitioner or a new medical practitioner joins an existing group practice, a question arises as to whether the new medical practitioner can have access to the patient records of the practice. Access is only appropriate where the patient concerned has given consent. Generally, consent can be implied from the fact that the patient has sought a consultation with the new medical practitioner.

6.8 Retirement, Death or Closure of a GP Practice

When a single handed GP ceases practice due to retirement or death and no GP is due to take over the practice, the retiring GP (or executor in the case of the medical practitioner being deceased) should take prompt and reasonable steps to notify patients and allow them the opportunity to transfer their medical records to another provider. If any patient cannot be contacted or does not respond, within a reasonable period, the medical practitioner (or executor) should maintain the records with due safeguards for a period of eight years and then securely destroy them.

In the case of GMS patients, the HSE will appoint a replacement GP to take over the "panel" of patients and the records can then be transferred to the new GP. In some cases the patient list will be "frozen" until a replacement GP is found so that it will not be possible for a patient to move to a new practice until this occurs.

In the case of a retirement or death within a partnership or group practice, the practice should inform the patients of the general practitioner involved of the retirement or death and advise that their medical record is being retained within the practice for their continuing care. Where the patient advises that he or she wishes to transfer to another practice then this request should be facilitated in the normal way.

6.9 Sale of a GP Practice

Where a practice has been sold to another practitioner, all patients should be notified as soon as possible after the sale is agreed but before the practice changes ownership so that patients have the opportunity to move from the practice to another provider if they wish.

Notification should ideally be by means of a letter which offers the patient the choice to remain with the practice or have their records sent to another GP of their choosing. In the event of the patient not responding within one month of being so advised, it can be presumed that he or she is satisfied that their records should remain with the practice and the new general practitioner.

7 Principle – Information should be kept safe and secure

7.1 Security Measures

GPs need to take reasonable steps to protect their medical records from loss, misuse or unauthorised access. There are a number of ways in which the medical records can be protected. These include:

7.1.1 Physical measures

- In the case of manual record systems, ensuring that there is no general access from the waiting room or other public areas of the practice to the filing room.
- Filing rooms and filing cabinets should be locked when not in use.
- Access to computer servers should be restricted and should not be accessible from public areas of the practice.
- Computer servers should be kept in cool well ventilated rooms and fitted with surge protectors and an auxiliary power supply to prevent data loss due to power surges or failure.
- When disposing of obsolete or redundant equipment many data controllers offer the equipment for sale to staff or donate it to charities. It is the responsibility of the data controller to ensure that all data previously stored on the devices has been removed prior to disposal. It is not sufficient to merely re-format the hard drives of the devices, as data can still be retrieved. Software is available that will overwrite the contents of the hard drive with a series of 1's and 0's to ensure that previous data can not be retrieved. Dependant on the nature of the data stored, it is recommended that hard drives should be overwritten between three and five times. There are a number of companies based in Ireland which offer secure and permanent hard drive destruction to clients wishing to permanently destroy sensitive information held on computer.

7.1.2 Electronic measures

- Access to the computer's operating system and practice software should be password protected.
- A user registration and removal policy should be put in place.

- Appropriate internet security software should be installed.
- A robust backup procedure should be in place so that if data is corrupted or lost, a recent copy of the electronic patient records will be available.
- Security updates and software patches should be regularly installed.
- In future, GPs management software will provide an audit trail of which records have been accessed by different users of the system. This should allow the data controller to ensure the patient records are not being accessed inappropriately.

7.1.3 Human measures

Sometimes we rely too heavily on mechanical and electronic measures at the expense of more basic measures such as good staff training. Training of practice staff should include:

- How to use the computer and software effectively.
- What to do and who to ask when faced with a problem.
- How to create a good password, change it regularly, keep it safe and not share it with others in the practice.
- An overview of the importance of patient confidentiality so that patient information is never given out inappropriately, especially over the phone.
- An understanding that neither fax nor e-mail are secure methods of transferring patient information. Although faxing is in use as a means of urgent information exchange in General Practice, its use should be kept to a minimum.

Inappropriate use of the Internet at work also poses a significant risk to the security of electronic patient records. Staff should be aware of the dangers of accessing certain web sites and should only access the Internet at work where it is required for the running of the practice. It is useful to have a clear policy for staff, locums and others outlining what you consider to be appropriate use of the internet. A sample Internet Security Policy for GPs is available from the GPIT website at www.gpit.ie

7.1.4 Laptops and USB Storage Devices

Laptops and other portable devices are now increasingly in use in general practice for managing patient records. They are also however much more prone to theft than desktop computers. It is important therefore to ensure that any patient records contained on these computers are encrypted. Portable computers should not be left unattended or if this unavoidable, they should be securely locked where they are going to be used.

In the same way that portable computers can be easily lost or stolen, USB storage devices are even more at risk. For this reason no identifiable patient information should be held on USB memory keys. Further guidance is available on the website of the Data Protection Commissioner in relation to security and obligations that arise in the event of a data security breach.

7.1.5 Use of Fax Machines

Where possible, transmission of personal health information by fax should be avoided. Where medical information is required urgently and a more secure mechanism is unavailable the following measures should be considered:

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

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

7.1.6 Use of e-mail

Documents sent by e-mail are not secure and can be accessed inappropriately by others before reaching their intended recipients. For this reason personal health information should not be transmitted by GPs to hospitals and other health providers by e-mail unless it is encrypted or a secure electronic pathway has been established between the GP and the secondary health provider.

7.1.7 Use of Short Message Service (SMS) communication

The use of text or SMS messages to patients can appear an efficient and attractive way of communicating with patients. There are difficulties however with sending confidential information in this way as text messages can be read by others and mobile phone numbers can change. It is advisable therefore to restrict messages by text to non clinical matters such as appointment reminders or notifications that test results are back. Patient consent is required in order to communicate with patients by means of text messages.

7.2 The Internet

Use of the internet is rapidly becoming a useful tool for General Practitioners. With the many benefits however it also brings increasing threats to the integrity and security of patient data. As mentioned above, the use of an appropriate internet security package can go a long way towards protecting data from malware such as computer viruses.

A firewall is a physical device or software application which protects against unauthorised access from outside the practice network and is also essential. A detailed guide on information security for GPs entitled *No Data No Business* is available from the GPIT website *www.gpit.ie*

7.3 Online hosting/ backup

A number of companies are now offering GPs the opportunity to backup their medical records on a remote server using a broadband internet connection. The method has a number of advantages over traditional methods as it does not rely on a member of the practice having to remember to replace discs or cartridges on a daily basis and it ensures a copy of the records exist outside of the practice premises.

In relation to the company that is to provide online backup services to a GP practice, there should be a contract in place which clearly describes the duties and role of the company in protecting access to the data and stipulates what would happen in the event of the company being taken over by another company or going out of business. Practices using online backup services should also inform patients of this in their practice information leaflet.

Personal health information can be transferred to an individual or organisation outside the European Economic Area only in certain specified circumstances. Further guidance on this is available from the website of the Office of the Data Protection Commissioner *www.dataprotection.ie*

Particular care should be taken where a GP is using a third party to host or store patient data. Such a third party is a data processor hosting personal data on behalf of the GP or the practice and there is a requirement for a formal legal contract to be in place which guarantees the patient information will remain confidential. The GP should ensure that the third party is not further transferring the data to another party for hosting or storage as the GP would no longer be in control of the data and therefore would be in breach of the Data Protection Acts.

8 Principle – Information should be accurate, complete and up to date

High quality and safe medical care relies upon accurate and reliable medical records. Ideally a system should be in place to continually update patient details, medical history, medications and allergies as these change.

Patients may occasionally bring to the attention of the practice their concerns about information held about them. They have rights of correction, rectification, erasure and blocking in relation to information held on them that is not in keeping with the principles of the Data Protection Acts, for example, inaccurate, non-relevant, excessive information etc.

Where the request for alteration is straightforward and not in dispute, for example, amending an address or telephone number, GPs should agree to the change as a matter of course. In other cases, particularly as regards whether the information is excessive or not relevant, the GP should exercise his or her professional judgement and explain the reasoning to the patient as well as outlining that the patient may bring the matter to the Data Protection Commissioner for resolution if they are still not satisfied.

As a rule, with every request for alteration or correction, the GP should annotate the record to indicate the nature of the request and whether or not they agree with it. For legal reasons, it is inadvisable to attempt to alter or erase the original entries in a medical record, and in some circumstances it may be unlawful to do so.

Where information has been materially and significantly enhanced, corrected, amended, blocked or deleted, there is a requirement to notify any person to whom it was disclosed within the previous 12 months unless such notification proves impossible or involve disproportionate effort.

Although GPs with manual record systems are not currently required to register with the Data Protection Commissioner, they are obliged to ensure that their processing of personal data complies in full with the requirements of the Acts.

High quality records are:

- Organised by the practice in a manner that minimises the potential for one person's information getting confused with another.
- Documented, dated and well organised for efficient retrieval including for advising the individual of preventative services provided by the practice.
- As detailed as necessary.
- Accurate and current to the greatest extent possible.
- Comprehensible and legible.

It is good practice to ask patients to review the information contained about them on a regular basis particularly their registration information, medical history and allergies to ensure that these are up to date and accurate.

9 Principle – Information should be adequate, relevant and not excessive

This provision is difficult to interpret in the context of General Practice as it is a matter of opinion what information is relevant and what is not in the day to day work of a GP. There will always be possible reasons why highly sensitive information such as sexual orientation and religious beliefs could be seen as relevant but the provision does impose a duty on the GP to only collect the information he or she feels is necessary to adequately manage the patient's problems. This will vary on a case by case basis.

9.1 Personal Public Service Number (PPSN)

The Office of the Data Protection Commissioner acknowledges that entities such as the Department of Social Protection or the HSE are legally permitted to seek the PPSN in the context of the provision of a service. In each case, the requests must be justifiable and the capture of the PPSN must not be made on a "just-in-case" basis or be used as a practice identifier. This latter point is of particular importance as any use of the PPSN by a GP that is beyond that required by the HSE may leave the GP open to legal action under the provisions of the Social Welfare Acts.

10 Principle – Information should be retained no longer than is necessary

In general, medical records should be retained by practices for as long as is deemed necessary to provide treatment for the individual concerned or for the meeting of medico-legal and other professional requirements. At the very least, it is recommended that individual patient medical records be retained for a **minimum** of eight years from the date of last contact or for any period prescribed by law. (In the case of children's records, the period of eight years begins from the time they reach the age of eighteen).

While there are no specific periods defined for record retention for Irish General Practice there are guidelines available for other services within the HSE, which were published by the National Hospitals Office in 2007. These guidelines suggest **minimum** retention periods as follows:

PATIENT TYPE	MINIMUM DURATION
General (Adult)	8 years after last contact
Deceased patients	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. If the illness or death could have potential relevance to adult conditions or have genetic implications, the advice of clinicians should be sought as to whether to retain the records for a longer
Mentally disordered persons (within the meaning of the Mental Health Acts 1945 to 2001)	20 years after the date of last contact between the patient/client/service user and any healthcare professional employed by the mental health provider, or 8 years after the death of the patient/client/service user if sooner
Death - Cause of, Certificate counterfoils	2 years
Maternity (all obstetric and midwifery records, including those of episodes of maternity care that end in stillbirth or where the child later dies)	25 years after the birth of the last child
Records/documents related to any litigation	As advised by the organisation's legal advisor. All records to be reviewed. Normal review 10 years after the file is closed
Suicide – notes of patients having committed suicide	10 years

11 Principle – Individuals are entitled to a copy of their personal data

Under data protection legislation, patients are entitled to get a copy of their medical records whether these are held on computer or on a manual record system. Patients wishing to do so are required to submit the request to the data controller (GP or practice manager) in writing. They are not required to give a reason for the request. A fee of no greater than €6.35 can be charged for this by the practice and the records must be provided to the patient within 40 days.

In general it is good practice to discuss the content of the medical record with the patient thereby avoiding any need to make a formal access request however there are a number of circumstances where a GP can legitimately refuse access to part or all of the medical record. These would include the following:

11.1 Potential harm to a patient

The Data Protection (Access Modification) (Health) Regulations 1989 allows for the refusal of access to the medical record if the disclosure of the record to the patient "would be likely to cause serious harm to the physical or mental health of the data subject". This decision is to be taken by the data controller if he or she is a health professional and suitably qualified to assess the likely impact on the data subject of the release of his health records. If he or she is not so qualified the decision has to be made in consultation with an appropriate health professional.

In any situation where access is denied, the general practitioner must advise the patient of the reason invoked for the restriction either at the time access is denied or as soon as is advisable thereafter. In addition, only the part of the medical record likely to cause harm can be withheld, the rest of the medical record should be released in the usual way.

11.2 Access by parents and guardians

It is considered that where a person is 16 years or older, he or she can independently of a parent or guardian exercise the right of access to personal information established under the Data Protection Acts. Significantly, he or she would also be considered to have the right to refuse access to their medical record by a parent or guardian. Where the individual is below that age, the general practitioner should exercise professional judgement, on a case by case basis, on whether the entitlement to access should be exercisable by (i) the individual alone, (ii) a parent or guardian alone, or (iii) both jointly. In making a decision, particular regard should be had to the maturity of the young person concerned and his or her best interests.

11.3 Third Party Information Provided on a Confidential Basis

Providing details to the patient on the source or sources of the personal information held is required unless the communication of that information would be contrary to the public interest. The exception may mean not only that the name of the source is withheld but that any information contained in the medical record that might identify the sources can also be denied.

In addition, it may be that access to certain personal health information can be withheld because of an unreasonable impact on the privacy of others. This could occur, for example, where information was provided by another person whose disclosure to the individual seeking access could have serious consequences.

The above exception will always involve a case by case judgement call by the GP on relative merits. In these cases it would only be necessary to withhold that section of the record which could identify the third party who provided the confidential information to the GP.

Where a dispute between the patient and the GP arises over access to medical records or the relevance or accuracy of information contained in the medical record, the patient can appeal to the Data Protection Commissioner.

11.4 Opinions Given in Confidence

The Data Protection Act 2003 provides that where the information provided to the medical practitioner by another person is an opinion, it may be disclosed to the patient without obtaining the consent of the provider. There is an exception where the medical practitioner believes that it was given in confidence or on the understanding that it would be treated in confidence. In this case the GP or data controller can refuse access to the opinion if the person who provided that opinion does not consent to its release. This situation would only arise in very exceptional circumstances and the patient can appeal this decision to the Data Protection Commissioner where the GP would have to argue that the opinion was not part

of the clinical consultation process and/or the release of the opinion to the patient was not otherwise required.

11.5 Other possible exemptions to a patient's right of access.

There are also a small number of legal grounds on which access to a patient's record can be withheld. These are general provisions and apply mainly to other types of information rather than health information. They include the following situations

- where disclosure would **prejudice** national security, crime prevention, detection or investigation of offences, the apprehension or prosecution of offenders, the assessment and collection of taxes or other monies owed to the State, local authority or HSE or the security of prisons,
- where it is would be contrary to the interests of protecting the international relations of the State,
- where the information is kept only for the discharge of functions, prescribed by the Minister for Justice, Equality and Law Reform, relating to financial impropriety,
- Where the information consists of estimates of liability on foot of claims made against the general practitioner,
- Where it is governed by legal professional privilege,
- Where the information is held only as research and statistical information and solely for that purpose with the express consent of the patient or
- Where the information is copy or back up information.

Appendix 1 – Selected Definitions from the Data Protection Acts

"data" means automated data and manual data.

"data controller" means a person who, either alone or with others, controls the contents and uses of personal data (for the purposes of these guidelines, a GP can be a data controller if they are in practice alone or a GP Practice can be the data controller where the files held are accessed by a number of GPs assigned to that practice).

"data subject" means an individual who is the subject of personal data (i.e. the patient).

"personal data" means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.

"processing", of or in relation to information or data, means performing any operation or set of operations on the information or data, whether or not by automatic means, including:

- **a.** Obtaining, recording or keeping the information or data
- **b.** Collecting, organising, storing, altering or adapting the information or data
- **c.** Retrieving, consulting or using the information or data
- **d.** Disclosing the information or data by transmitting, disseminating or otherwise making it available, or
- **e.** Aligning, combining, blocking, erasing or destroying the information or data

"sensitive personal data" means personal data as to –

- **a.** The racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject
- **b.** Whether the data subject is a member of a trade union
- **c.** The physical or mental health or condition or sexual life of the data subject
- **d.** The commission or alleged commission of any offence by the data subject, or
- **e.** Any 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.

Appendix 2 – Sample Practice Privacy Statement

Practice Privacy Statement

This Practice wants to ensure the highest standard of medical care for our patients. We understand that a General Practice is a trusted community governed by an ethic of privacy and confidentiality. Our practices are consistent with the Medical Council guidelines and the privacy principles of the Data Protection Acts. We see our patients' consent as being the key factor in dealing with their health information. This leaflet is about making consent meaningful by advising you of our policies and practices on dealing with your medical information.

MANAGING YOUR INFORMATION

- In order to provide for your care here we need to collect and keep information about you and your health on our records.
- We retain your information securely.
- We will only ask for and keep information that is necessary. We will attempt to keep it as accurate and up to-date as possible. We will explain the need for any information we ask for if you are not sure why it is needed.
- We ask you to inform us about any relevant changes that we should know about. This would include such things as any new treatments or investigations being carried out that we are not aware of. Please also inform us of change of address and phone numbers.
- All persons in the practice (not already covered by a professional confidentiality code) sign a confidentiality agreement that explicitly makes clear their duties in relation to personal health information and the consequences of breaching that duty.
- Access to patient records is regulated to ensure that they are used only to the extent necessary to enable the secretary or manager to perform their tasks for the proper functioning of the practice. In this regard, patients should understand that practice staff may have access to their records for:
  - » Identifying and printing repeat prescriptions for patients. These are then reviewed and signed by the GP.
  - » Generating a social welfare certificate for the patient. This is then checked and signed by the GP.
  - » Typing referral letters to hospital consultants or allied health professionals such as physiotherapists, occupational therapists, psychologists and dieticians.
  - » Opening letters from hospitals and consultants. The letters could be appended to a patient's paper file or scanned into their electronic patient record.
  - » Scanning clinical letters, radiology reports and any other documents not available in electronic format.
  - » Downloading laboratory results and Out of Hours Coop reports and performing integration of these results into the electronic patient record.
  - » Photocopying or printing documents for referral to consultants, attending an antenatal clinic or when a patient is changing GP.
  - » Checking for a patient if a hospital or consultant letter is back or if a laboratory or radiology result is back, in order to schedule a conversation with the GP.
  - » When a patient makes contact with a practice, checking if they are due for any preventative services, such as vaccination, ante natal visit, contraceptive pill check, cervical smear test, etc.
  - » Handling, printing, photocopying and postage of medico legal and life assurance reports, and of associated documents.

DISCLOSURE OF INFORMATION TO OTHER HEALTH AND SOCIAL PROFESSIONALS

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

DISCLOSURES REQUIRED OR PERMITTED UNDER LAW

- The law provides that in certain instances personal information (including health information) can be disclosed, for example, in the case of infectious diseases.
- Disclosure of information to Employers, Insurance Companies and Solicitors
- In general, work related Medical Certificates from your GP will only provide a confirmation that you are unfit for work with an indication of when you will be fit to resume work. Where it is considered necessary to provide additional information we will discuss that with you. However, Social Welfare Certificates of Incapacity for work must include the medical reason you are unfit to work.
- In the case of disclosures to insurance companies or requests made by solicitors for your records we will only release the information with your signed consent.

USE OF INFORMATION FOR TRAINING, TEACHING AND QUALITY ASSURANCE

- It is usual for GPs to discuss patient case histories as part of their continuing medical education or for the purpose of training GPs and/or medical students. In these situations the identity of the patient concerned will not be revealed.
- In other situations, however, it may be beneficial for other doctors within the practice to be aware of patients with particular conditions and in such cases this practice would only communicate the information necessary to provide the highest level of care to the patient.
- Our practice is involved in the training of GPs and is attached to the ABCD Vocational Training Programme. As part of this programme GP Registrars will work in the practice and may be involved in your care.

USE OF INFORMATION FOR RESEARCH, AUDIT, AND QUALITY ASSURANCE

- It is usual for patient information to be used for these purposes in order to improve services and standards of practice.
- In fact GPs on the specialist GP register of the Medical Council are now required to perform audits. In general, information used for such purposes is done in an anonymous manner with all personal identifying information removed.
- If it were proposed to use your information in a way where it would not be anonymous or the Practice was involved in external research we would discuss this further with you before we proceeded and seek your written informed consent.
- Please remember that the quality of the patient service provided can only be maintained and improved by training, teaching, audit and research.

YOUR RIGHT OF ACCESS TO YOUR HEALTH INFORMATION

- You have the right of access to all the personal information held about you by this practice. If you wish to see your records in most cases it is the quickest to discuss this with your doctor who will outline the information in the record with you. You can make a formal written access request to the practice and the matter can be dealt with formally. There may be a charge of up to Ð6.35 where a formal request is made.

TRANSFERRING TO ANOTHER PRACTICE

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

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

Appendix 3 – Sample Patient Registration Form

Patient Registration and Medical Summary Form

In order to provide for your care we need to collect and keep information about you and your health in your personal medical record. Please complete the following form. The information will be used to create your personal medical record on the practice computer.

Our practices are consistent with the Medical Council guidelines and the privacy principles of the Data Protection Acts. For further details please see our Practice Privacy Statement

PART 1

Today's date: _____

Surname: _____ **First name:** _____

Known as: _____

Title: Mr /Mrs./Ms/ Other _____

Date of birth: _____ **Gender:** Male / Female

Address: _____

_____

Phone: Home: _____ Work _____

Mobile _____

I am happy to receive alerts from the practice by:

Mobile phone ❑ E-mail ❑

GMS number: _____ Expiry date: _____

Next of kin:

Name: _____

Address: _____

Relationship: _____

Phone: _____

Previous GP name and address: _____

_____

Pharmacy name and address _____

_____

PPSN number: To avail of certain governmental schemes (e.g. Social welfare certificates, Mother and Child Maternity Scheme, Cervical Check, Childhood vaccinations) it will be necessary for you to provide us with your PPSN number.

Further information: The following information is not essential but may be of use to your doctor when they are diagnosing a problem or deciding on a treatment plan for you.

Marital Status: _____

Occupation: _____

Ethnic origin: _____

PART 2 – HEALTH HISTORY

Allergies: _____

_____

_____

_____

_____

Medical history: _____

_____

_____

_____

_____

Surgical history: _____

_____

_____

_____

_____

Current medications:

If you are unsure you could bring your empty pill boxes with you or get a printout from your pharmacist

_____

_____

_____

_____

_____

PART 3 – PATIENT STATEMENT

I _____ (Print Name)

have received a copy of the Practice Privacy Statement

_____ _____

Signature Date

Appendix 4 – Sample Waiting Room Notice

MEDICAL RECORDS – WHO HAS ACCESS?

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

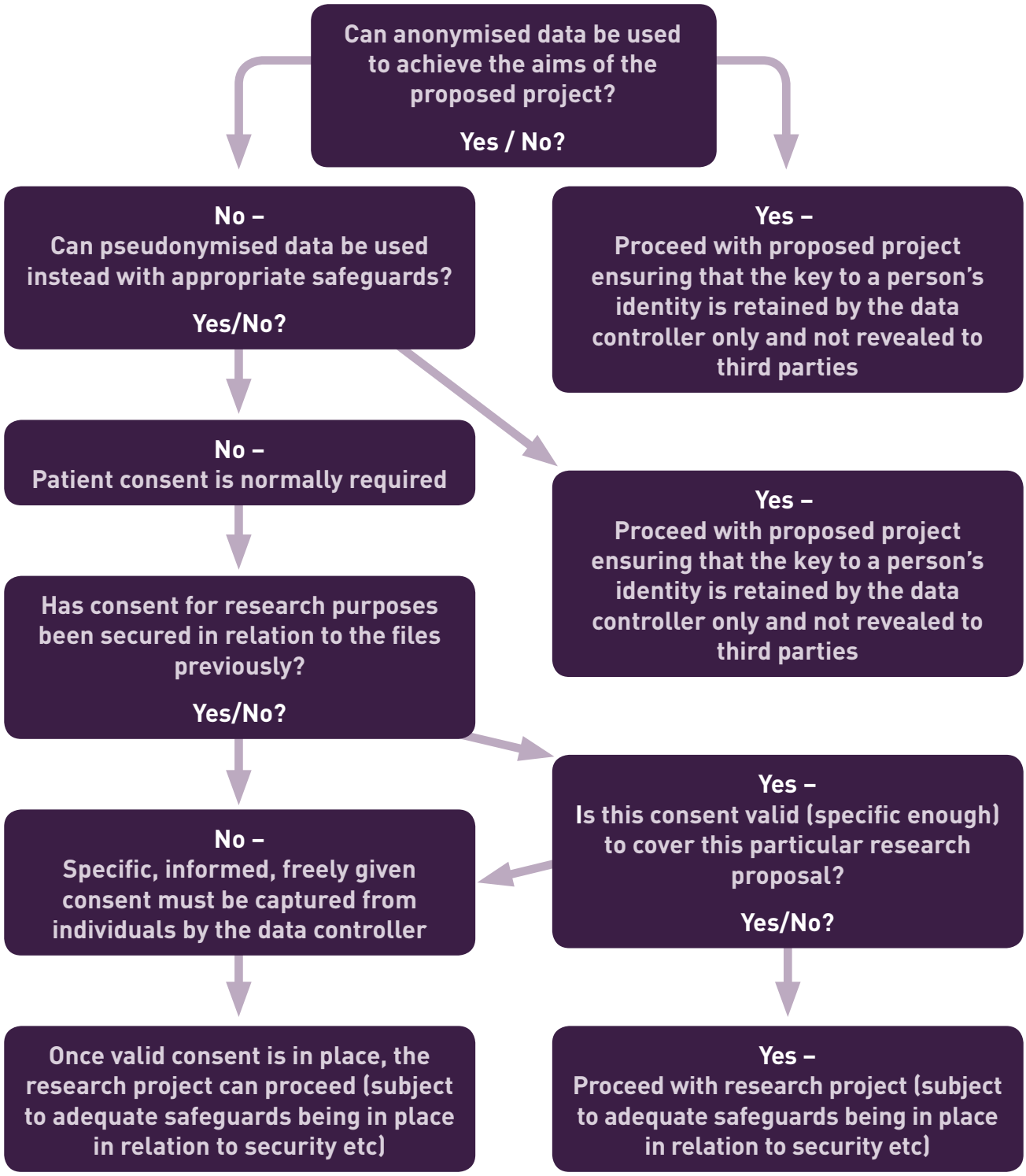
In order to provide for your care we need to collect and keep information about you and your health in your personal medical record.

Our practices are consistent with the Medical Council guidelines and the privacy principles of the Data Protection Acts.

For further details please ask at reception for a copy of our *Practice Privacy Statement.*

Thank you.

Appendix 5 – Best Practice Approach to Undertaking Research Projects using Personal Data



Source: Data Protection Guidelines on Research in the Health Sector
www.dataprotection.ie

Appendix 6 – General Practice Data Protection Checklist

Policies & Procedures

- ❑ Register with Data Protection Commissioner
- ❑ Identify person responsible for Data Protection in the practice
- ❑ Conduct staff training on confidentiality and privacy
- ❑ Ensure confidentiality clause is present in staff contracts
- ❑ Put in place a confidentiality agreement with your hardware and software support companies and any other entity accessing patient or staff information

Obtaining Information

- ❑ Give information leaflet on data protection to all patients
- ❑ Use agreed data collection form for new patients
- ❑ Do not collect PPSN unless required for a specific service

Access Control

- ❑ Require password access on all PCs and servers
- ❑ Ensure all users log in with their own user name and password
- ❑ All accounts should have 'strong' passwords
- ❑ Permissions set to only allow authorised staff to access data
- ❑ Ensure your practice software system provides an audit trail
- ❑ Ensure the physical security of both paper and electronic records

Information Sharing

- ❑ Be aware of the Information Sharing Guidelines for Primary Care Teams
- ❑ Ensure written consent is provided for every request for a PMA report
- ❑ Ensure anonymity of records when carrying out audit or research

Managing Devices

- ❑ Don't put patient records on USB memory sticks
- ❑ Encrypt the hard drive of any laptops or mobile devices that hold patient records

Data Retention

- ❑ Be aware of the data retention periods for different kinds of patient records
- ❑ Implement a defined policy on retention periods for all patient records

Information Security

- ❑ Implement the information security measures advised by the document 'No Data No Business'
- ❑ Put in place a practice policy on use of the Internet
- ❑ Don't use email for sending patient identifiable information

Backups

- ❑ Backup all patient records at least daily
- ❑ Store backups off site in a secure location
- ❑ Do a test restore on a regular basis

This Data Protection Checklist should be used alongside the documents:

- A Guide to Data Protection Legislation for Irish General Practice, available from www.gpit.ie
- Data Protection Audit Resource, available from www.dataprotection.ie
- No Data No Business, available from www.gpit.ie
- Interim Guidelines on Information Sharing in Primary Care Teams, Draft 7, Revision 13, 2008, available from the HSE

Appendix 7 – Sample practice confidentiality agreement for medical students

ANYTOWN MEDICAL PRACTICE
Main Street Anytown,
PH: 01-2345678 Fax: 01-9012345

Name of Medical Student: _____

Student ID number: _____

Medical School: _____

Period of Attachment From: _____ To: _____

Name of GP assigned to: _____

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

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

Medical Student:

Name: (Block Capitals) _____

Signature: _____

Date: _____

Responsible GP:

Name: _____

Signature: _____

Date: _____

Appendix 8 – Sample request for transfer of GP records

DR JOSEPH BLOGGS
ANYTOWN MEDICAL PRACTICE
Main Street Anytown,
PH: 01-2345678 Fax: 01-9012345

<Date>

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

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

Dear *<GP Name>*

The above has decided to register with this practice. I would be grateful if you could send me a copy of the medical records. Signed consent in accordance with the Data Protection Acts has been provided below.

Yours Sincerely

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

PATIENT SECTION

<Date>

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

_____
Patient Signature

Acknowledgment

Much of the information and guidance in this document comes from the original guideline document entitled "Managing and Protecting the Privacy of Personal Health Information in Irish General Practice" produced by the ICGP and GPIT group in 2003.

In this regard a debt of gratitude is owed to Mr. Peter Lennon from the Department of Health and Children who was the principal author of this document in collaboration with representatives from the ICGP, IMO and GPIT group.

References

1. Data Protection Amendment Act 2003. http://www.irishstatutebook.ie/2003/en/act/pub/0006/index.html.
2. Data Protection Act, 2008. http://www.irishstatutebook.ie/1988/en/act/pub/0025/index.html
3. Data Protection Acts 1988 and 2003: Informal Consolidation. http://www.dataprotection.ie/docs/Data_Protection_Acts_1988_and_2003:Informal_Consolidation/796.htm
4. Freedom of Information Act 1997. www.irishstatutebook.ie
5. Medical Council of Ireland *Guide to Professional Conduct and Ethics for Registered Medical Practitioners*. 7th Edition, 2009.
6. HSE Information Sharing Framework Working Group. *Interim Guidelines on Information Sharing in Primary Care Teams*; Draft 7, Revision 13. 2008.
7. HAYNES, K. THOMAS, M. 2007. *Clinical Risk Management in Primary Care*. Oxford: Radcliffe Publishing. ISBN 978 1 85775 869 6
8. LENNON, P. *Protecting Personal Health Information in Ireland Law & Practice*. Oak Tree Press. ISBN 1 904887 02 3
9. MILLS, S. *Clinical Practice and the Law*. Tottel Publishing ISBN 978 1 84592 786 8
10. The Medical Protection Society. 2009. *MPS Guide to Medical Record in Ireland*. ISBN 978 1 903673 10 2; http://www.medicalprotection.org/ireland/booklets/medical-records
11. National General Practitioner Information Technology Group. 2008. *No Data No Buisness*. http://www.icgp.ie/go/in_the_practice/information_technology/publications_reports 12th June 2010
12. National General Practitioner Information Technology Group. 2009. *Scanning and Shredding Documents: Impact Statement*. http://www.icgp.ie/go/in_the_practice/information_technology/publications_reports. 12th June 2010
13. National General Practitioner Information Technology Group. 2008. *GPIT Policy Document on Acceptable Usage of the Internet*. http://www.icgp.ie/go/in_the_practice/information_technology/publications_reports
14. HSE National Hospitals Office. 2007. *Code of Practice for Medical Records Management*.
15. *Data Protection Guidelines on research in the Health Sector*. Office of the Data Protection Commissioner; http://www.dataprotection.ie/docs/Guidelines_on_research_in_the_Health_Sector/573.htm;November 2007.

The Irish College General Practitioners (ICGP) is the professional body for general practice in Ireland. The College was founded in 1984 and is based in Lincoln Place, Dublin 2. The College's primary aim is to serve the patient and the general practitioner by encouraging and maintaining the highest standards of general medical practice. It is the representative organisation on education, training and standards in general practice.

The Irish College of General Practitioners, 4/5 Lincoln Place, Dublin 2
Tel: 01-676 3705, Fax: 01-676 5850, Email: info@icgp.ie, Web: www.icgp.ie

< BACK << CONTENTS <<< FRONT COVER