An Coimisinéir Cosanta Sonraí

Data Protection Commissioner

Data Protection Guidelines on research in the Health Sector

Contents:

Foreword:

I am delighted to be in a position to make available the attached guidelines which seek to step through the basis on which research and clinical audit in the health area can be carried out in a manner consistent with the framework of data protection legislation. My role as Data Protection Commissioner is to protect the privacy of individuals based on the requirements of the Data Protection Acts 1988 & 2003.

This role statutorily requires me to see the world in a way that puts the privacy rights of each individual at the forefront of my considerations. However, I also recognise that there are other factors to be considered in many instances and that the privacy rights of an individual are not paramount in all circumstances, e.g., investigation of crime etc. Equally the Data Protection Acts provide us all with choice in the vast majority of situations in terms of how our personal data is used.

Specifically in relation to research in the health sector, there are provisions in the Data Protection Acts to enable research to take place under certain conditions. With this in mind, I felt that guidelines to draw these issues out might be of benefit to all those persons in the field seeking to understand their responsibilities and obligations under the Acts. As a first step in their formulation, my Office held a consultative seminar in November 2006 entitled "Promoting Health Research and Protecting Patient Rights".

The seminar brought together representatives from across the health research and patient care spectrum to consider the key issues in this area and to try to formulate an agreed approach towards developing definitive guidelines which would take full account of data protection legislation. The seminar was followed in the earlier part of this year by the preparation of a draft guidelines document which was circulated for observations to relevant parties and made available on the website of my Office, www.dataprotection.ie. We received 12 submissions which have now been considered and, where possible, the views integrated into this final version of the document.

I hope that this document provides a comprehensive overview of the data protection considerations which need to be taken account of in advance of undertaking research which involves the use of personal data. I would also intend to use these guidelines as a framework for investigating any complaints which are brought to our attention in relation to relevant health research projects.

The capture of consent has been a widely debated issue and an attempt is made to explore and provide advice on its collection in this document. The document aims to strike an appropriate balance between the patient's right to personal data privacy and the desirability of making data available for research. It strives to present a position whereby the principles of data protection can promote and work with research and clinical audit once the patient's basic right to privacy is respected.

Anonymisation of patient records and/or freely given and informed patient consent are the foundation stones of how this Office wishes to see medical research undertaken from a privacy perspective. Where consent has not been obtained in relation to historical data, it is possible that data controllers, usually the relevant hospitals, can examine other options as detailed in this document, having exhausted other avenues for seeking consent, to legitimise access to such patient records. A best practice approach is suggested in the flow chart on page 5.

I recognise and it was the subject of a large amount of observations on the draft guidelines that a particular issue arises in relation to population registries or areas of study that require 100% coverage of the population of interest. As I have stated, my principal role is to safeguard the fundamental right to privacy of individuals in relation to how their data is collected and processed. In this respect, while the Data Protection Acts do allow for research carried out by the Data Controller itself or on their behalf without the need for express consent, this will not usually be sufficient in such cases to gather data in relation to the whole cohort of persons of interest. Equally given the focus on the rights of individuals, the Acts correctly do not provide a public good exemption for health research. In such circumstances and where 100% coverage is desired, I advocate specific legislation with inbuilt safeguards governing the operation of such databases. The National Cancer Registry has operated very effectively in such circumstances.

These guidelines provide detailed advice regarding compliance with data protection obligations only; they make no reference to the separate ethical obligations regarding confidentiality which we appreciate need to also be considered when undertaking research in this area. In this respect, the Research Ethics Committee structure was raised by a number of parties who participated in the consultation process as an area which should receive attention in this document. It is understood that this structure within the HSE and possibly beyond is currently under discussion. It would be the intention of this Office to offer assistance where requested in relation to the role of data protection in a Research Ethics Committee setting. Our hope would be that data protection considerations would become embedded in a standardised consideration process where access to personal data is envisaged. We look forward to working with the HSE on this important development.

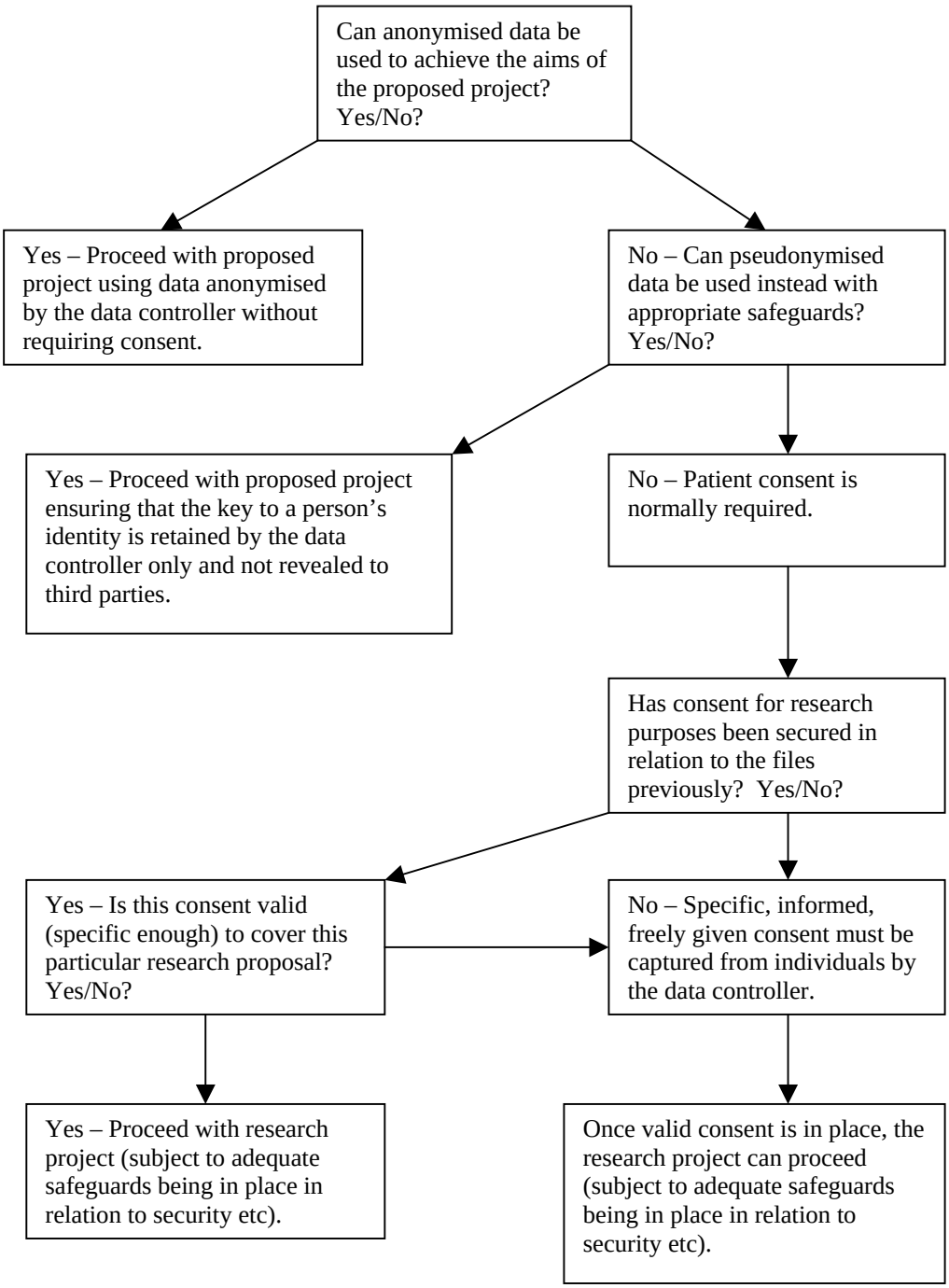
These guidelines concentrate on the gathering of patient data for research and clinical audit purposes. The subsequent conduct of the research or clinical audit project would obviously need to also comply with data protection legislation particularly in relation to access to and the safekeeping of the data. This document does not seek to address these requirements but I am happy to work closely with appropriate bodies in the area to develop guidelines or codes of practice should that be deemed of assistance. These guidelines are also not intended to deal specifically with the conduct of clinical trials where those trials are carried out under the framework of the EU Clinical Trials Directives.

Finally, I recognise that full implementation of the approach advocated in these guidelines would result in a sea-change in the methods employed for seeking and using patient information for research purposes in the health sector. I am fully cognisant of this in advocating this change but strongly believe that the end result in terms of the necessary availability of data for research and the protection of the privacy rights of individuals will more than compensate for the time and effort that would be expended.

I commend these guidelines and hope that they will prove useful to those persons in the research field grappling with the issues raised.

Billy Hawkes
Data Protection Commissioner
November, 2007

Best Practice Approach to Undertaking Research Projects using Personal Data:



1. The Data Protection background

The Data Protection Acts 1988 & 2003 provide the legislative basis for the approach of the Office of the Data Protection Commissioner with regard to personal data across all sectors of society – public, private and voluntary. The 2003 Data Protection Amendment Act transposed the 1995 EU Directive – 95/46/EC – the protection of individuals with regard to the processing of personal data and on the free movement of such data – which sets similar common standards for privacy across the EU.

The 1995 Directive, inter alia, contains specific minimum requirements in terms of the processing of personal health information which is categorised as a "special category of data" (in our Acts this is called sensitive personal data) which require special and additional protection in terms of obtaining, processing, security and disclosure. Data Protection requirements complement the strong ethical obligations imposed on health professionals in relation to their patients.

Legislative Position
For the sake of completeness and clarity, the legislative basis under which the sensitive health information of a person may be processed in the first instance for the purposes of treating the person and other activities directly related to that treatment as well as further processed for research and clinical audit purposes, are set out in the appendix. In summary, the Acts specifically envisage patient data being processed 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 data subject giving an unambiguous consent to their data being used for specified research purposes.

The Acts also provide an exemption for processing for statistical, research or scientific purposes carried out by the data controller itself where there are no disclosures of personal data to any outside third parties. Furthermore, the data will not be considered to have been unfairly obtained on account of the fact that the use of the data for research was not disclosed, as long as no damage or distress is likely to be caused to an individual. However, these exemptions can only be claimed by a data controller itself in respect of research carried out by it.

However, in the experience of the Office, research where there is no disclosure to outside third parties beyond the data controller is rare, so these guidelines focus on the standard issue of how research can be conducted on personal data without being able to rely upon this exemption. In any case, best practice would suggest that allowing the patient choice and providing them with information in relation to how their data is used should be the standard approach.

2. Data Protection and the use of Patient Information for Research purposes

The necessity for these guidelines arises from an acceptance that the legislative position as contained in the Data Protection Acts can be somewhat complex in terms of what is expected of a health professional, or other person owing a similar duty of confidentiality to the patient, seeking to access patient identifiable data for research or clinical audit purposes in terms of ensuring the fundamental rights and freedoms of the patient. At its simplest, however, the requirements can be reduced to an obligation to respect the confidentiality of information about patients (data subjects). Under the Data Protection Acts, the responsibility for ensuring the confidentiality of patient data and for securing any necessary consent for its further use lies with the data controller. The data controller – in this context could typically be a health facility, agency, or an organisation such as the Health Research Board, a Third level educational institution, HIQA, National Cancer Registry of Ireland etc. An example to illustrate this point would be where patient data is held for one HSE Service/Study, it may not be subsequently used for a separate purpose unrelated to the treatment or care of the patients concerned without their consent. To be clear on this point, if a purpose were identified where individuals need to be urgently contacted to ensure their immediate well-being, the provision in the Acts which permits the processing of information "in the vital interests" of those individuals would apply.

Equally a data controller could be an individual such as a GP or other medical professional working in a private capacity who is responsible for collecting information in the context of the treatment of a patient. It is this data controller who is legally responsible for the processing of the data under the Data Protection Acts. For the avoidance of doubt this personal legal responsibility arises only where the individual is working and responsible for the collection of the data in that private capacity

The most straightforward way in which access to patient identifiable information for research or clinical audit purposes can take place in line with the requirements of the Acts, is with the consent of the person for the intended use.

2.1 Provision of Explicit Consent:

Under the Data Protection Directive, the provision of explicit consent is a justification for the processing of sensitive data such as health data. In their working papers on this issue, EU Data Protection Commissioners working together through the Article 29 Working Party, concluded that, in order to be valid, consent must be a "freely given, specific and informed indication of the data subject's wishes". What is being put forward here is a relatively simple model that every effort should be made to ensure that the patient knows what could happen to their data for purposes unrelated to their treatment and are given an opportunity to consent or refuse consent for such use. In this way, if any proposed use of a patient's data for purposes unrelated to their treatment would likely come as a surprise to them, then a new and separate consent should be sought. Again to be clear the Data Protection Acts support the flow of information in relation to the treatment/supportive care of individuals without the need for explicit consent and the guidelines are not intended to deal with such primary use of data.

Specific

Where it is desired by a data controller to process a patient's information for a purpose other than the patient's treatment, it is strongly advocated, in line with European practice, that in so

far as is practically possible, an informed and explicit consent be sought as soon as possible after a patient presents at a health facility rather than at a later point when access to that data might be sought. The exact administrative method for implementing such a practice would be a matter for the health facility in the first instance taking account of its own particular circumstances. The advantage of such an approach is that a health facility would set out in a fully transparent manner to the patient what it considers to be the permissible and desired uses of patient data. This should seek to highlight, based on past experience or known future plans, the specific purposes for which patient identifiable information may be accessed for purposes unrelated to the patient's treatment.

Such an approach would require each data controller to consider in a thorough manner what such potential uses might be and specifically capturing these in an appropriate consent supported by an informative patient leaflet. In this context, the freely given and informed consent of the patient would be obtained before the research is conducted, thereby complying fully with Data Protection obligations.

The manner and form in which such consent would be sought could vary from one health facility to another depending on its own circumstances. Such a consent would be by way of an 'opt in'. Patients should also be informed of their right to revoke their consent at a later date if so desired.

Although obviously of large benefit in terms of progressing matters from the current position where consent is not routinely sought at the outset, consent along the lines of that outlined above, will be unlikely to be sufficiently specific or cognisant of all potential uses of a person's data. Additional research initiatives, not envisaged at the time of seeking the initial consent, involving the use of patient data would need to be predicated on further specific consents going forward.

Such a situation will also likely arise where a patient presents to a health facility with different conditions on separate occasions. In such circumstances it would be unlikely that an initial consent for condition specific related research would cover research currently related to the new condition also. In this respect, it must also be anticipated that patients will feel free to give consent for research on their data for some conditions but may refuse research on their data for other conditions where there may perhaps be extra sensitivity in relation to the condition or ethical considerations.

Such a system for routinely collecting and recording consent would also require a robust administrative system for correctly documenting patients' preferences to ensure that all subsequent access to their health data is fully in line with their stated wishes.

Informed

The advantage of the above approach is that the patient would be informed at all times as to the possible uses of their data and can decide, based on the information provided, as to whether they would be agreeable to their data being used in such a manner. The health facility can decide, based on its own practices, as to the extent of information to be provided. However, it is recommended that as much information as possible be provided to patients in the patient information leaflet. This would avoid the need, in all instances, to keep revisiting the patient to update their consent for specific additional purposes.

Such leaflets prepared by health facilities or GPs, as appropriate, should also provide assurances and details concerning all the safeguards in place designed to protect the patient's

confidentiality. It is recommended that these leaflets outline how data may be disclosed in the future for the benefit of the patient, or for purposes not directly related to, or indeed completely separate from, the patient's own healthcare treatment. An outline of the types of research that may be conducted should be provided e.g. studies that use information from patient health records for the patients own healthcare as opposed to studies that use information from patient health records as part of a survey. Patients should also be informed, if it is the case, that they could receive requests to participate in questionnaires or in randomised trials that focus on their particular health issues.

Freely Given

Another key issue in terms of the means of gathering consent from patients is the requirement that such a consent be freely given. In this context it must be recognised that the patient may perceive themselves, in certain scenarios, to be in a vulnerable position as regards the treating medical team. Accordingly, it is strongly recommended that every effort be made to ensure that the context for seeking consent for further uses of patient data be separated from any direct linkage with the patient's treatment.

In relation to capacity to consent, the Data Protection Acts contain the following provision:
Section 2A(1)(a) states that personal data shall not be processed unless Section 2 of the Acts is complied with and "the data subject has given his or her consent to the processing or, if the data subject, by reason of his or her physical or mental incapacity or age, is or is likely to be unable to appreciate the nature and effect of such consent, it is given by a parent or guardian or a grandparent, uncle, aunt, brother or sister of the data subject and the giving of such consent is not prohibited by law".

2.2 Anonymisation

The instigation of a process for the collection of specific consent for the use of patient identifiable data for research or clinical audit purposes not related to the treatment of that patient is, as outlined above, the optimum measure for ensuring compliance with the requirements of the Data Protection Acts in this area.

Of course, where patient identifiable data is not required, which would likely be the case in a large number of situations, it is strongly recommended that patient data be anonymised before it is accessed for secondary research or clinical audit purposes. Irrevocable anonymisation of personal data puts it outside data protection requirements as the data can no longer be linked to an individual and therefore cannot be considered to be personal data. Ideally such anonymisation of data for research purposes should be an automatic process performed as patient data is processed through IT or manual systems, whichever is the case. Where patient data is anonymised, there is no need from a data protection perspective to seek the consent of patients for the use of the data for research and clinical audit purposes. There may, of course, be ethical considerations in some cases but these are outside the scope of these guidelines.

A final issue in this area is that care needs to be taken when rendering data anonymous, as depending on the nature of the illness and the profile of the patient, there may be instances in which the data may actually still be identifiable. Where this might possibly be the case, an extra effort should be made to further remove any potential identifying information. Where this is not possible, due to the nature of the research to be conducted, a judgement will have to be made as to whether to follow the guidance above in terms of seeking the consent of the person for such use.

2.3 Pseudonymisation

Equally, it is recognised that the need to link episodes of care and prevent duplication of data in research, in some instances, requires that information may need to be capable of being matched or linked. This can be achieved through appropriate pseudonymisation (e.g., use of initials, coding) methods without the need to retain all identifying characteristics with the data.

Similar to the advice above in relation to anonymisation, where pseudonymisation methods are used, it is recommended that extra efforts, beyond use of initials etc, be incorporated where a condition is particularly rare. Where sufficient measures are put in place to ensure that personal data is not accessible or likely to be identifiable by parties external to the data controller, the requirement to capture consent to use the data for research purposes, in such circumstances, will no longer apply (as outlined in flow chart on page 5).

2.4 Health Intelligence Registries

It is also accepted that the development and maintenance of population based databases and registries designed to promote health nationally can give rise to some particular data protection difficulties. A strong case has been made by those developing and managing such initiatives that these databases and registries need to achieve maximum coverage of the relevant population if they are to meet their objectives. In order to compile the resource and achieve 100% coverage, the personal health information of relevant individuals needs to be accessed.

The Data Protection Acts are formulated on the basis that the right to protection of personal data is not absolute and can be restricted, in certain limited circumstances, e.g. vital interests of the data subject, when specified in an enactment etc. Where a database or registry is being developed or maintained for the benefit of the health or well-being of the population or a sector of the population, an exemption for such databases from the requirement for consent under the Data Protection Acts, must be contained in legislation. This will ensure that the exact circumstances and conditions attaching to the set aside of a person's fundamental data protection rights can be set out in legislation and thereby ensure, in so far as possible, that the fundamental rights and freedoms of the patient are respected. The National Cancer Registry (as provided for in the Health (Provision of Information) Act 1997) is perhaps the best example of such an approach. Despite the set aside from the requirements for consent for the disclosure by data controllers of patient identifiable information for the purposes outlined in that legislation to the Registry, all other rights of the individual to be informed about the existence of the database and obtain, update or correct the personal information or obtain access remain intact.

2.5 Development of Electronic Health Records (EHRs)

This Office has seen an increase in queries in relation to the development of Electronic health record systems in general. It must be noted that any processing of personal data in such a system must recognise and incorporate the principles as set out in the Data Protection Acts. As with processing of health information in a manual file system, an electronic system must also respect the principle of purpose limitation, that information must not be further processed for purposes incompatible with the reasons for which it was originally collected.

Any research data (that has not been anonymised) derived from electronic systems should also respect the conditions as aforementioned.

The development of national electronic patient record systems has been taking place across Europe and is the subject of continuing discussions at the EU level. Current discussions suggest that while consent can be used to justify processing of a person's data in a national EHR system, the putting in place of appropriate safeguards for such processing would likely best be achieved via a specific legislative provision that would also allow people the option, should they wish to exercise it, not to have their information included on the system. Further information on these ongoing discussions is available at http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm.

As has been recognised there are a large number of privacy and technical issues that must be considered and incorporated into the development of such a national EHR system in this country.

2.6 Adequate Safeguards

Of course, the capturing of consent is not an end in itself. The putting in place of appropriate safeguards to ensure that patient personal data is only used for the specified purpose(s) supplied, and can only be accessed or further disclosed to those persons to whom it is intended, is of perhaps even greater importance. Comprehensive security and access controls in relation to the storage of manual and electronic data are key requirements.

2.7 Use of Historical Data

It is recognised in this area that patient files that are valuable for medical research purposes are held by health facilities but patient consent to such use has not been obtained. In this respect, the approach of a private medical data compilation company in the UK is put forward as a good practice approach. This company has an extensive system in place to attempt to capture patient consent for access to data where no consent was initially sought. This involves the hospital twice writing to the data subject seeking a response, telephoning once thereafter and finally, if no response is received, such cases are submitted for ethics committee approval.

However, it is also acknowledged that securing such patient consent may not be practical due to the passage of time or numbers involved in all cases. In these limited circumstances and it must be stressed that this should be seen as very much the exception rather than the rule, the data controller must satisfy itself that the legislative position would allow for access to such data with appropriate safeguards incorporated in relation to confidentiality and security, for the purposes of the research. In any case every effort should be made to establish contact with the patient, if this proves not possible or not feasible and it is intended to access records without specific consent, then consideration needs to be given to appropriate notices in the media.

In addition, as a condition of any such access, the patient files should be anonymised (by the data controller or a data processor subject to an appropriate data protection contract) to allow for any potential future research to be conducted on anonymised data.

In such cases, the data controller must accept responsibility for ensuring that the confidentiality of patient records is not compromised due to the employment of external data collectors. For example, HSE researchers in general cannot access patient files for research

purposes, without an appropriate consent of the individuals involved being in place, if they are not directly involved in the treatment of those individuals. In order to avail of the "medical purposes" provisions in the Acts, the processing must be undertaken either by a health professional or a person who, in the circumstances, owes a duty of confidentiality to the patient that is equivalent to that which would exist if that person were a health professional, e.g. medical scientist. The strict confidentiality obligations on the data processors must be set out in writing before they are granted access to patient data.

An important point of clarification that arises, particularly in this area, is that the requirements of data protection legislation cease upon the death of the patient. Accordingly, for records of a certain age there can be little doubt that all the patients are dead. It is also recognised that this may give rise to difficulty in some situations as it may be unknown if all such persons are dead. In this respect, separately the Office of the Data Protection Commissioner will be commencing a consultation process on what might be deemed to be an acceptable period to elapse for records which contain personal data to be made available for archives purposes. The outcome of that process may be useful in the health area also in relation to historical patient records.

2.8 Persons accessing patient identifiable data

The Data Protection Acts require that where access to patient identifiable information is not accompanied by an explicit consent that it be undertaken for medical purposes and be undertaken by a health professional or 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 were a health professional. The term health professional is defined in the appendix to this document and is intentionally broad to ensure all appropriate health professionals can access patient data for medical purposes which also include research.

Questions as to whether a staff member, who is not a health professional and is to access patient identifiable information without consent, can be considered to owe an equivalent duty of confidentiality to the patient, need to be assessed on a case by case basis. As a general guide such persons would need to have a contractual duty of confidentiality that would carry an appropriate penalty should there be a breach of confidentiality.

3. Clinical Audit

It is acknowledged that the deployment of increasingly sophisticated information and communication technologies throughout the health sector has seen a marked increase in new systems of audit, review and evaluation. Clinical audit is designed to improve the quality of care provided to patients generally. It is normally undertaken by staff members of the health facility to assess particular services carried out in the hospital relating to particular courses of treatment, specific medical teams etc. Given the fundamental role played by clinical audit in patient care, implied consent is normally all that is required when the audit could likely be of benefit to that patient. Implied consent will also be considered as sufficient in those cases where no direct benefit is likely to accrue to the patient concerned and where the audit is to be carried out by the health facility itself [see section 2.8].

Where the clinical audit may be carried out by persons not involved in the care of the patient, i.e. in this case external to the data controller, informed consent will need to be in place for

access by such persons[1]. In such circumstances, informed consent may be captured by the inclusion of the possibility of external clinical audit in the general information material provided to the patient on how their information will be used.

This guidance is given on the assumption that the project is clearly clinical audit in nature.

4. Advice Summary

Anonymisation/Pseudonymisation
Anonymisation or pseudonymisation (subject to adequate safeguards) should be explored as the optimal position in relation to patient identifiable information where it might be used for research or clinical audit purposes and adopted if at all possible. This would be an ideal solution in cases where capturing consent is deemed particularly difficult.

Consent
The key issue is respect for the patient's reasonable expectation that their health information will be kept confidential and not used or disclosed without their consent other than to those directly involved in patient care and directly related activity. [2]

In the absence of a specific legal basis to underpin the processing of personal health data for research or clinical audit purposes, consent needs to be part of the process in order to meet the legal obligations as set out in the Data Protection Acts. Capturing an explicit and informed patient consent for further processing of a person's data for research purposes at the first opportune point a person presents to the health services[3] and thereafter as necessary, is advocated as the optimal way forward both from a data protection and efficiency perspective. Such an approach should be systematically built into health facility procedures so that the patient fully understands what further use is planned for their personal information and the safeguards that will be put in place. The patient should be given an opportunity to explicitly grant or deny consent for such use. The consent should also be sought in a context where it can be freely given without any sense on the patient's part that refusal would carry a penalty, whether real or implied, in relation to treatment.

Consent not sought
In very limited circumstances, where personal information is deemed integral to the success of a research project and where capture of consent is not possible for specific reasons, then the

[1] 'Provider institutions must ensure that the express consent of the patients is obtained for the process of clinical audit by staff not involved in the care of the patient' (EuroSOCAP, 2006) http://www.eurosocap.org/Downloads/European-Standards-on-Confidentiality-and-Privacy-in-Healthcare.pdf. It is recommended that this use of patient information be listed on an information leaflet by the healthcare service providing care and at the first opportune point a person presents to the service.

[2] This includes any activity carried out for the purposes of treating the patient outside the health facility also such as testing of samples by laboratories. Normally patient consent can be deemed to apply, where there is any doubt an appropriate data controller to data processor contract would provide the basis for such processing within the Data Protection Acts.

[3] This is intended to capture the vast majority of cases at a health facility. The capturing of consent in relation to exceptions such as A&E admissions in emergency situations will need a separate method of capturing consent.

research can only be undertaken by the data controller itself with appropriate safeguards for the confidentiality of the patient information in place.

Historical Data
In relation to personal data of a historical nature where no consent is in place for its use for research purposes, any access by a person or entity external to the data controller must be undertaken in the context of the Data Protection Acts. In particular, the data should be anonymised by the data controller prior to allowing access to the data to any external researcher. If access to patient identifiable information is required, or it is not possible to anonymise the information, every effort must be made to contact the persons involved and seek their consent by the data controller. If having undertaken all the above, access is still anticipated by a health professional or person otherwise owing a duty of confidentiality that is not an employee of the data controller, an appropriate data controller to data processor contract will need to be put in place stipulating the conditions attaching to such access.

Population Registries
In relation to specific projects of national public health importance such as the National Cancer Registry, appropriate safeguards can be provided via legislation. It must still be emphasised however that all other data protection rights in terms of further processing, disclosure, access, security etc will remain.

Clinical Audit
Clinical audit is in some cases different from research in that it normally takes place within a hospital and has the potential to be of direct benefit to a patient who is in receipt of regular treatment and whose treatment is reviewed by a clinical audit team. As with the general recommendation for research, it is recommended that the role of clinical audit teams be captured in an information leaflet provided to the patient at first point of contact with the service to cover the functions of clinical audit teams to review the quality of care to patients generally. In situations where direct benefit to a patient can be clearly demonstrated or where all access to patient identifiable data will take place for the purposes of audit by staff members of the health facility, it may be considered sufficient to rely upon the provisions of the Acts where the processing is necessary for 'medical purposes' and carried out by a health professional or 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 were a health professional".

5. Contact Details:

Any queries regarding these guidelines can be forwarded by email to info@dataprotection.ie or by post to:

Office of the Data Protection Commissioner
Canal House
Station Rd
Portarlington
Co Laois
Tel: 057 8684800
Fax: 057 8684757

Appendix

Legislative Position

"2B. Processing of Sensitive Personal Data
2B- (1) Sensitive personal data shall not be processed by a data controller unless
(a) section 2 and 2A (as amended and inserted, respectively, by the Act of 2003) are complied with, and
(b) in addition, at least one of the following conditions is met:
(i) the consent referred to in paragraph (a) of subsection (1) of section 2A (as inserted by the Act of 2003) of this Act is explicitly given,"

"iii) the processing is necessary to prevent injury or other damage to the health of the data subject or another person or serious loss in respect of, or damage to, property or otherwise to protect the vital interests of the data subject or of another person in a case where –

(I) consent to the processing cannot be given by or on behalf of the data subject in accordance with section 2A(1)(a)(inserted by the Act of 2003) of this Act, or
(II) the data controller cannot reasonably be expected to obtain such consent, or the processing is necessary to prevent injury to, or damage to the health of, another person, or serious loss in respect of or damage to, the property of another person, in a case where such consent has been unreasonably withheld"

A data subject's consent according to Article 2(h) of the Data Protection Directive (95/46/EC) "shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."

The Data Protection Acts provide exemptions in section 2(1)(5)(a) and (b) for statistical, research or scientific purposes carried out by the data controller itself where there are no disclosures of personal data to any outside third parties. Furthermore, the data will not be considered to have been unfairly obtained on account of the fact that the use of the data for research was not disclosed, as long as no damage or distress is likely to be caused to an individual. However, these exemptions can only be claimed by a data controller itself in respect of research carried out by it.

Another relevant section relates to where the processing is necessary for the performance of a function conferred on a person by or under an enactment [2A(1)(c)(iv)]. An example of legislation in this area is the Health (Provision of Information) Act 1997 which allows for the provision of information to the national cancer registry board for the purposes of any of its functions.

In addition, Section 2A of the Acts sets out the conditions which are required to render such data processing legitimate, at least one of which must be met. The most relevant would likely be:

(1) (d) the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and

freedoms or legitimate interests of the data subject.

Finally, where sensitive data, such as personal health data, is concerned additional conditions of Section 2B, must also be met, the most relevant of which is:

(1) (viii) the processing is necessary for medical purposes and is undertaken by—

(I) a health professional, or
(II) 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 were a health professional,

2B(4)
'health professional' includes a registered medical practitioner, within the meaning of the Medical Practitioners Act, 1978, a registered dentist, within the meaning of the Dentists Act, 1985, or a member of any other class of health worker or social worker standing specified by regulations made by the Minister after consultation with the Minister for Health and Children and any other Minister of the Government who, having regard to his or her functions, ought, in the opinion of the Minister, to be consulted;

"Medical purposes" is defined to include "the purpose of preventive medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services".

Health professional is further defined in S.I. No 82 of 1989 - Data Protection (Access Modification) (Health) Regulations, 1989 as follows

"health professional" means—

(a) a person who is a medical practitioner, dentist, optician, pharmaceutical chemist, nurse or midwife and who is registered under the enactments governing his profession, and

(b) a chiropodist, dietician, occupational therapist, orthoptist, physiotherapist, psychologist, child psychotherapist or speech therapist.