



Processing of Patient Personal Data: A Guideline for General Practitioners

File name: GP_GDPR_Guideline_v1_0.pdf

Date: 03/04/2018

Version: 1.0

Distribution: General Practitioners

Governance: Irish College of General Practitioners

(ICGP) Authors: ICGP Data Protection Working Group

Document History

Date	Version number	Comments
05/01/2018	0.1	First draft
25/01/2018	0.2	Editing of first draft, addition of multiple sections, addition of FAQs, addition of Appendices
02/02/2018	0.3	Editing of second draft, revision of tables, formatting
09/02/2018	0.4	Editing, formatting, inclusion of table captions
16/02/2018	0.5	Editing of the document in the context of a Guideline
27/02/2018	0.6	Editing following feedback from ICGP Working Group
28/03/2018	0.7	Editing following review by Office of the Data Protection Commissioner
03/04/2018	1.0	First public release version, following feedback from ICGP Working Group

Table 1 Document History

Part 2: Frequently Asked Questions

Part 2 of this Guideline deals with Frequently Asked Questions.

Retirement or Death

Q. I am a single-handed GP who is retiring shortly and facilitating a new doctor who has been appointed to my GMS list. What should I do with both my GMS and private patient records?

A. The incoming GP has a contract with the GMS and is entitled to the records of all patients on the GMS lists. It cannot be assumed that private patients will attend that GP, and records should be forwarded to that or other GPs on explicit consent from the Patient only. The existing (retiring) doctor should, however, maintain the patient medical records accumulated at that time for an adequate period consistent with meeting legal and other professional responsibilities. During that period, the provisions of the Data Protection Acts continue to apply to that information.

Transfer of individual records

Q. I have received an email from a woman requesting that I forward the medical records of herself, her husband and her children to another GP in her new location. How should I proceed?

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

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

Solicitor requests

Q. A solicitor has sent me a letter, with patient consent attached, requesting that I send the solicitor the entire patient record including third party correspondence. Am I ok to do this?

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

Health Insurance Company requests

Q. A patient of mine recently had a procedure in a private hospital. Her insurer is now requesting further information from me. Have they a right to this?

A. This is the patient's personal data. You must have the patient's explicit consent and must only release information which the Data Subject has explicitly consented to. It might be reasonable to suggest that the insurance company contact the consultant who performed the procedure and with whom they have a contract. Our advice would be to disclose to the patient themselves and allow them to disclose to whomever they wished.

Email Communication

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

A. If there is a specific request by email from a patient to send their results back by that format, then it is reasonable to acquiesce to that request. However, if you are contemplating a standardised process of returning results, you should restrict the content of any message, and consider the potential for a data breach. You should keep the information exchanged to a minimum. An explicit and informed request from the patient should be recorded.

Phone Requests

Q. A social worker who I don't know telephones me because of possible child abuse/neglect concerns relating to a child patient of mine. They want to know if I have any concerns about this child, its siblings or parents. How should I respond?

A. The general principle under Child Protection legislation is that the safety and well-being of children take priority. However, if you have any suspicion about the nature of the request, you should take steps to verify the identity of the caller. A written request from the Department of Social Work, which explains the basis for seeking information, is required in most cases.

Incidental Access to Information

Q. Certain non-practice members may have access to patient records when they are in the practice. These include medical students, HSE or pharma employed nurses, IT support staff and cleaners. How do we handle this?

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

Data Access Request

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

An individual can only make an Access Request for their own personal data. Legal guardians can also make an access request on behalf of a child. However, once a child is capable of understanding their rights to privacy and data protection, the child should normally decide for themselves whether to request access to data and make the request in their own name (this is not age dependent). It would also be important in such a case that the GP be satisfied that the person was genuinely acting on behalf of, and in the best interests of, the child whose data was being requested. Revealing of medical information of a child who is capable of making decisions themselves will in most situations constitute a breach of the Data Protection Acts if undertaken without the consent of the child capable of making their own decisions.

Personal Public Service number (PPS number)

Q. Can a GP ask for a patient's PPS number?

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

Research Projects

Q. Do I need a patient's consent to enrol them in research projects?

A. The capture and sharing of clinical patient information for research purposes should be anonymised. Exceptions to this arise where legislation is in place to allow analysis and research on patient identifiable clinical information. Examples of this include the National Cancer Registry and Infectious Disease regulations. Where research involves identifiable patient clinical information, explicit patient consent must be sought by the GP and documented in the patient record. Where the data is anonymised, it is no longer personal data and data protection regulations do not apply. It will be a matter for each GP to carry out an assessment in this regard and to review that assessment periodically to ensure that the data remain anonymous or unlikely to be re-identified.

In general the concept of data minimisation and anonymisation should be maintained. Where informed patient consent is used as the legal basis for research, the data controller must be able to demonstrate that consent has been forthcoming and must allow for the right of the patient to withdraw consent at any time.

Faxes

Q. Is it OK to use Faxes in general practice?

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

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

CONFIDENTIALITY NOTICE:

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

SMS Texts

Q. Is it OK to use SMS texts in general practice?

A. If you use SMS texts, you need to have a practice policy in place that covers consent, appropriate age groups, content of texts and confidentiality. Please refer to the article entitled 'Patient texting – let's be careful out there' in the December 2017 edition of Forum, the Journal of the Irish College of General Practitioners.

Use of Healthmail

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

A. Documents sent by normal email are not secure and can be accessed inappropriately by others before reaching their intended recipients. Healthmail, secure clinical email, is a HSE service that allows exchange of patient identifiable clinical information between GPs and HSE clinicians and between GPs and voluntary, maternity and children's hospitals. Healthmail is suitable for the electronic exchange of patient identifiable clinical information, including attachments. The GP is the data controller of his or her Healthmail account.

Access to Clinical Records by Secretarial and Administrative Staff

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

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

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

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

GP Practice Software Management system should provide an audit log of when patient information has been accessed, and by whom. Such an audit log makes it possible for the data controller in a practice to detect any unauthorised access to personal health information.

Freedom of Information Requests

Q. A General Medical Services (GMS) patient has submitted a Freedom of Information Request for their medical record. How should I proceed?

A. The HSE is a designated body under the Freedom of Information 2014. The medical card patient should submit the FOI request to the HSE and the HSE will then ask you for a copy of the patient's record. If there is a risk that disclosure of the record would be harmful to the patient, you should point this out to the HSE.