DATA PROTECTION AND FREEDOM OF INFORMATION LEGISLATION

Guidance for Health Service Staff
1. Introduction ......................................................................................................................... 5
2. Data Classification ............................................................................................................... 5
3. Personal and confidential data .......................................................................................... 7
4. Obtain and process information fairly ............................................................................ 8
5. Exceptions to the duty of confidence ................................................................................ 9
   5.1 Common Law .................................................................................................................. 9
   5.2 The Data Protection Acts 1988 and 2003 ..................................................................... 9
   5.3 Protections for Persons Reporting Child Abuse Act 1998 ............................................ 10
6. Keep data for specified, explicit and lawful purposes ..................................................... 10
7. Use and disclose data only in ways compatible with the purposes for which it was provided .................................................................................................................................. 10
   7.4 What information are HSE staff authorised to disclose? .............................................. 11
   7.5 Health care staff access issues ..................................................................................... 11
   7.6 Students ........................................................................................................................ 11
   7.7 Conclusion of care ......................................................................................................... 12
   7.8 Records of family members ......................................................................................... 12
   7.9 Quality assurance and audit - HIQA .............................................................................. 12
   7.10 Research and consent ................................................................................................. 12
   7.11 Use of data for research purposes .............................................................................. 12
   7.12 Fundraising and public support campaigns ................................................................. 12
   7.13 Insurance companies .................................................................................................. 13
   7.14 Public/employer liability insurance/Clinical Indemnity Scheme .................................. 13
   7.15 Information sought in relation to adoption ................................................................ 13
   7.16 Deceased service users .............................................................................................. 13
   7.17 Complaints handling .................................................................................................. 13
   7.18 HSE Publications ....................................................................................................... 14
   7.19 Filming/photography/audiotape ................................................................................. 14
   7.20 Personal information of service providers ................................................................. 14
   7.21 Communicating information to relatives .................................................................... 14
   7.22 Organ/tissue transplants ............................................................................................ 14
8. Disclosures of Data ............................................................................................................ 14
   8.2 Child protection .......................................................................................................... 15
   8.3 The Refugee Act, 1996 and Immigration Act 2003 ...................................................... 16
   8.4 Social Welfare Consolidation Act, 2005 ..................................................................... 16
   8.5 Cancer Services ........................................................................................................... 16
   8.6 Registers of births, deaths, and marriages ................................................................. 17
   8.7 Health Act 2007 - HIQA ............................................................................................. 17
   8.8 Health and Safety Authority ......................................................................................... 17
9. Information Required for the purpose of Investigations/Enquiries/ Court Orders ............ 17
10. Informed Consent ............................................................................................................ 20
    10.1 What is informed Consent? ....................................................................................... 20
    10.2 Alternatives to Consent – please also see Section 7 .................................................. 21
11. Keep data safe and secure ............................................................................................... 25
    11.4 Paper Records ........................................................................................................... 25
    11.5 Electronic records ...................................................................................................... 26
    11.6 Conversations/Phone Calls/Voicemails/SMS (text) messages ................................ 26
    11.7 Post ........................................................................................................................... 26
    11.8 Fax transmission ....................................................................................................... 27
    11.9 Telehealth .................................................................................................................. 27
11.10 Printing and copying.................................................................................28
11.11 Training and demonstrations..................................................................28
11.12 Use of Interpreters..................................................................................28
11.13 Electronic health records..........................................................................28
11.14 Electronic communication.........................................................................28
11.15 Passwords..................................................................................................29
11.16 Encryption................................................................................................29
11.17 Mobile phones...........................................................................................30
12. Keep data accurate, complete and up-to-date..............................................31
13. Ensure that data is adequate, relevant and not excessive..........................31
14. Retain data for no longer than necessary for the purpose(s) for which it is acquired..........................................................................................32
14.2 Disposal of records....................................................................................32
14.3 What is Confidential?.................................................................................33
14.4 Segregation of confidential waste..............................................................33
14.5 Disposal of Confidential Waste.................................................................33
15. Give a copy of their personal data to the relevant individual, on request......33
15.2 How can a person access this information?................................................34
15.3 Parliamentary Questions...........................................................................34
16.1 Does a Data Protection request have to be in a specific form?..................34
16.2 What rules cover the use, disclosure and transfer of personal health information?..........................................................34
16.3 What entitlements do service users have to personal health information?....35
16.4 Can access be refused?...............................................................................35
16.5 If the requester is unhappy with the initial decision what avenue is open to them?..........................................................35
16.6 Must all requests for information or access to records be made under the Data Protection Acts?..........................................................35
16.7 What if the request has already been dealt with under the Freedom of Information Acts?..........................................................36
16.8 Employment rights.....................................................................................36
17.1 Decisions of Public Bodies affecting the person.........................................37
17.2 Parents, guardians and next-of-kin rights*...............................................37
17.3 What is personal information in the context of the FOI Acts?....................37
17.4 What is a record according to the FOI Acts?............................................38
17.5 What records can be requested under the FOI Acts?.................................38
17.6 To whom are requests for access under the FOI Acts addressed, and who makes the decision to grant or refuse access?.................................38
17.7 Does an FOI request have to be in a specific form?..................................39
17.8 What are the statutory charges/fees?..........................................................39
17.9 If the requester is unhappy with the initial decision what other option is open to them?..........................................................40
17.10 Can staff seek access to their personnel records?.....................................40
17.11 Are the records of contracted service providers covered by the FOI Acts?40
18. Administrative access policy.......................................................................40
18.1 Does an administrative request have to be in a specific form?..................41
18.2 When is the decision due?.........................................................................41
18.3 Requests by third-parties..........................................................................41
18.4 Persons with an intellectual disability.......................................................41
18.5  Records of deceased persons .............................................................. 42
18.6  Exceptions to the administrative access process................................. 42
18.7  Is there a fee involved when requesting access under the administrative access route? .............................................................. 42
19.  Data Protection Breach Management Policy .............................................. 42
19.2  Identification and Classification ............................................................ 43
19.3  Containment and Recovery ................................................................. 43
19.4  Risk Assessment ............................................................................... 43
19.5  Notification of Breaches ................................................................. 44
19.6  Evaluation and Response .................................................................. 44
19.7  Roles and Responsibilities ................................................................. 44
20.  Enforcement ......................................................................................... 45
21.  Contact details HSE Area Consumer Affairs Offices ................................ 45
22.  Appendices ........................................................................................ 46
1. Introduction

1.1 The health service creates, collects and processes a vast amount of data in multiple formats every day. The HSE has a responsibility to ensure that this data is obtained fairly, recorded correctly, used and shared both appropriately and legally and stored securely. The purpose of this document is to provide guidance for the proper management of such data.

2. Data Classification

2.1 All data (irrespective of its format) owned, created, received, stored and processed by the HSE must be classified according to the sensitivity of its contents. Classification controls should take account of the organisational needs for sharing or restricting data, and the associated impacts and risks (e.g. consequences if data is mishandled). All data owned, created, received, stored or processed by the HSE must be classified into one of following categories:

(a) Public
(b) Internal
(c) Confidential
(d) Restricted

2.2 Public Data is defined as data that is available to the general public and is intended for distribution outside the HSE. There would be no impact on the HSE, its staff, clients or service users if this type of data was mishandled or accidentally released. Some examples of public data include:

(a) Service user/Client brochures
(b) Staff Brochures
(c) News or media releases
(d) Pamphlets
(e) Advertisements
(f) Web content
(g) Job postings
(h) Public Health Information

2.3 Internal Data is defined as data that is only intended for internal distribution among HSE staff, contractors, sub-contractors, agency staff and authorized third parties (i.e. service providers etc). There would be no significant impact on the HSE, its staff, or service users if this type of data was mishandled or accidentally released. Some examples of internal data include:

(a) Internal telephone directory
(b) Internal policies & procedures (excluding those published on the web)
(c) User manuals
(d) Training manuals and documentation
(e) Staff newsletters & magazines
(f) Inter-office memorandums
(g) Business Continuity plans
(h) Non person identifiable data

2.4 **Confidential data** is defined as data which is protected by Irish and/or E.U. legislation or regulations, HSE policies or, legal contracts or other legal duties of confidence. There could be a significant and adverse impact and/or penalties on the HSE, its staff or service users if this type of data was mishandled or accidentally released. Some examples of confidential data include:

(a) Service user / Staff personal data (Except that which is restricted as defined below in 2.5)
(b) Service user / Staff medical records (Except that which is restricted as defined below in 2.5)
(c) Unpublished medical research
(d) Personnel records
(e) Financial Data / Budgetary Reports
(f) Service Plans / Service Performance Monitoring Reports
(g) Draft Reports
(h) Purchasing information
(i) Commercially sensitive data
(j) Vendor contracts
(k) Data covered by Non-Disclosure Agreements or which is reported to the HSE in confidence
(l) Passwords / Cryptographic private keys

2.5 **Restricted data** is defined as highly sensitive confidential data. There would likely be a significant and adverse impact and/or penalties on the HSE, its staff or service users if this type of data was mishandled or accidentally released. Some examples of restricted data include:

(a) Service user / Staff sensitive medical data (i.e. mental health status, HIV status, STD status etc)
(b) Childcare / Adoption data
(c) Social Work data
(d) Addiction Services Data
(e) Disability Services Data
(f) Unpublished financial reports
(g) Strategic corporate plans
(h) Sensitive medical research
(i) Data collected as part of criminal/HR investigations
(j) Records of security incidents

3. **Personal and confidential data**

3.1 The HSE regards the lawful and correct treatment of personal and confidential data as a critical component in providing services and to maintaining service user confidence. All information about living service users whether it is held manually or in electronic format is subject to the requirements of the Data Protection Acts, which set out the standards that must be satisfied when obtaining, recording, holding, using or disposing of personal data.

3.2 As the organisation carries out its functions, the HSE needs to collect and use certain types of information about people, including ‘personal data’ as defined by the Data Protection Acts. This can relate to service users, current, past and prospective employees, suppliers, staff and others with whom it communicates. In addition, it may occasionally be required by law to collect and use certain types of personal information to comply with the requirements of legislation.

3.3 Data Protection rights apply whether the personal data is held in electronic format or in a manual or paper based form. There are eight key principles which underline the HSE’s responsibilities under data protection legislation. The HSE must:

(a) obtain and process information fairly;
(b) keep it only for one or more specified, explicit and lawful purposes;
(c) use and disclose it only in ways compatible with these purposes;
(d) keep it safe and secure;
(e) keep it accurate, complete and up-to-date;
(f) ensure that it is adequate, relevant and not excessive;
(g) retain it for no longer than is necessary for the stated purpose or purposes; and
(h) give a copy of personal data to an individual, on request.
4. **Obtain and process information fairly**

4.1 To obtain data fairly, the data subject must, at the time the personal data is being collected, be made aware of who will use the data being requested, what the data will be used for, and how the HSE processes data.

4.2 To **fairly process** personal data it must have been fairly obtained and the data subject must have given consent to the processing or the processing must be necessary for one of a number of reasons, including:

(a) to prevent injury or other damage to the health of a data subject or another person;

(b) to prevent serious loss or damage to property of the data subject or another person;

(c) to protect the vital interests of the data subject or another person where the seeking of the consent of either is likely to result in those interests being damaged;

(d) for the administration of justice;

(e) compliance with a legal obligation, (other than that imposed by contract);

(f) 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;

(g) for the purpose of obtaining legal advice, or in connection with legal proceedings, or for the purposes of establishing, exercising or defending legal rights;

(h) processing by a health professional for medical purposes;

(i) in relation to the administration of a Social Welfare scheme, only where HSE staff as part of their role are processing data for this purpose.

(j) for the purpose of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

4.3 A duty of confidence arises when one person discloses information to another (e.g. service user to health care staff) in circumstances where it is reasonable to expect that the information will be held in confidence. This concept is an expression of the service user’s expectation that whatever transpired during medical care is treated as confidential.

4.4 The current Medical Council guidelines reflect the Hippocratic tradition and the obligations imposed by law, which states:
“Confidentiality is a time honoured principle of medical ethics. It extends after death and is fundamental to the Doctor/Patient relationship. While the concern of relatives and close friends is understandable, the Doctor must not disclose information to any person without the consent of the Patient”. A Guide to Ethical Conduct and Behaviour, 7th ed. (Medical Council, Dublin 2009)

4.5 One of the most important legal obligations that health care staff owe to the service user is the protection of confidences. However, there is no specific legislative provision governing this duty of confidence. The duty of confidence in the medical context is more in the line of a moral and ethical duty. It is therefore governed by codes of professional conduct as well as by the general common law duty of confidence and extends beyond the medical profession, and includes any health care professional or personnel receiving medical or other personal information in a relationship of confidence. While this is not an unqualified duty, it should only be overridden if the holder of the information can justify disclosure as being required, for example by reference to a particular law, if it is necessary to protect the interests of a service user or other person, where it is necessary in the public interest or where the individual has given consent to such disclosure.

4.6 Health care staff must not disclose personal health information to any other person, except those properly entitled to receive it. It must be remembered that the confidences belong to the service user and not the health care staff member, who is merely the custodian.

5. Exceptions to the duty of confidence

5.1 Common Law

(a) Professional confidence is not absolute and may be broken under one of the following conditions:

(i) when required by legislation or when ordered by a judge in a Court of Law, or by a Tribunal established by an Act of the Oireachtas;

(ii) when necessary to protect the interest of the service user;

(iii) when necessary to protect the welfare of society;

(iv) when necessary to safeguard the welfare of another individual or service user;

(v) when a service user gives consent to disclosure of their personal health information to a third party.

There are also statutory exceptions to the duty of confidence which include the following:

5.2 The Data Protection Acts 1988 and 2003

(a) The Acts impose a duty on data controllers not to use or disclose data in any manner inconsistent with the purpose for which the data was collected.
However, the Acts set out some narrow exceptions, such as where there is an urgent requirement to disclose information e.g. imminent danger to health/safety, information required urgently for the investigation of suspected offences, provision of legal advice, to assist in legal proceedings, court order etc). Where those exceptions apply, then the request should be given immediate priority and the person dealing with the request should notify his or her superiors.

5.3 Protections for Persons Reporting Child Abuse Act 1998

(a) According to the ‘Children First’ guidelines all staff must be alert to the possibility that children with whom they are in contact may be suffering from abuse. Concerns are to be reported to the HSE. This responsibility is particularly relevant to professionals such as teachers, child care workers and health care staff who have regular contact with children in the course of their work. It is also an important responsibility for staff and volunteers involved in sports clubs, parish activities, youth clubs and other organisations caring for or involving children.

(b) The HSE Childcare Service Managers co-ordinate child protection services. They are responsible for receiving all notifications of child abuse. Generally speaking under this Act a person does not incur any civil liability for reporting to a Garda their opinion that a child has been or is being abused provided they are acting reasonably and in good faith. Accordingly, information should never be withheld or delayed if it would endanger a child or children or if it would result in children failing to receive adequate care.

5.4 The above examples are not exhaustive. There are other situations where the disclosure of personal information without consent may be warranted and would be permissible. If in doubt, seek guidance.

6. Keep data for specified, explicit and lawful purposes

6.1 The HSE holds information for a variety of purposes. Much of this information is held for use in the provision of healthcare or social services provided by the HSE. Information must only be kept for the lawful and clearly specific purpose(s) for which it was obtained and must only be processed in a manner compatible with that purpose. A data subject has a right to question the purpose for which the HSE holds their data and the HSE must be able to identify and explain that purpose. This can include data relating to employees such as duty details, operational directives and financial claims.

7. Use and disclose data only in ways compatible with the purposes for which it was provided

7.1 HSE employees and those providing a service on the HSE’s behalf must not disclose data in relation to any data subject to someone who is not entitled to receive it. Any use or disclosure must be necessary for the purpose/s or compatible with the purpose/s for which the data is collected and held.
The general advice that applies here is that the data subject should be aware of the purposes for which their data is held such that they would not be surprised to learn that a particular disclosure is taking place. Note however that statutory disclosures such as those referred to in Section above are permitted.

7.2 In all cases the identity of the person outside the HSE to whom the disclosure is being made should be established along with the specific purpose of the disclosure. In addition, a record of all such disclosures should be maintained by the relevant department. In cases where there is any doubt as to the appropriateness of the disclosure, or the status of the data concerned, the local Consumer Affairs Area Office should be contacted for advice. (see contact details at the end of this document)

7.3 Where the HSE engages a third party to provide services on its behalf and where the services will require the service provider to process personal data, the HSE is required by law to have a written contract in place with the service provider which provides sufficient guarantees with regard to data protection compliance. The HSE has developed detailed Services Agreements for this purpose which are available from the HSE’s Office of Legal Services (see Section 10.2(b)(xii) below regarding Third Party Health Providers).

7.4 What information are HSE staff authorised to disclose?

(a) Anonymised information can be disclosed without consent to support audit and risk management activities within the HSE, and to provide statistical information to other organisations such as the Department of Health, universities and research institutions. Service users should be advised, where possible, that their information may be used in anonymised form for such purposes. If it is not possible to use anonymous information, or where it may be possible to identify individuals from the information given, service users must be contacted by relevant staff to obtain their consent.

7.5 Health care staff access issues

(a) Health care staff involved in the continuing care or treatment of a service user may access the health record of that service user. Service user records can only be shared by health care staff on a need to know basis.

7.6 Students

(a) Student health care staff enrolled in recognised teaching institutions and working in healthcare settings may have access to healthcare records, with the approval and under the direction of their supervisor. Wherever possible personal health information must be anonymised before it is used for teaching purposes. Where this is not possible the health care staff must obtain service user’s consent. Students on placement in HSE services must sign a confidentiality agreement.
7.7 Conclusion of care

(a) When an episode of care concludes for whatever reason, including the death of a service user, the right of access by health care staff to the healthcare record is normally terminated. Access may still be authorised for purposes other than service user care, such as clinical audit, FOI/DP access, research or legal proceedings.

7.8 Records of family members

(a) Clinicians will normally have access to the records of only those service users they are treating. They do not have a right of access to the healthcare records of members of a service user’s family without the written consent of the person to whom the record relates.

7.9 Quality assurance and audit - HIQA

(a) The Health Information & Quality Authority was established under the Health Act 2007. Its statutory functions are to set standards on safety and quality relating to HSE services and those of service providers. It may also carry out inspections of certain services. Section 12 of the Health Act 2007 entitles HIQA to require the HSE or a service provider to provide it with any information or statistics that HIQA needs in order to determine compliance with safety and quality standards.

7.10 Research and consent

(a) As a general rule personal health information can only be used for the purpose of medical research with the written consent of the service user. The service user must be advised on all the aspects of the proposed research and what it entails, and how their personal health information will be used. Staff should ensure that the written consent is available on the health record. (see the Data Protection Commissioner’s Guidelines on Research in the Health Sector which are available on www.dataprotection.ie).

7.11 Use of data for research purposes

(a) Where the research sample size is so small or unique that even anonymised data may lead to the identification of the individual, additional measures must be taken to ensure that privacy and confidentiality is protected. In general, data for clinical audit and related purposes should be anonymised. The activities involving research, or the compilation of statistics, must be approved by a properly constituted HSE Ethics Committee and conducted in accordance with that committee’s requirements and Data Protection Law. This applies to both internal and external research requests, for example, requests from pharmaceutical companies.

7.12 Fundraising and public support campaigns

(a) Access to personal health information (including contact information) for the purpose of fundraising or gaining public support must not be granted without the express prior consent of the service user.
7.13 **Insurance companies**

(a) Staff dealing with such requests should only provide relevant information which they consider is required to meet the insurance company’s requirements. For example, where an insurance company is seeking information about an injury which is the subject of a claim but submits a request for a copy of a person’s full medical file, then this should be carefully assessed and only relevant information provided.

7.14 **Public/employer liability insurance/Clinical Indemnity Scheme**

(a) When an incident occurs in any location throughout the health service, the local supervisory officer/department manager must complete an incident report in accordance with risk management guidelines. A system known as STARS-Web is used to track such incidents and report them to the HSE’s insurers, the Clinical Indemnity Scheme (CIS). A failure to report an incident may void the HSE’s insurance cover and accordingly, it is not necessary to await receipt of a legal claim prior to notifying an incident to the CIS. The HSE and the CIS will retain such reports in confidence and will not retain such data in personalised form once the final period for bringing a legal claim has expired.

7.15 **Information sought in relation to adoption**

(a) Any application by an adoptee for access to birth-related information should be referred to the relevant local social work department within the HSE. Alternatively the applicant should write directly to the Adoption Authority of Ireland at Shelbourne House, Shelbourne Road, Ballsbridge, Dublin 4.

7.16 **Deceased service users**

(a) The Data Protection Acts do not apply to deceased persons. However, given the potential harm and distress that can arise from the inappropriate disclosure of such information requests for access to records of the deceased should be submitted and dealt with through the Freedom of Information process, to ensure that appropriate reasons exist to set-aside the privacy rights of the deceased person.

7.17 **Complaints handling**

(a) Complaints or allegations made to the HSE about members of the public require the HSE to take reasonable steps to assess the likely truth of the allegation before taking further appropriate steps. Complaints or information may also arise about a HSE employee or service provider that gives rise to concerns (e.g. doctor, nurse, private healthcare provider etc.). The Health Acts provide for the making of protected disclosures by employees of the HSE where an employee makes, in good faith, a disclosure regarding any serious concerns about standards of safety or quality in health and social care services. The HSE is required to investigate the subject matter of any protected disclosures and may, in addition, refer it to a third party (e.g. Irish Medical Council, HIQA or An Garda Síochána) as appropriate.
7.18 **HSE Publications**

(a) Any HSE publications such as newsletters or leaflets should not include images of staff, service users or visitors without their informed consent.

7.19 **Filming/photography/audiotape**

(a) A service user must not be photographed, filmed, or recorded on audiotape unless consent is given. If given, these records must form part of the service user record. The use of CCTV cameras without consent may be appropriate in public places where security or safety issues arise. However, the location of cameras, the circumstances in which images will be retained and disclosed and the requirements governing notices and signage are subject to the Data Protection Acts. The reviewing of CCTV footage for staff monitoring purposes and the retention of CCTV footage for more than thirty days is generally unlawful under the Data Protection Acts. The Data Protection Commissioner has published detailed guidance on Data Protection and CCTV which is available at [www.dataprotection.ie](http://www.dataprotection.ie).

7.20 **Personal information of service providers**

(a) As part of standard service delivery the staff member’s name and job title are to be available to service users. Other personal information, such as, home address or home telephone number, is not to be made available.

7.21 **Communicating information to relatives**

(a) Information concerning a service user’s condition is confidential and ideally should only be given to relatives with the service user’s consent. There are however circumstances such as severe illness, coma etc., where information may be given to next-of-kin without the service user’s consent. On admission to hospital the service user, where possible, should be asked to nominate a responsible person or relative with whom all relevant information concerning their care and treatment may be shared. Personal information about service user admissions or service user conditions should not be disclosed to the media or anybody else including chaplains or other religious, without the express instruction of the service user or next of kin.

7.22 **Organ/tissue transplants**

(a) In relation to the donor of a transplanted organ or tissue, information must not be disclosed which may lead to the identity of the donor. Confidentiality is always maintained, except in the case of living donations, which are usually within the same family.

8. **Disclosures of Data**

8.1 There are specific occasions when the HSE is obliged to share information with other organisations. Disclosures of data which are required by statute, such as the examples set out below, are expressly permitted by Section 8(e) of the Data Protection Acts 1988 and 2003. So as to ensure that the HSE meets its statutory obligations, when a HSE staff member receives a request for information which is stated to be permitted by law, he or she should in the first instance:
(a) check that it is a valid request i.e. check the precise authority of the person requesting access, including reference to the section of the Act under which access is authorised;

(b) check the nature of the access requested, to ensure that only material relevant to the statutory demand is released;

(c) thereafter, as efficiently as possible, gather the relevant information held;

(d) consider the information having regard to this Policy and any other relevant ethical or statutory provisions applicable;

(e) consult with relevant parties within the HSE (or other body holding the information);

(f) seek advice if necessary from the Consumer Affairs Office or Senior Manager; and

(g) come to a decision. If the resultant decision is to disclose the information, it should be disclosed in the most secure manner appropriate to the information.

Examples of where information is required to be disclosed by statute include the following:

8.2 Child protection

(a) The welfare of the child is the first and paramount consideration which should be addressed when considering issues around the obtaining and disclosure of information relevant to childcare. Information should never be withheld or delayed if it would endanger a child or children or if it would result in children failing to receive adequate care. Specific guidance on the application of data protection and natural justice rules in the context of child care services is set out in the Children First National Guidelines for the Protection and Welfare of Children 2011. Per the Guidelines, all information regarding concern or assessment of child abuse is to be shared on “a need to know” basis in the interests of the child.

(b) No undertakings regarding confidentiality can be given. Those working with a child and family are to make this clear to all parties involved.

(c) Ethical and statutory codes concerned with confidentiality and data protection provide general guidance in relation to confidentiality. They are not intended to limit or prevent the exchange of information between different professional staff having responsibility for ensuring the protection of children. Giving information to others for the protection of a child is not a breach of confidentiality.

It must be clearly understood that information gathered for one purpose must not be used for another without consulting the person who provided that information.
Clear guidelines must be in place for the transfer of relevant records relating to child protection cases when a child is moved to another area within the country. Particular reference has to be made to the transfer of information/records to Northern Ireland in view of the special arrangement which now exists between the two jurisdictions and further information is available in the Children First Guidelines in relation to this.

When considering the disclosure of information, it is important to bear in mind the potential application of the in camera rule. The in camera rule provides for certain proceedings to be heard in private, including family law cases and cases relating to children, in order to prevent disclosure of details of a private and sensitive nature. An example of legislation providing for this is in the Child Care Act 1991 where certain childcare proceedings are held in private. Legal advice should be taken before disclosing information which relates to a case that is subject to the in camera rule.

8.3 The Refugee Act, 1996 and Immigration Act 2003

(a) The purpose of the Refugee Act 1996 is to put in place procedures for dealing with asylum applications on a statutory footing. Section 8(5)(a) of this Act requires Immigration Officers to notify HSE when a child arrives unaccompanied in this State:

“Where it appears to an Immigration Officer that a child under the age of 18 years who has arrived at the frontiers of the State is not in the custody of any person, the immigration officer shall, as soon as practicable, so inform the Health Board in whose functional area the place of arrival is situate and thereupon the provisions of the Child Care Act, 1991, shall apply in relation to the child”

(b) Under Section 8 of the Immigration Act 2003, the HSE has a statutory duty to disclose personal information to the Garda Immigration Bureau regarding non-nationals for the purpose of administering the law governing entry to, and removal from, the State. (This would not extend to medical information in the normal course)

8.4 Social Welfare Consolidation Act, 2005

(a) Authorisation for the transfer of certain information associated with schemes administered in association with Social Welfare. Legislation between the Minister for Social Protection to another Minister or specified body is contained in Section 261 of the Social Welfare Consolidation Act, 2005. The Act defines the HSE as one of the ‘specified bodies’.

8.5 Cancer Services

(a) The Irish National Cancer Registry set up in 1991 and began registering cancers nationwide in January 1994. The National Cancer Registry has been collecting comprehensive cancer information for the whole population of the Republic of Ireland since 1994. The information they collect is used in research into the causes of cancer, in education and information programmes, and in the planning of a national cancer strategy to deliver the best care to the whole population.
(b) The Health (Provision of Information) Act, 1997 allows for the provision of information to the National Cancer Registry Board, the Minister for Health, the HSE, hospitals or other agencies participating in cancer screening programmes authorised by the Minister.

8.6 Registers of births, deaths, and marriages

(a) There is a legal obligation on designated staff to report these events to the appropriate registrar’s office. The registers of births, deaths and marriages are a matter of public record. This means that anyone can request a search and obtain a certificate of any event following provision of information concerning the event and payment of the specified fee.

8.7 Health Act 2007 - HIQA

(a) Section 12 of the Health Act 2007 entitles HIQA to require the HSE or a service provider to provide it with any information or statistics that HIQA needs in order to determine compliance with safety and quality standards.

8.8 Health and Safety Authority

(a) When a staff member is absent from work for a period greater than three calendar days as a result of an injury received in the course of duty, the Health and Safety Authority must be notified by the local supervisor/manager.

9. Information Required for the purpose of Investigations/Enquiries/Court Orders

9.1 In addition to the items identified in Section above, information may also be required to be disclosed in the context of the performance of an investigation, enquiry or legal proceedings. The most common examples in practice are summarised below:

(a) Ombudsman: Section 7(1)(a) of the Ombudsman Act 1980 provides the Ombudsman with powers to acquire information or documents for the purpose of a preliminary examination or investigation by him or her under the Act. Any person in possession of such information or documents may also be required to attend before the Ombudsman.

(b) Ombudsman for Children: Section 14 of the Ombudsman for Children Act 2002 provides the Ombudsman for Children with the power to acquire information or documents for the purpose of a preliminary examination or investigation. Any person in possession of such information or documents may also be required to attend before the Ombudsman for Children.

(c) Information Commissioner: The Information Commissioner may, for the purposes of a review under the Freedom of Information Acts, require the HSE to provide any documentation as is considered necessary.
(d) **Data Protection Commissioner**: The Data Protection Commissioner may, for the purposes of the investigation of a complaint under the Data Protection Acts, require the HSE to provide any documentation as is considered necessary.

(e) **In relation to requests for information from the National Suicide Research Foundation, please contact your local Consumer Affairs office for guidance.**

(f) **Court order for discovery**: A Court Order for discovery is made where a party to proceedings seeks copies of documents, notes and memoranda which will either strengthen his case or weaken his opponent’s case. A party in litigation can seek discovery where the HSE is a party. It can also be sought in litigation where the HSE is not a party and has no involvement (this is known as “third party discovery” and also as “non-party discovery”). In litigation involving the HSE, where an order for discovery is sought, the HSE’s solicitors ordinarily deal with the matter. In a normal case, proceedings will have already been issued involving the HSE. A request is then made through the HSE’s solicitors requiring the HSE to discover on oath the documents in its possession, power or procurement. The HSE’s solicitors prepare an affidavit (a sworn statement) on behalf of the person required to swear the Affidavit setting out full details of all documents and other records held by the HSE which are relevant to the proceedings or in respect of which an order has been made. It is generally the case that all documents and records have to be discovered but the courts do recognise that there are exceptional circumstances where discovery may not be warranted or justified because of over-riding policy considerations or more important interests. One such exception arises in the case of what is called “legal professional privilege”. Where there is a relationship between a lawyer (solicitor or barrister) and a client, the jurisprudence of the courts provides that any documents, notes, memoranda or other communications between lawyer and client for the purpose of rendering or obtaining legal advice, should as a general principle be immune from discovery. This privilege applies to both in-house and external legal advisors.

(g) **Non-party discovery**: In third party or non-party discovery, someone may seek discovery of the HSE records. For instance, in a road traffic accident case where somebody brings proceedings seeking compensation for personal injury, it might arise that the defendant/insurance company wishes to see the healthcare records of the injured party. If the injured party does not consent to those records being disclosed, an application may be made to the court and the court in due course may make an order directing the health service to disclose specified healthcare records of that party. All court applications and court orders for third party discovery should be referred to the HSE’s solicitors.

(h) **Voluntary discovery**: Voluntary discovery is an administrative method of sharing relevant information between two parties in civil proceedings. This must be sought by individuals / parties and rejected by the holding party (HSE) prior to applying to the courts for an order of discovery.
(i) **Search warrants**: Compliance with a search warrant is required by law and record management personnel are advised that they should inform their immediate supervisor of any official demand for access to records. The warrant must be specific regarding the records required.

(j) **Tribunal of Inquiry**: A Tribunal of Inquiry is a body set up either by specific statute or by resolution of the Oireachtas to inquire into specific matters, which are of public interest and of urgent importance. A Tribunal of Inquiry has similar powers to the High Court to subpoena witnesses, documents and to make orders for discovery.

(k) **Irish Medical Council**: For the purposes of an inquiry, the Irish Medical Council may establish a Preliminary Proceedings Committee and a Fitness to Practice Committee. Either committee has all the powers, rights and privileges that are vested in the Court or a judge of the Court on the occasion of an action and that relate to:

(i) enforcing the attendance of witnesses;

(ii) examining witnesses on oath or otherwise, and

(iii) compelling the production (including discovery) of records.

(l) **An Bord Altranais (Nursing Board)**: The Fitness to Practice Committee of An Bord Altranais, for the purpose of holding an inquiry under Section 38(3) of the Nurses Act, 1985, has the powers, rights and privileges vested in the High Court or a judge thereof on the hearing of an action in respect of:

(i) the enforcement of the attendance of witnesses and their examination on oath or otherwise, and

(ii) the compelling of the production of documents;

and a summons signed by the Chairman of the Committee or by such other member of the Committee as may be authorised by the Committee shall be sufficient for enforcing the attendance of witnesses and compelling the production of documents.

(m) **The Dental Council (An Chomhairle Fiaclóireachta)**: The Fitness to Practice Committee of the Dental Council, for the purpose of holding an inquiry under Section 38(3) of the Dentists Act, 1985, has the powers, rights and privileges vested in the High Court or a judge thereof on the hearing of an action in respect of:

(i) the enforcement of the attendance of witnesses and their examination on oath or otherwise, and

(ii) the compelling of the production of documents

and a summons signed by the Chairman of the Committee or by such other member of the Committee as may be authorised by the Committee shall be sufficient for enforcing the attendance of witnesses and compelling the production of documents.
Health & Social Care Professionals Council: The Health & Social Care Professionals Council was established by statute in 2005 and began work in 2008. Its functions concern standards in the education, practice and policy of a number of professions. It also deals with fitness to practice issues of these professions. The professions designated under this legislation are:

(i) Chiropodist/podiatrist;
(ii) Clinical biochemist;
(iii) Dietician;
(iv) Medical scientist;
(v) Occupational therapist;
(vi) Physiotherapist;
(vii) Psychologist;
(viii) Radiographer;
(ix) Social care worker;
(x) Social worker;
(xii) Speech & Language therapist.

A committee of inquiry set up under this legislation has all the powers, rights and privileges that are vested in the court or a judge of the court with regard to enforcing the attendance and examination of witnesses as well as compelling the production of documents. The health professional does not have a right of access to a complainant’s medical file in a case whereby a complaint has been made to the relevant fitness to practice body.

Mental Health Tribunal: Under the Mental Health Act, 2001, a tribunal of Inquiry will be established to look into an involuntary admission to a psychiatric hospital. The Tribunal may demand the attendance of any individual and the production of any document or record it considers appropriate.

10. Informed Consent

Some general information is outlined below, however, the National Consent Advisory Group of the HSE has established a National Consent Policy. At the time of writing, the Group has published draft Policy on consent which should be consulted for further information. It is available at www.hse.ie

10.1 What is informed Consent?

Consent is based on the principle that individuals are entitled to choose freely whether or not to receive a medical intervention, use a service or participate in research and it endorses the concept of personal autonomy (i.e. the right to make decisions without external influence).
In order for consent to be deemed valid, informed and genuine, there are five criteria that must be met, namely:

(i) voluntariness;
(ii) the provision of information;
(iii) understanding;
(iv) competence; and
(v) the accurate recording of the individual’s decision.

(b) For the consent to be valid, the service user must:

(i) Have received sufficient information in a comprehensible manner about the nature, purpose, benefits and risks of an intervention/service or research project.
(ii) Not be acting under duress; and
(iii) Be competent to take the particular decision.

10.2 Alternatives to Consent – please also see Section 7

(a) In exceptional circumstances, information can be disclosed in the absence of consent. While there is no “public interest” test in the Data Protection Acts relating to the disclosure of personal data to third parties in the absence of consent, there are some circumstances where exceptions may be made in the absence of consent from the service user, including:

(i) when ordered by a judge in a Court of Law, or by a Tribunal established by an Act of the Oireachtas;
(ii) where required by other legislation;
(iii) where necessary to protect the welfare or vital interests of the service user or another individual; or
(iv) where urgently required to prevent injury or other damage to the health of a person.

(b) The following are everyday examples of such situations

(i) **Children’s information**: The law defines a child (or minor) as a person who has not reached 18 years (excluding a person who is or has been married). It is, however, provided by Section 23 of the Non-Fatal Offences Against the Person Act 1997 that a minor on reaching the age of 16 years, may give a valid consent in his or her own right to any prescribed medical treatment. Where the individual is below that age, consent may still be given but this requires that the medical practitioner involved must assess whether a child or minor has the maturity to understand and make his or her own decision about the proposed treatment.
Health care staff should therefore be very careful in relation to consent, disclosure and access issues, concerning the personal health information of persons under the age of 18 years. Health care staff should exercise professional judgement, on a case-by-case basis, on whether the entitlement to access should be exercisable by (a) the individual alone, (b) a parent or guardian alone, or (c) both jointly. In making a decision, particular regard should be had to the maturity of the minor concerned and to his or her best interests. Therefore, a minor’s personal health information may be released to a parent/guardian in accordance with the law and due regard to the best interests of the child.

(ii) **Incapacitated service user**: If a service user is unconscious or unable, due to mental or physical condition, to give consent or to communicate a decision, the health care staff concerned must take decisions about the use of information. This needs to take into account the service user’s best interest and any previously expressed wishes, and be informed by the views of relatives or carers as to the likely wishes of the service user.

(iii) **Serious threats to health**: In cases of emergency or when a service user is at serious risk, personal information may be disclosed for the purpose of preventing or reducing that risk or to avoid a serious and imminent danger to the life or health of any individual.

(iv) **Obligations to warn for the protection of the welfare of society**: There are a range of special circumstances where a health care provider will be excused from breaching confidentiality in order to protect the public. Some of these are established through statute, others through judicial interpretation of the law, usually known as common law, e.g. Section 8 of the Data Protection Acts.

(v) **General ‘Duty to Warn’ to protect members of the public**: Where a member of staff becomes aware, in the course of managing personal information of a service user, that a risk to public safety exists, they will be excused from breaching confidentiality where information is disclosed in order to protect the public. In this context ‘public safety’ includes instances where the risk is to a particular individual.

(vi) **Notifiable diseases**: Certain infectious diseases are subject to specific regulations, designed to protect public health. Section 29 of the Health Act, 1947 entitles the Minister for Health to specify which diseases are designated as Infectious Diseases. In relation to confidentiality, consent and disclosure issues, the Infectious Diseases Regulations require that records be maintained in a confidential manner and that the written consent of a service user be obtained before releasing identifying details. In the case of minors, consent may be given by a parent or guardian. The Minister may however certify that the obtaining of consent would not be “in the interest of the common good” in relation to certain records.
If a doctor finds that an individual is suffering from a communicable disease, the potential risk to public health and others must be carefully assessed. The doctor will have to have strict regard to the statutory obligations in the matter of reporting such a case. Where others may be at risk and not aware that an individual has a serious infection, a doctor is to attempt to obtain the person’s permission to tell them, so that medical, nursing and paramedics are better able to treat and manage them and also everyone coming into contact may take appropriate precautions. If the individual refuses consent to disclosure, the Medical Council considers that those who might be at risk of infection while treating the individual are to be informed of the risk to themselves. They, in turn, are of course bound by the general rules of confidentiality. There are several infectious diseases that are not included but would attract a duty of care to notify public health, e.g. HIV.

(vii) An Garda Síochána: Gardaí may access personal and medical records where there is written consent or on foot of a valid search warrant. The restrictions of the Data Protection Acts may be set aside on receipt of a letter from An Garda Síochána or the Defence Forces, signed by an officer not lower than a Chief Superintendent or Colonel stating that records are required in the interests of national security. Staff must still be satisfied that the information sought is warranted and justifiable. Under the Public Order Act 1994 (Section 19), it is a criminal offence to wilfully obstruct a Garda in the execution of his/her duty. HSE staff are under a common law duty of confidence requiring them not to disclose information which is obtained or comes to their attention during the course of their HSE employment. However this duty is not absolute and in certain limited circumstances may be overridden by an obligation to report crimes and provide information to the Gardai. The Criminal Justice Act, 2011 (section 19) states:

“A person shall be guilty of an offence if he or she has information which he or she knows or believes might be of material assistance in preventing the commission by any other person of a relevant offence, or securing the apprehension, prosecution or conviction of any other person for a relevant offence and fails without reasonable excuse to disclose that information as soon as it is practicable to do so to a member of the Garda Síochána.”

Such requests from the Gardai should, normally, be in written form. Where the treating health care staff in a hospital, or any other health service premises, become aware during the clinical management of a service user that a serious crime may have been committed it must be notified to the Gardai.

(viii) Court order: A court order is a direction or command of the Court. An application for an order affecting the HSE is usually made on notice to the HSE. The health care provider, its officers and staff are legally bound to comply with access requests covered by a court order, search warrant or other legal instrument.
If a staff member receives such a document, they must contact their senior line manager for advice and appropriate action. The manager should then refer the matter to their line manager who will contact the HSE’s legal advisors for guidance.

(ix) **Subpoena/witness summons:** A subpoena is issued by the High Court and a witness summons is issued by the Circuit Court and District Court. These are documents compelling witnesses to attend court and bring relevant information with them. If staff members receive a subpoena or witness summons they must contact their manager immediately.

(x) **Coroner:** The Coroner is an independent officer with responsibility under the law for the medico-legal investigation of certain deaths. The Coroner of the relevant district must be informed if certain deaths have taken place. A Coroner must enquire into the circumstances of sudden, unexplained, unnatural or violent deaths. In the case of sudden, unnatural or violent death there is a legal responsibility on the doctor, registrar of deaths, funeral undertaker, householder and the person in charge of any institution or premises in which the deceased person was residing at the time of death, to inform the Coroner. The death may be reported to a Sergeant of the Garda Siochana who will notify the Coroner. However, any person may notify the Coroner of the circumstances of a particular death. The notification must include the facts and circumstances relating to the death. Failure to comply with this requirement is a criminal offence. When the investigation is concluded it becomes a public record. If there is no inquest, the post mortem report becomes a public record, on conclusion of the investigation. In addition to the Coroners Act, all deaths in an approved centre (as defined by the Mental Health Act 2001 which replaced the Mental Treatment Act 1945) must be reported to the Coroner.

(xi) **Inquests:** An inquest is an inquiry in public by a coroner, sitting with or without a jury into the circumstances surrounding a death. By law, an inquest must be held when a death is due to unnatural causes. Before an inquest can be held, the final report from the pathologist (including any specialised tests) must be received by the coroner. In addition the inquest file which includes all of the draft depositions of potential witnesses and other information must be complete. Adequate notification must be given to the family, witnesses and all who have a proper interest in the inquest.

(xii) **Third party health providers:** The HSE’s Service Level Agreement under Section 38 and Section 39 of Health Act 2004 clearly outlines the providers’ requirement to comply with Data Protection legislation. The Service Level Agreements state that the providers must comply with all of the rules and policies governing the obtaining, retention, use, disclosure, security and deletion of information.
The Agreements also require the providers of services to promptly inform the HSE of any actual or suspected breach of security which would give rise to the actual or potential loss, theft, unauthorised release or disclosure of information or any part thereof. Organisations or agencies providing services to the HSE or on its behalf must also sign the HSE Service Provider Confidentiality Agreement.

11. **Keep data safe and secure**

11.1 High standards of physical and technical security are essential to protect the confidentiality of personal data. With the ever-increasing number of ways in which information can be shared, transmitted and exchanged, it is important to put in place measures to ensure the privacy and protection of this information.

11.2 All personal health information, whether in manual or electronic format, must be protected from unauthorised access, removal, alteration or loss through the use of appropriate security systems and record management controls.

11.3 The Data Protection Acts do not prescribe specific security standards. However, the HSE ICT Directorate has in conjunction with representatives from service, administrative and clinical areas developed the following policies:

(a) Information Security;
(b) Information technology;
(c) Electronic Communications;
(d) Password Standards;
(e) Encryption; and
(f) Mobile Phone Device.

The above polices are available on the HSE intranet site [http://hsenet.hse.ie](http://hsenet.hse.ie) on the ICT policy page.

11.4 **Paper Records**

The following guidelines should be followed with regard to personal and sensitive data held on paper files.

(a) Paper records and files containing personal data should be handled in such a way as to restrict access only to those with reasons to access them;

(b) Personal and sensitive information held on paper, must be kept hidden from public view e.g. callers to offices/nurses stations/public hatches. Care should be taken not to leave documents containing personal information where they may be visible or accessible to unauthorised persons. If Computers or VDUs are left unattended for a short period, staff must ensure that no personal information may be viewed. Access should be disabled where it is anticipated that computers or VDUs will be unattended for longer periods;
(c) Rooms, cabinets or drawers, in which personal records are stored, should be locked when unattended. A record should be maintained of files removed and returned;

(d) While appreciating the need for information to be accessible, staff must ensure that personal records are not left on desks or workstations at times when unauthorised access might take place;

(e) Staff should not take service user records home. In exceptional cases, where this cannot be avoided these records must be stored securely.

11.5 Electronic records

(a) If computers or VDUs are left unattended, staff must ensure that no personal information may be observed or accessed by unauthorised staff or members of the public. The use of secured screen savers is advised to reduce the chance of casual observation. Computer screens in public areas should be positioned so that they can only be viewed by authorised staff.

(b) Staff must not leave laptop computers or other portable electronic devices, and/or records containing personal information, unattended in cars. All records and portable equipment must be stored securely. If records containing personal information must be transported in a car, they should be locked securely in the boot of the car.

11.6 Conversations/Phone Calls/Voicemails/SMS (text) messages

(a) It is important to ensure that service user and/or staff information is not discussed in areas either among staff or by telephone where it is likely to be overheard.

(b) Personal information should not be given over the telephone unless it can be clearly established that the caller is whom they claim to be and proof of identity is essential. Staff must exercise caution and reasonable care in such cases, for example, checking with the caller for a payroll reference number, or a date of birth, or mother’s maiden name. It may also be appropriate to take a caller’s telephone number, and then check the validity of the number by ringing the number back.

(c) Personal information should not be left on voicemail/answering machine.

(d) SMS appointment reminders should only be sent where the person has been informed that they will receive them and has not objected. The content of the SMS must not contain medical information or test results.

11.7 Post

(a) Mail containing personal information should be marked clearly with “Strictly Private and Confidential”. If the information is particularly sensitive or proof of delivery is necessary, information of this nature should be sent by registered post.
11.8 Fax transmission

(a) Staff must respect the privacy of others at all times and only access fax messages where they are the intended recipient or they have a valid work related reason. If you receive a fax message and you are not the intended recipient you must contact the sender and notify them of the error. Fax machines must be physically secured and positioned to minimise the risk of unauthorised individuals accessing the equipment or viewing incoming messages.

(b) The following circumstances exist where it is acceptable to transmit confidential and personal information by fax:

(i) All persons identified in the fax message fully understand the risks and agree.

(ii) There are no other means available.

(iii) In a medical emergency where a delay would cause harm to a service user.

(c) The following steps are to be taken to maintain security and confidentiality when transmitting personal information by fax:

(i) The fax message must include a HSE fax cover sheet.

(ii) Only the minimum amount of information necessary should be included in the fax message.

(iii) Before sending the fax message, contact the intended recipient to ensure he/she is available to receive the fax at an agreed time.

(iv) Ensure that the correct number is dialled.

(v) Keep a copy of the transmission slip and contact the intended recipient to confirm receipt of the fax message.

(vi) Ensure that no copies of the fax message are left on the fax machine.

11.9 Telehealth

(a) Telehealth is the use of Information and Communication Technology (ICT) to deliver health services, expertise and information over distances. It includes Internet or web-based “e-health” and video-based applications. The use of this technology is relatively new and guidance in relation to privacy rights has not yet been developed.

(b) However as in other areas of personal health information there must be adherence to data protection and privacy laws. Security measures must be in place to protect any stored personal health information as well as the safeguarding of any personal health information in transit.
11.10 **Printing and copying**

(a) Paper records containing personal health information must not be copied unless it is essential to do so.

11.11 **Training and demonstrations**

(a) The anonymity of service users has to be maintained during research activities and at seminars and conferences. Use of photos, slides and other visual aids, which allow identification of individuals, must not occur unless the informed consent of the service user has been obtained.

11.12 **Use of Interpreters**

(a) Interpreters are obliged to keep confidential any information they may be privy to in the course of their duties. Confidentiality agreements are required for professional interpreters.

11.13 **Electronic health records**

(a) Electronic health records represent the potential to hold all diagnostic and personal medical information on computer databases. Electronic health records differ from paper records in many ways and warrant special consideration. It is possible to have multiple accesses to a single electronic record at different sites. It is possible to control access to an electronic record in a way that is not possible with a paper record. All of the principles of Data Protection apply to electronic health records.

11.14 **Electronic communication**

(a) In circumstances where it is necessary to transmit confidential or personal information via email, the following procedure must be followed:

(b) Only the minimum amount of confidential or personal information should be sent as is necessary for a given function to be carried out and the sender must take great care to ensure that it is sent only to the intended recipient(s).

(c) Where it is necessary to transmit confidential or personal information to an email address outside of the HSE domain (i.e. one that does not end in “@hse.ie”), the following additional procedure must be followed:

(i) The transfer must be made in accordance with the Data Protection Act 1988 and 2003.

(ii) The transfer must be authorised by the information owner and the local Consumer Affairs office. Such authorisation must be issued in advance of the first instance and may apply thereafter.

(iii) All confidential or personal information sent with the email message must be encrypted.

(iv) The password used to decrypt (read) the confidential or personal information must not be sent along with the original email message.
Further information on the HSE Encryption Policy is available on the HSE intranet at http://hsenet.hse.ie on the ICT policy page.

Confidential information regarding HSE business practices and procedures or personal information about any HSE service user, client or employee must not be posted or discussed on internet social networking websites, internet video hosting/sharing websites, internet discussion forums, message boards or internet chat rooms.

Confidential or personal information must only be transmitted via the public internet when the information has been encrypted and the transfer has been authorised by the information owner and the Consumer Affairs section.

### 11.15 Passwords

(a) Where possible all confidential and personal information must be stored on a secure HSE network server with restricted access. Where it has been deemed necessary by the information owner to store confidential or personal information on any device other than a HSE network server the information must be encrypted.

(b) All passwords must be unique and must be a minimum of 8 characters in length. If existing systems are not capable of supporting 8 characters, then the maximum number of characters allowed must be used. Passwords must contain a combination of letters (both upper & lower case), numbers (0-9) and at least one special character (for example: ", £, $, %, ^, &, *, @, #, ?, !, €). Passwords must not be left blank. No password may be re-used by a user within a 12 month period.

(c) User-level passwords such as those used to access HSE computer devices, information systems and networks must be changed at least every 90 days.

(d) System-level passwords such as those used by HSE information system administrators and network administrators must be changed at least every 60 days.

(e) Users must ensure passwords assigned to them are kept confidential at all times and are not shared with others including their co-workers or third parties. In exceptional circumstances where a password has to be written down, the password must be stored in a secure locked place, which is not easily accessible to others.

(f) The complete HSE Password Standards Policy is available on the HSE intranet at http://hsenet.hse.ie on the ICT policy page.

### 11.16 Encryption

(a) Confidential and personal information stored on shared HSE network servers which are situated in physically insecure locations (For example remote file/print servers) must be protected by the use of strict access controls and encryption.
(b) HSE desktop computers which for business or technical reasons need to store/host HSE clinical or employee information systems and/or confidential or personal information locally (as opposed to a secure HSE network server) must have HSE approved encryption software installed.

(c) All HSE laptop computer devices must have HSE approved encryption software installed prior to their use within the HSE. In addition to encryption software the laptop must be password protected and have up to date anti-virus software installed.

(d) Laptop and mobile computer devices must not be used for the long-term storage of confidential and personal information.

(e) Only HSE approved USB memory sticks which are distributed by the ICT Directorate maybe used to store or transfer HSE data. HSE I.T. security policies specifically prohibit the storage of HSE data on unapproved encrypted / unencrypted USB memory sticks and USB memory sticks which are the personal property of staff and are not owned or leased by the HSE.

(f) HSE employees who have been issued with a HSE approved USB memory stick must take all reasonable measures to ensure the memory stick is kept secure at all times and is protected against unauthorised access, damage, loss and theft.

(g) HSE approved USB memory sticks must only be used on an exceptional basis where it is essential to store or temporarily transfer confidential or personal data. They must not be used for the long term storage of confidential and personal data, which must where possible be stored on a secure HSE network server.

(h) The complete HSE Encryption Policy is available on the HSE intranet site http://hsenet.hse.ie on the ICT policy page

11.17 Mobile phones

(a) Users must ensure their HSE mobile phone device is protected at all times. As a minimum all mobile phone devices must be protected by the use of a Personal Identification Number (PIN). Where it is technically possible the mobile phone device must be password protected and all passwords must meet the requirements of HSE Password Standards Policy.

(b) Users must take all reasonable steps to prevent damage or loss to their mobile phone device. This includes not leaving it in view in an unattended vehicle and storing it securely when not in use. The user may be held responsible for any loss or damage to the mobile phone device, if it is found that reasonable precautions were not taken.

(c) Confidential and personal information should not be stored on a HSE mobile phone device. Unless the information is encrypted in accordance with the HSE encryption policy.
(d) In view of the need to observe confidentiality at all times, users must be vigilant when using their HSE mobile phone device in public places in order to avoid unwittingly disclosing sensitive employee, service user or client information.

(e) Users must respect the privacy of others at all times, and not attempt to access HSE mobile phone device calls, text messages, voice mail messages or any other information stored on a mobile phone device unless the assigned user of the device has granted them access.

(f) Mobile phone devices equipped with cameras must not be used inappropriately within the HSE. In this regard:

(g) All email messages sent from a HSE mobile phone device which contain confidential and/or personal information must be sent and encrypted in accordance with the HSE Electronic Communications Policy which is available on the HSE intranet http://hsenet.hse.ie on the ICT policy page.

(h) Users must report all lost or stolen mobile phone devices to their line manager and their local mobile phone administrator immediately.

(i) Local mobile phone administrators must report the incident to their senior manager, the mobile phone service provider and the relevant Assistant National Director of Finance immediately.

(j) Incidents where a lost or stolen HSE mobile phone device contained confidential or personal information must be reported and managed in accordance with the HSE Data Protection Breach Management Policy available on the HSE intranet site http://hsenet.hse.ie on the ICT policy page.

(k) The complete HSE Mobile Phone policy is available on the HSE intranet http://hsenet.hse.ie on the ICT policy page.

12. Keep data accurate, complete and up-to-date

12.1 Staff must ensure that personal data is kept up to date.

12.2 Procedures must be in place to ensure personal data held is accurate, including reviewing records on a regular basis, identifying areas where errors are most commonly made and providing training to eliminate those errors.

12.3 Every individual has a right to have any inaccurate information rectified or erased. Guidance on best practice in relation to healthcare records is available in the HSE Standards and Recommended Practices for Healthcare Records Management which can be accessed on the HSE intranet site http://hsenet.hse.ie

13. Ensure that data is adequate, relevant and not excessive.

13.1 HSE staff should ensure that the data they ask for and retain is the minimum amount needed for the specified purpose. The data must be adequate, relevant, and not be excessive.
Each department within the HSE must periodically examine the personal data sought by it and if there are no valid reasons for collecting certain data, then the practice must be reviewed immediately.

14. **Retain data for no longer than necessary for the purpose(s) for which it is acquired.**

14.1 Each department of the HSE must be clear about the length of time data will be kept and the reason why the information is being retained. To meet this requirement each Department should adhere to records management guidelines as set out in the 2012 Records Retention Policy.

14.2 **Disposal of records**

(a) When original records are selected for disposal in accordance with this policy, a clear disposal policy must be applied. It is vital that the process of record disposal safeguards and maintains the confidentiality of the records. This can be achieved internally or via an approved records shredding contractor, but it is the responsibility of the service to satisfy itself that the methods used provide adequate safeguards against accidental loss or disclosure of the records.

(b) A register of records destroyed should be maintained as proof that the records no longer exist. The register should show:

(i) name of the file;  
(ii) former location of file;  
(iii) dates covered by the file;  
(iv) date of destruction;  
(v) who gave the authority to destroy the records.

(c) For healthcare records, the register of records destroyed should also include:

(i) healthcare record number;  
(ii) surname;  
(iii) first name;  
(iv) address;  
(v) date of birth;

(d) For healthcare records, this register must be kept in perpetuity. The register should be signed by the relevant staff member and counter signed by their line manager.
14.3 **What is Confidential?**

(a) Any documents containing person identifiable information such as name, address, date of birth, PPS Number, Employee Number, medical record is deemed confidential. Other documents may also be confidential if they contain information about HSE business or finances. Examples of confidential documents include financial records, payroll records, personnel files, legal documents and/or healthcare records.

14.4 **Segregation of confidential waste**

(a) Only a minority of documents are confidential, and should be disposed in confidential paper wheelie bins or security bags. Alternative paper recycling options should be provided for non confidential paper/magazines etc.. Risk waste (yellow) bags/containers should never be used for the disposal of confidential healthcare records.

(b) Store confidential documents using locked wheelie bins or bags locked into a secure area. If HSE staff transport confidential documents within or between HSE sites, the confidential documents should never be viewed by members of the public.

14.5 **Disposal of Confidential Waste**

(a) There are two confidential waste disposal options: on site HSE shredding, or shredding by an approved waste contractor.

(b) **Shredding On-Site:** HSE staff may shred confidential records into confetti-like particles using in-house shredders.

This shredded paper can be recycled as part of a recyclables collection. Otherwise bags of confidential records can be collected for shredding in a shredding contractor’s vehicle on-site.

(c) **Shredding Off Site:** Confidential waste should be secure until uplift by the shredding contractor. Confidential waste bags/wheelie bins should be collected by the shredding contractor, and shredded off-site at an agreed location. If confidential waste is transported off site, documents should never be viewable to members of the public. It is the responsibility of the HSE manager in each location to comply with relevant waste management legislation. This contract would need to be subject to a data processing arrangement.

(d) Further information on the HSE Waste Management Policy is available on the HSE intranet site at [Waste_Management_Policy_and_Statement_of_Principles_.pdf](#).

15. **Give a copy of their personal data to the relevant individual, on request**

15.1 On making an access request any individual, about whom the HSE keeps personal data, is entitled to:
(a) a copy of the data being kept about him/her;

(b) know the purpose/s for processing his/her data;

(c) know the identity of those to whom the HSE discloses the data;

(d) know the source of the data, unless it is contrary to public interest;

(e) know the logic involved in automated decisions;

(f) a copy of any data held in the form of opinions, except where such opinions were given in confidence;

in each case, subject to certain restrictions set out in the Data Protection legislation.

15.2 How can a person access this information?

(a) The Freedom of Information (FOI) and Data Protection (DP) Acts provide a specific statutory regime and framework for people to seek access to their personal information and to obtain reasons for decisions which affect them. They also place huge responsibility on health service providers to keep accurate and up to date records, to keep records safe and secure and, subject to certain statutory safeguards and exceptions, to give people access to their personal records on request. (The Data Protection Acts only apply to people who are living).

15.3 Parliamentary Questions

(a) The HSE has a Standard Operating Procedure which sets out the procedures to be followed when dealing with the provision of information to elected public representatives and it can be accessed on the HSE intranet site http://hsenet.hse.ie.


16.1 Does a Data Protection request have to be in a specific form?

Yes, a request for access to records:

(a) must be in writing

(b) may be accompanied by a fee (up to and no more than €6.35)

(c) must specify the personal data required.

(d) The HSE is entitled to require from the applicant such information as may reasonably be required in order to satisfy itself of the identity of the applicant and to locate any relevant personal data.

16.2 What rules cover the use, disclosure and transfer of personal health information?

Personal health information should only be used or disclosed for the purpose for which it was collected or for another directly-related purpose.
It can be used or disclosed for some other purpose only where:

(a) the service user concerned has explicitly consented to the proposed use or disclosure;

(b) the health care staff reasonably believe 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 or public safety;

(c) the use or disclosure is required or authorised by law;

(d) the information concerns a service user who is incapable of giving consent, and is disclosed to a person responsible for the service user to enable appropriate care or treatment to be provided;

(e) any disclosure to a third party should be limited to that which is either authorised or required in order to achieve the desired objective;

(f) personal health information can be transferred to an individual or organisation outside the European Economic Area only in certain specified circumstances – further information in relation to this is available at www.dataprotection.ie

16.3 What entitlements do service users have to personal health information?

As a general rule, a service user is entitled to:

(a) have access to their personal health information irrespective of the form in which it is kept;

(b) know the sources of that information, the purposes for which it is being held and the parties to which it is intended to disclose it;

(c) have any personal health information concerning them enhanced, corrected, blocked or otherwise amended to make it consistent with the rules set out above.

16.4 Can access be refused?

Access can be refused to some or all of the service user’s personal health information only if providing access is likely to cause serious harm to the physical or mental health of the requester or providing access would disclose the personal data of another person without their consent or would disclose a confidential expression of opinion about the requester or the disclosure is otherwise not required by law.

16.5 If the requester is unhappy with the initial decision what avenue is open to them?

Unlike the FOI Acts there is no internal review stage under Data Protection legislation. However, the requester has a right to complain to the Data Protection Commissioner who may carry out an independent investigation of the matter.
16.6 **Must all requests for information or access to records be made under the Data Protection Acts?**

No—many requests may involve the release of documents, which may be accessed without resort to the Data Protection Acts. The HSE has an Administrative Access Policy which provides guidance on the release of documents outside of the Data Protection Acts.

16.7 **What if the request has already been dealt with under the Freedom of Information Acts?**

The request is to be processed separately under the Data Protection process as if it were a new request. Each constitutes a discrete, self-contained statutory regime.

In addition to the rights arising from the obligations imposed on Data Controllers by the 8 Rules of Data Protection, service users also have the following rights:

(a) **Right of rectification or erasure:** Service users have the right to have information which is inaccurate rectified, or in some cases have the information erased.

(b) **Right to block certain uses:** A service user can prevent their personal data from being used for certain purposes, e.g. research.

(c) **Right to object:** A service user, if they feel that the use of their data involves substantial and unwarranted damage or distress to them, may request a data controller to stop using this personal data, or not to start using the data.

The right does not apply if:

(d) Consent has already been obtained;

(e) The use is necessary for a contractual obligation;

(f) The use is required by law;

(g) The processing is to protect the vital interests of the data subject.

16.8 **Employment rights**

Nobody can be forced, as a condition of recruitment, employment or the provision of a service, to make an access request, or to reveal the results of such a request. Where vetting for employment purposes is necessary, this can be facilitated where the individual gives consent to the data controller to release personal data to a third party.

17. **Freedom of Information Acts, 1997 and 2003**

The Freedom of Information Acts confer on all persons the right to seek access to information held by public bodies, to the greatest extent possible, consistent with the public interest, the right to privacy and the rights of third parties.
The Freedom of Information legislation provides that every individual has the right to apply for access to records (personal or non-personal) held by a public body and to have inaccurate or misleading personal information amended, corrected, or deleted. (*subject to specific exemptions, having regard to the public interest and the right to privacy)

17.1 **Decisions of Public Bodies affecting the person**

Individuals who are affected by decisions of public bodies have the right to know the criteria used in making those decisions.

17.2 **Parents, guardians and next-of-kin rights**:  
Parents, guardians and next-of-kin have the following rights in respect of certain other persons e.g. children, deceased or persons with a mental incapacity:

(a) right of access to records

(b) right of amendment of records, if they are incomplete, incorrect or misleading

(c) right to reasons for decisions.

(*subject to the provisions of the FOI Acts)

17.3 **What is personal information in the context of the FOI Acts?**

Personal Information is considered to be information which *would ordinarily be known only to the individual or their family or friends* or *is held by a public body on the understanding that it would be treated as confidential*.

(a) Personal information includes information relating to:

(i) educational, medical, psychiatric, or psychological history

(ii) financial affairs of individual

(A) employment and employment history

(B) personnel records

(C) criminal history

(D) religion, age, sexual orientation or marital status

(E) social welfare entitlements

(F) assessment of liability to pay tax or duty to state or public bodies

(G) property of the individual
name, symbol or code identifying an individual in public records containing personal information;
views or opinions of another person about the individual.

Personal information for staff of public bodies does not include:
(iii) names of staff members (but not any private information such as home address);
(iv) information relating to office/position held;
(A) terms of occupancy of position or terms of the contract;
(B) anything written or recorded by a staff member in the course of performing their functions of their office or position.

This type of staff information may be released, subject to the need to protect the public interest and right to privacy.

17.4 What is a record according to the FOI Acts?

A record can include:
(a) paper records: books, files, letters, loose papers, diaries, post-it notes, and computer printouts;
(b) electromagnetic records: disks, servers, databases;
   (i) audio-visual records: films, tapes, videos, CDs;
   (ii) visual records: photographs, maps, plans, X-Rays, microfiche, microfilm.

17.5 What records can be requested under the FOI Acts?

(a) all records created after the Act commenced for the former Health Boards on 21st October, 1998;
(b) personal records of, whenever created
   (i) personnel records of staff created after 21st October 1995 or earlier if such records are being used, or are proposed to be used, adversely against a staff member
   (ii) earlier records, if accessible, in order to understand later records.

17.6 To whom are requests for access under the FOI Acts addressed, and who makes the decision to grant or refuse access?

The Acts stipulate that applications are to be made to the ‘head of the public body’, that is, in the case of the HSE, the CEO. In practice this function will be delegated by the CEO, under Section 19 of the Health Act 2004, to officers in the various services, who will act as delegated Decision-Makers.
The Decision-Makers consider requests under the Freedom of Information Acts and decide whether or not records can be released, bearing in mind the requirements of the Acts to protect confidentiality, having regard to the public interest and the right to privacy.

17.7 Does an FOI request have to be in a specific form?

A request under the acts must:

- be in writing
- specify the records required and the manner in which access is sought e.g. inspect the originals, obtain photocopies etc
- state that the request is being made under the FOI Acts

17.8 What are the statutory charges/fees?

<table>
<thead>
<tr>
<th>Type of Request/Application</th>
<th>Standard Fee*</th>
<th>Reduced Fee**</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request for a record under section 7 for non-personal information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Initial Request</td>
<td>€15</td>
<td>€10</td>
</tr>
<tr>
<td>Internal Appeal</td>
<td>€75</td>
<td>€25</td>
</tr>
<tr>
<td>Appeal to Information Commissioner</td>
<td>€150</td>
<td>€50</td>
</tr>
<tr>
<td>Request under section 7 for personal information</td>
<td>No charge</td>
<td>No charge</td>
</tr>
<tr>
<td>Application under section 17 for amendment of a record containing incorrect, incomplete or misleading personal information</td>
<td>No charge</td>
<td>No charge</td>
</tr>
<tr>
<td>Application under section 18 for the reasons for a decision affecting the individual</td>
<td>No charge</td>
<td>No charge</td>
</tr>
</tbody>
</table>

*Fee will not apply where a person appeals a decision to charge a fee or deposit, or a fee or deposit of a particular amount under section 47 of the FOI Acts

** Please note that fees are correct at the time of printing, please check [www.hse.ie](http://www.hse.ie) for updates.

***Reduced fee will apply in respect of medical card holders or dependants of a medical card holder and third parties who appeal a decision of a public body to release their information on public interest grounds.
If the requester is unhappy with the initial decision what other option is open to them?

The first option is for the requester to seek an internal review. This is forwarded to the delegated Internal Reviewer (who is a more senior member of staff than the initial Decision Maker). A decision is required to be made within 15 working days from the date of receipt of the request for an internal review.

If the requester is unhappy with the decision of the Internal Reviewer, they can appeal to the Information Commissioner (established under Section 33 of the FOI Acts (1997-2003)). The appeal is to be made within 6 months of the date of notification of the HSE’s decision. There is a right of appeal to the High Court, on a point of law only, if either the requester or the HSE is unhappy with the Commissioner’s decision. The Supreme Court deals with any further appeal arising out of a High Court decision.

Can staff seek access to their personnel records?

Staff of the HSE are entitled, under section 6 of the FOI Act 1997 & 2003, to seek access to their personnel records, created on or after 21st October, 1995 - up to three years prior to commencement of the Act. Earlier records can be accessed if such records are being used, or are proposed to be used, in a way which adversely affects the staff member.

Access is to be provided, in accordance with these provisions, either by allowing inspection of the original record or by making photocopies, whichever is preferred by the staff member, having regard to the need to protect privacy and the public interest.

Are the records of contracted service providers covered by the FOI Acts?

Yes, the Acts state that records in the possession of a person providing a service for the HSE under a contract shall in so far as it relates to the service be regarded as being held by the HSE.

Community pharmacists, general practitioners, opticians, private dentists and other professionals provide services on behalf of the HSE on a contract for service basis. The Freedom of Information Acts apply to their records insofar as they relate to the services provided under contract.

The FOI Acts do not apply to private arrangements made between the service user and private healthcare providers outside of any contractual scheme with the HSE; however, for access to personal information the Data Protection Acts apply to such private practice - a private service user of a GP may apply under the Data Protection Acts for access to their records.

Administrative access policy

As a matter of policy, the HSE supports the right of a service user to see what information is held about them within its service.
Generally, access to personal health information is to be provided administratively, that is outside the legislative process, subject to exceptions which are detailed below.

18.1 **Does an administrative request have to be in a specific form?**

Yes an application for administrative access by a service user seeking access to their health record has to:

(a) be in writing and sent to the appropriate service manager;

(b) supply relevant information to locate records;

(c) be accompanied by appropriate identification.

The treating health care staff, where possible, are to be consulted in the handling of these applications to ensure that only information relevant to the application is released. Consultation with the service user is encouraged, particularly to assist in identification of the actual documents to which access is sought or to narrow the field of inquiry, for example, to a particular episode of care.

18.2 **When is the decision due?**

An acknowledgement is usually issued within three working days of receiving the request. Access to the health record is to take place within 15 days of receipt of the application. Where a decision cannot be reached within the 15 working day deadline, the applicant has to be informed of this, giving the reasons for the delay and the approximate date when a decision is likely to be made.

18.3 **Requests by third-parties**

Where possible, service users are to be encouraged to apply personally for their health records. However, the service user may consent in writing for a third party to have access to their health records. The third party may include, but is not limited to, a relative, medical practitioner or a legal representative.

18.4 **Persons with an intellectual disability**

Where a request is made on behalf of a person with an intellectual disability, the officer processing the request is to take into account the following:

(a) the relationship of the requester to the service user

(b) the reasons for the request

(c) the best interests of the service user concerned

When dealing with persons with intellectual, physical or sensory disabilities, the HSE has adopted various guidance and policies which can be accessed on the HSE intranet site at http://hsenet.hse.ie.
18.5 **Records of deceased persons**

All applications for access to deceased person’s records must be processed under the Freedom of Information Acts.

18.6 **Exceptions to the administrative access process**

Greater care must be taken where health records contain particularly sensitive information, for example:
(i) documents relating to suspected or actual child abuse
(ii) documents revealing the involvement and deliberations of an investigation into alleged sexual abuse
(iii) documents containing information in relation to testing for and/or treatment of HIV/Aids (including statements regarding HIV Status) and notifiable diseases under the Health Acts
(iv) deceased person’s health record
(v) in circumstances where it is considered that access might be prejudicial to the physical or mental well being or emotional condition of the person
(vi) in circumstances where it is considered that the health record contains information about a third party or information received in confidence from a third party
(vii) any other sensitive information such as documents revealing confidential sources of information
(viii) any application by an adoptee applying for access to birth-related information

The requester is to be made aware that such requests are to be made under the Freedom of Information Acts and forwarded to the relevant FOI/DP Decision Maker or Consumer Affairs Area Office.

18.7 **Is there a fee involved when requesting access under the administrative access route?**

No, a copy of the health record is usually provided free of charge to the requester unless a large number of records is involved. Copies of x-rays, videos and photographs can be provided at an appropriate copying charge. Where a report is requested which requires the creation of a new document, current policy regarding charges for the production of such reports is to apply.

19. **Data Protection Breach Management Policy**

19.1 There are five elements to the HSE’s data breach management plan:

(a) Identification and Classification;
(b) Containment and Recovery;
(c) Risk Assessment;
(d) Notification of Breach; and
(e) Evaluation and Response.
19.2 **Identification and Classification**

Directorates must put in place procedures that will allow any staff member to report any information/data security breach. It is important that all staff are aware to whom they should report such a breach. Having such a procedure in place will allow for early recognition of the breach so that it can be dealt with in the most appropriate manner. Details of the breach should be recorded accurately, including the date and time the breach occurred, the date and time it was detected, who/what reported the breach, description of the breach, details of any ICT systems involved, corroborating material such as error messages, log files, etc. In this respect, staff need to be made fully aware as to what constitutes a breach. In respect of this policy a breach maybe defined as the unintentional release of HSE confidential or personal information/data to unauthorised persons, either through the accidental disclosure, loss or theft of the information/data.

19.3 **Containment and Recovery**

Containment involves limiting the scope and impact of the breach of data/information. If a breach occurs, Directorates should:

(a) decide on who would take the lead in investigating the breach and ensure that the appropriate resources are made available for the investigation.

(b) establish who in the organisation needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. For example, this might entail isolating a compromised section of the network, finding a lost file or piece of equipment, or simply changing access codes to server rooms, etc.

(c) establish whether there is anything that can be done to recover losses and limit the damage the breach can cause.

19.4 **Risk Assessment**

In assessing the risk arising from the security breach, Directorates should consider what would be the potential adverse consequences for individuals, i.e. how likely it is that adverse consequences will materialise and, in the event of materialising, how serious or substantial are they likely to be. In assessing the risk, Directorates should consider the following points:

(a) What type of Information/data is involved?

(b) How sensitive is the information/data?

(c) Are there any security mechanisms in place (e.g. password, protected, encryption)?

(d) What could the information/data tell a third party about the individual?

(e) How many individuals’ are affected by the breach?
19.5 **Notification of Breaches**

All information/data breaches must be reported to the Consumer Affairs or ICT Directorate immediately. Members of staff and their line manager must complete a Data Breach Incident Report and forward (via fax or email a scanned copy) this to their local Consumer Affairs Officer for breaches involving manual (paper based) information/data or the their local ICT call centre/helpdesk for breaches involving electronic data.

Please note; Data Protection Breaches have to be reported to the Data Protection Commissioner. In that regard the Area Consumer Affairs/Regional Consumer Affairs officers are the **only HSE officers designated** to report a breach to the Data Protection Commissioner. Under no circumstances should directorates inform the Data Protection Commissioner’s Office directly of a breach.

Directorates should consider notifying third parties such as the Gardaí if necessary.

19.6 **Evaluation and Response**

(a) Subsequent to any information/data security breach a thorough review of the incident should occur. The purpose of this review is to ensure that the steps taken during the incident were appropriate and to identify areas that may need to be improved. Any recommended change to policies and/or procedures should be documented and implemented as soon as possible thereafter.

(b) Each Directorate should identify a group of people within the organisation who will be responsible for reacting to reported breaches of security.

19.7 **Roles and Responsibilities**

Line Managers are responsible for:

(a) The implementation of this policy and all other relevant HSE policies within the business areas for which they are responsible.

(b) Ensuring that all HSE employees who report to them are made aware of and are instructed to comply with this policy and all other related HSE policies.

(c) Consulting with the Consumer Affairs and/or the ICT Directorate in relation to the appropriate procedures to follow when a breach of this policy has occurred.

(d) Each user is responsible for:

(e) Complying with the terms of this policy and all other relevant HSE policies, procedures, regulations and applicable legislation;

(f) Respecting and protecting the privacy and confidentiality of the information they process at all times;

(g) Reporting all misuse and breaches of this policy to their line manager.
20. **Enforcement**

20.1 The HSE reserves the right to take such action as it deems appropriate against users who breach the conditions of this policy. HSE employees who breach this policy may be denied access to the organizations information technology resources and may be subject to disciplinary action, including suspension and dismissal as provided for in the HSE disciplinary procedure.

21. **Contact details HSE Area Consumer Affairs Offices**

Contact details for HSE Area Consumer Affairs Offices:

<table>
<thead>
<tr>
<th>Dublin Mid Leinster</th>
<th>HSE Dublin North East - Cavan</th>
<th>HSE West - Galway</th>
<th>HSE South - Kilkenny</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tullamore:</strong></td>
<td>Tel: 045 880494</td>
<td>Tel: 049 4377343</td>
<td>Tel 056-7785598</td>
</tr>
<tr>
<td>Fax: 1890 200 894</td>
<td>Fax: 049 4377379</td>
<td>Fax: 046 9251264</td>
<td>Fax 056-7785549</td>
</tr>
<tr>
<td><strong>Naas:</strong></td>
<td>Kells:</td>
<td>Kells:</td>
<td><strong>Cork:</strong></td>
</tr>
<tr>
<td>Tel 057-9357876</td>
<td>Tel: 046 9251774</td>
<td>Tel 061-483286 / 87</td>
<td>Tel 021 4923708</td>
</tr>
<tr>
<td>Fax 057-9357881</td>
<td>Swords:</td>
<td>Fax 061 483350</td>
<td>Fax 021 4923627</td>
</tr>
<tr>
<td><strong>Naas:</strong></td>
<td>Tel: 01 8908728</td>
<td>Donegal:</td>
<td><strong>Donegal:</strong></td>
</tr>
<tr>
<td>Tel 045 880494</td>
<td>Fax: 01 8131882</td>
<td>Tel 074-9189152</td>
<td>Tel 074 9130380</td>
</tr>
<tr>
<td>Fax 1890 200 894</td>
<td></td>
<td>Fax 074 9130380</td>
<td></td>
</tr>
</tbody>
</table>

National Lead Office -
Freedom of Information, Data Protection & Record Management
Block 4, Central Business Park,
Clonminch,
Tullamore,
Co. Offaly
Tel: (057) 935 7879
22. **Appendices**

22.1 A full list of the Health Service Data Protection Policies and Record Management Policy are available on the HSE intranet at:

http://hsenet.hse.ie/HSE_Central/Consumer_Affairs/Access/Data_Protection/dpdocs.html