NURSING AND MIDWIFERY CONSULTATION ON THE PROPOSED HEALTH INFORMATION BILL

AN INFORMATICS PERSPECTIVE

Submitted by
Jim Brown, Director and
Paula Kavanagh-Nursing Informatics Officer
NMPDU, HSE West-Ballyshannon

September 2008
# Table of Contents

1 Summary 3

2 Introduction 3

3 Purpose of Health Information Bill 4

4 Legislative Framework 4

5 Definition Personal Data 4

6 Principles of Data Protection 5

7 Information Concepts 5  
   - Privacy 6  
   - Confidentiality 6  
   - Consent 6  
   - Security 7  
   - Integrity 7

8 Information Technologies 7  
   - Electronic Health Record 7  
   - Internet Based Health Accounts 7  
   - Information Databases 8  
   - Telehealth 10

9 Framework for Information Governance 11

10 Reports of Relevance 13

11 Appendices 14  
   I. Swot Analysis of Technologies 14  
   II. Patient Empowerment in Health Record Management 16  
   III. Extract GoogleHealth Record Available in Ireland 17  
   IV. Extract CSO-Example of Information Databases 18  
   V. Extract Health Informatics Review NHS 2008 19
Summary

This discussion document outlines the purpose of the Health Information Bill from an informatics perspective. It reiterates the legislative framework, taking cognisance of the definition of personal data and the electronic movement of personal information under the principles of data protection. Information concepts of privacy, confidentiality, consent, security and integrity of electronic data are outlined. Information technologies (IT) are explored in relation to the electronic health record and the corresponding information governance structures required. Key information sharing concepts are explored in the context of the use of data for health care management and the issues underpinning the information governance framework for health. A brief listing of reports relating to health information and informatics is provided.

Introduction

The discussion paper (provided by the Department of Health and Children) is thorough and offers a valuable literature review on health information internationally, and covers the legislative framework well. The impact of technology on information management needs further emphasis. Information collection, usage and sharing has been transformed through the use of computers and technology. The scale, speed of access, dissemination and share ability of information is immeasurable with standards of ten years ago. It is near impossible to predict what new heights data sharing may reach. The health information bill is planned at an opportune time to take into account the information age and the move from paper to pc (personal computer), with changes in practice in information storage, moving from hard copy to hard drive. This bill is required to take cognisance of the changes in information management, taking account of the culture of different organisations in dealing with patient information, clarifying the legislative position and information governance framework required and the role of the Health Information Quality Authority in its enactment.

A brief outline is offered on the following topics:

- Purpose of Health Information Bill
- Legislative Framework
- Definition Personal Data
- Principles of Data Protection
- Information Concepts
  - Privacy
  - Confidentiality
  - Consent
  - Security
  - Integrity
- Information Technologies
  - Electronic Health Record
  - Internet Based Health Accounts
  - Information Databases
- Framework for Information Governance
Purpose of the Health Information Bill

**Purpose of the Bill** - Better use of personal health information for improved patient care and safety.

- To establish a **Legislative Framework** to enable information to be used to best effect to enhance medical and patient safety.
- To facilitate the greater use of **Information Technologies** for better delivery of patient services.
- To underpin an effective **Information Governance Structure** for the health system generally.

**Legislative Framework**

Personal health information is private and sensitive and patient expectations are that this information will remain private and confidential and secure at all times. Information sharing is an integral part of nursing and midwifery practice. Nurses and midwives are bound by:

- The EU-Data Protection Directive (Directive 95/46/EC)
- National Law
- The Constitution of Ireland (Right to Privacy and Dignity)

All the above legislative documents play a significant role in information management in the healthcare setting and are covered comprehensively in the discussion document. The Code of Professional Conduct (2000) does outline the potential dangers to confidentiality of computers and electronic processing, but may need to be more explicit in relation to electronic information exchange.

**Personal Data**

**Personal Health Information** as outlined in the discussion paper needs an accurate definition and is a crucial element of the Health Information Act and information sharing. Data is deemed personal if it enables someone to link information to a specific person.

**Definition of Personal Data**

“Any information relating to an identified or identifiable natural person, (An identifiable person is one who can be identified, directly or indirectly in particular by reference to an identifiable number or one or more factors specific to physical, physiological, mental, economic, cultural or social identity)”  

**Directive 95/46/EC**

The definition of personal data can be clear cut, in relation to information traditionally collected, such as name, personal public services number (PPS) and date of birth, but becomes less so when dealing with sensitive data such as racial origin, political or religious information, physical and mental health information and information pertaining to sexual life and criminal convictions.
Data relating to the individual, such as email correspondence, digital photos of clinical wounds, digital x rays taken of chest etc, electrocardiogram digital recordings, digital recordings of voice consent, etc, form another category of personal information that requires attention.

The fluidity of data is a positive element of the electronic age but brings its own risks. In tracking data, information can be collected, recorded, used, organised, filed, stored, modified, edited, deleted, retrieved, disposed of, transmitted, disseminated and/or published. Within this level of activity and movement, it is paramount that the principles of data protection are adhered to and the concepts of privacy, confidentiality, consent, security and integrity are maintained.

**Principles of Data Protection**

The EU Data Protection Directive (Directive 95/46/EC), adopted by the European Union, is designed to protect the privacy and protection of all personal data, collected for or about citizens of the EU. Directive 95/46/EC takes into account all key elements of the European Convention on Human Rights, which respect the rights of privacy in personal and family life, as well as in the home and in personal correspondence. It deals with processing, using, or exchanging any such data within the EU and has been adopted and incorporated into the Data Protection Act (1988) and Amendment (2003) in Ireland.

The Seven Principles of the EU Directive 94/46/EC are:

- **Notice**: subjects whose data is being collected should be given notice of such collection.
- **Purpose**: data collected should be used only for stated purpose(s) and for no other purposes.
- **Consent**: personal data should not be disclosed or shared with third parties without consent from its subject(s).
- **Security**: once collected, personal data should be kept safe and secure from potential abuse, theft, or loss.
- **Disclosure**: subjects whose personal data is being collected should be informed as to the party or parties collecting such data.
- **Access**: subjects should be granted access to their personal data and allowed to correct any inaccuracies.
- **Accountability**: subjects should be able to hold personal data collectors accountable for adhering to all seven of these principles.

**Information Concepts**

Information obtained by nurses and midwives, in their professional capacity, to provide care, have an ethical and legal obligation to ensure privacy and confidentiality of that information. The following key concepts are outlined and explored:

- **Privacy**: The right to control how individual information is obtained, used and disclosed
- **Confidentiality**: Duty to safeguard the information entrusted to an individual as part of care contract
- **Consent**: Informed Consent-explicit versus implicit debate
Health Information Bill- Nursing and Midwifery Perspective

- **Security** - Measures to safeguard information from unauthorised access, use or disclosure.
- **Integrity** – Consistency and Accuracy of records and data

**Privacy**

Privacy is the right to control how an individual’s own information is obtained, used and disclosed. The HRB (2008) highlight the protection of an individual’s privacy and confidentiality and assurances and security measures to ensure protection, will be central to successful data protection practice in healthcare, medical research and public health. The unique identifier issue has raised many concerns in relation to public privacy as it is seen to undermine the individual’s control of information by allowing numerous organisations, who wish to use this number to obtain information without the individual’s knowledge or consent.

**Confidentiality**

Confidentiality of information is a requirement within the health service and must be assured to enable patients disclose sensitive information necessary for their healthcare. Patients have a right to control and determine individual’s access to their own health information. Every decision to disclose confidential patient information outside the healthcare services violates the patient’s right to privacy, and is in breach of the healthcare professional’s obligation of confidentiality. The disclosure will only be justified in exceptional circumstances, that is, if the disclosure serves an interest that in the particular circumstances outweighs the patient’s right to privacy. Disclosure may occur in order to protect the overriding interests of third parties or to protect public interest. The Health Information-A National Strategy Report (2004) highlights the occasions on which information can be divulged:

- On obtaining Explicit Consent from the Patient
- With Implied Consent from the Patient for Predetermined Purposes
- To Prevent Substantial Harm to the Patient or Third Party
- As Required by Court Order or Statute
- Public Interest Requires it

Other exceptions noted are for the National Cancer Registry (Health Act 2007) and for Notifiable Infectious Diseases (Health Act 1947)

**Consent**

Consent is defined as “any freely given specific and informed indication of his/her wishes by which the data subject signifies his/her agreement to personal data relating to him/her being processed”

EU Data Directive (95/46/EC)

In a recent study entitled Data Sharing Review undertaken by Richard Thomas and Mark Walport for the Prime Minister of Britain (2008), the predominant view of consent is that people should be able to exercise choice and control over information about themselves. They speak of proportionality where a number of factors need to be considered and balancing the opportunity to prevent harm with implications of breech in individual privacy.
The Discussion Paper from the DOHC (2008) highlights the conflict between the rights of the patient to determine who has access to their medical records and the needs of the health service to use patient information for a range of purposes that will improve service planning and benefit society as a whole. It outlines the debate between explicit consent (clearly and unmistakably stated by the patient, recorded, and witnessed) and implicit consent (consent is inferred within a circle of care, allowing information sharing among health professionals in that episode of care). It is within the bracket of implicit consent, where ambiguities lie, particularly in terms of research, education, planning and administration. Data disclosure should not be led by uncertainty over legal and ethical rules. The Irish Data Protection Commissioner stresses the importance of clear guidelines on what is and what is not permissible.

Security

Personal health information should be held securely, safely and consistently. Appropriate measures need to be taken to safeguard that information against unauthorised access or use. Records held electronically need full protection against misuse, inappropriate use or unauthorised use.

Integrity

The consistency and accuracy of the data must be maintained at all times. Malicious and/or accidental interference with the health record must be prevented by having appropriate security measures in place and a tracking device which identifies all data viewers, data inputters and data editors (including deletion) to that record. Many critical decisions are now made on the strength of electronic data which may not be evident on a paper trail and must be wholly trustworthy.

Information Technologies

Electronic Health Record

The electronic health record has been offered as a major solution for information management in the healthcare arena. In providing access to an electronic record, one must be clear as to what the electronic health record (EHR) is. The EHR has been defined by the International Standards Organisation (ISO) in Health Informatics as “a repository of information stored electronically, accessible by multiple users in a standardised format with the purpose of supporting information availability to those who need it when they need it” (ISO 2005). Simply, the EHR is an electronic system listing every health visit exchange, and tracking events as they happen. The EHR holds databases of information on set target groups and populations and is a vital tool for forward planning and population mapping, as well as offering substantial educational benefits to health care professionals.

The electronic patient record (EPR) is the individual collection of health records pertaining to one client and forms part of the greater electronic health record. It is fundamentally important to get the EPR right so that information can be standardised in the EHR and shared across health services. When all systems of health information are capable of sharing, the EHR then becomes an effective tool. The electronic health record, as discussed in the Discussion Paper on the Proposed Health Information Bill (DOHC 2008) offers seamless, integrated care across all sectors of healthcare and can contribute greatly to care delivery, when combined with health information systems
such as financial, risk assessment, adverse reporting systems and evidence based databases.

In developing the EHR in Ireland, information exchange and access to information electronically must take cognisance of the data protection issues that arise. Issues with large collections of data held in the EHR can occur when the purpose of data usage is diverse. In cases of paper records, breaches of confidentiality could occur, but were limited to time, place and opportunity.

With electronic records, the potential risk of breach is much higher, as large volumes of information are accessible, through a computer, in numerous locations, to many people. People at various levels of an organisation, require different information from the EHR. In order to ensure that the right people, access the right information, strict levels of entry to data information must exist, with privilege levels set appropriately. Information extracted from the EHR is high risk data as it no longer has the security mechanisms of the EHR system. Encryption of the data on extraction is not widespread. USB keys or disks can now hold vast quantities of data and while offering immediate access for reference to the employee, they offer a major security threat to patient confidentiality.

Another issue with the EHR is data inputting of information. Mistakes may not be easy to recognise electronically and may be taken as fact, leading to the wrong prescription being written, the wrong results scanned to a patient’s record, the wrong allergy alert placed on the chart, a wrong care entry with follow on care plan enacted, all of which can have devastating consequences. So while it can lead to prevention of risk when used correctly, it can rise the risk substantially if care is not taken with data entry. The following issues can arise with the EHR:

- Privilege Level not Appropriate or Wrongful Access
- Unwieldy Access to Information due to Privilege Levels and Information Levels
- Lack of Respect/Understanding for Confidentiality of the Electronic Patient Record
- Security of Information via Password
- Screen Blocks and Awareness while Screens are Active (Prevent onlookers access)
- Automatic Shutdown of Screen Fields (if computer left unattended)
- Data Entry Inaccuracies, or Wrong Record Entry
- Security of Data within the System
- Ability to Download Information to USB Ports-Risk of Security Breech
- Laptop Use and Risk of Theft or Loss
- Theft or Loss of Portable Device such as USB Key, Disks or CD’s

Centrally Managed Health System-Internet Based

A major issue with the EHR is ownership of information. Health information is seen to belong to the individual to whom it relates (DOHC 2004). With the EHR, the health Service is the custodian of the information for the client. This then opens the debate as to control and access to that data by relevant health care professionals and clients themselves. The NHS has made significant progress in relation to the development of the EHR across the NHS, but has met much resistance to information access and sharing, from both clients and health care professionals.
The summary care record (SCR), developed in the NHS, as part of their national programme for IT(NPfIT) is a centrally stored health summary, created from a person’s general practitioner record and stored on a secure Extranet (N3). The plan of action is to have SCR’s for all patients of the NHS. This has met much resistance from patients who do not wish their data to be shared. (There is an opt-out clause for patients but this in turn defeats the future purpose of the SCR).

There is resistance from GP’s who feel it is a breach of confidentiality to upload sensitive and confidential information to the SCR without prior consent, which is taken as implicit unless the opt-out clause is enacted. This puts patients at risk who do not have an understanding of the concept.

Another concept in development by the NHS is HealthSpace, which is a separate secure internet based site, which allows patients to record and organise their own health records. This is a facility provided for the patient to assist them in planning and managing their own health. Only 0.12% of invited clients have actually set up this account (UCL 2008). This concept needs investigation from another perspective, where patients hold summary access to all health encounters, on an electronic “health card” which could be automatically loaded to a centrally run patient health account system. The patient could grant access to health professionals at each subsequent health encounter, depending on relevancy. (Appendix Two)

This concept of the patient owning and managing the record suggests that health institutions give an account of their services and the outcomes of care to all patients electronically, which is then stored on a secure internet health account. This concept differs from the healthcare institutions holding the record and requesting permission to share the information. This paradigm shift from symptom based hospital centred system approaches to preventative person centred health systems will mean a re-examination of the management and ownership of health information in Ireland. In empowering clients to manage their health, clients need to be offered the tools to manage their health records.

Returning client health information to patients and planning for them to control this information in an electronic enabled environment is a direction that needs to be investigated and facilitated. HealthSpace has begun this process in the UK. GoogleHealth is a US based model of online access to health records solely in the hands of the client. This system is live in the US only, in its full capacity. It is available worldwide in information storage mode but does not facilitate information sharing outside of the US. (Appendix Three). The Google search engine has worldwide exposure and use and in the future, it is possible that clients will have googlehealth accounts to which health care professionals register to gain access and information. This control of health information by a private company (ehealth to ghealth) has the potential to change the face of healthcare in the future. The question that needs to be asked is can the health service offer a better service and solution before ghealth takes hold.

**Information Databases**

A great deal of data is generated but not converted into user information and knowledge. The use of large databases of information offer unique opportunities for quality assurance purposes, audit and risk analysis and performance management and measurement.
Opportunities to use non identifiable aggregate data for population health planning and disease mapping are essential in maximising the global health of the world. The availability of data for these purposes must be strictly controlled in relation to data protection to ensure individuals can not be identified or access to privileged information is divulged. (Appendix Four)

Positive examples of information databases and their application is the statistical data available through the Central Statistics Office (Appendix Five), offering statistics from information databases from numerous sources, such as:

- Census Survey  
  CSO
- Old Age Pensioners  
  Dept of Social and Family Affairs
- Social Welfare Payment/Expenditure  
  Dept of Social and Family Affairs
- No of Psychiatric Pts In Hospitals/Units  
  DOHC
- GMS Report General Medical Service  
  GMS

The All Ireland Health Directory or Ireland and Northern Irelands Population Health Observatory (INsPHO) offer further opportunities for data sharing, research purposes and health planning, examples are outlined as follows:

- Hospital In Patient Enquiry Scheme  
  HIPE
- Irish Cardiac Surgery Register  
  ICSR
- National Perinatal Reporting System  
  NPRS
- Public Health Information System  
  PHIS
- National Cancer Registry Data  
  NCRD

“Relevant, accurate, valid, comprehensive, and timely information, used intelligently, is a cornerstone in driving continuous improvement in our health and social care services, improving the public’s health, and reducing health inequalities” according to INsPHO. Issues to consider are the data standards and data sets from where information is gathered. Data manipulation can occur to present data in one format and be acceptable but if used for another purpose is not acceptable. The unique identifier is a crucial element in database development to ensure there are no duplications and to allow for cross referencing. The personal public service number (PPS) number has been identified as a unique identifier for health in the Health Information Strategy (DOHC 2004) but requires considerable investigation before this is developed.

**Telehealth**

Telehealth is not a new concept but is not widely adopted in the health service. Video conferencing offers many unique opportunities to offer care in remote locations. It raises issues of confidentiality and consent for patients using the service. The following criteria are suggested:

- Informed and recorded consent of the patient has to be obtained before any video consultation or video-conferencing is undertaken.
- The informed consent of the patient must be obtained before any consultation is recorded. This includes informing the patient of the proposed uses of the recording.
- Clinical guidelines have to specify who is permitted in each room during a video conference.
Health Information Bill- Nursing and Midwifery Perspective

- Patients must know exactly who is sitting in on the session and are to be introduced to all people present. The patient should be advised that the consultation may be terminated at any time.
- Clinician’s notes must acknowledge that the consultation was conducted using video conferencing technology and note any disruptions which occur in the course of the consultation.
- Video equipment and telecommunications lines used for telehealth must be protected by appropriate security measures.

Framework for Information Governance

The culture to respect the privacy of personal health information is paramount. Information governance led by Legislation, European Standards, Professional Codes and Standards, Acts and Laws are crucial. Principles set down in the National Health Information Strategy 2004 DOHC are to:

- Safeguard the privacy and confidentiality of personal health information
- Ensure that health information systems are efficient and effective
- Promote the optimal use of health information
- Ensure the high quality of health information.

Balancing the individual’s rights over societal needs is the crux of health information governance. A significant number of issues will arise in developing an information governance framework which will protect the patient sufficiently and will facilitate societal learning and population trend analysis in health.

A health informatics review in the UK, undertaken by the Department of Health (DOH 2008) examines the role of informatics in health care with a focus on data management, sharing and data governance issues. It highlights the core objective of the NHS Core Record Service (the EHR for the NHS) –“To provide for each person a comprehensive electronic record for their health and care” This is a mammoth task and one not to be underestimated. The EHR needs to be different things for different people and service needs change throughout the care cycle.

Information systems in Ireland must be capable of managing a typical day in the HSE as recorded by Health Matters (2008).

**A Day in the Life**

On a typical day in the HSE in 2007 there were:

- 11,909 inpatient episodes;  
- 1,670 day case patients receiving treatment;  
- 8,280 people attending outpatient departments;  
- 479 emergency calls to the ambulance service;  
- 3,140 people attending emergency departments;  
- 192 babies born;  
- 99,846 home help hours delivered;  
- 22,278 callers to the GP out of hours service;  
- 140 food inspections carried out;  
- 2,090 people in sheltered work;  
- 5,322 children in care;  
- 2,840 people in rehabilitation training; and  
- 193 callers to the HSE Information Line – 1850 24 1850

Health Matters Summer Edition 2008

Nursing and Midwifery Planning and Development Unit, Ballyshannon
Accordingly, the health information systems must be capable of managing similar transactions as listed by DOH (2008)

**Listing of current status of NPfIT June 2008**

<table>
<thead>
<tr>
<th>Activity</th>
<th>Progress made</th>
</tr>
</thead>
<tbody>
<tr>
<td>Providing IT infrastructure and broadband for the NHS</td>
<td>32,000 connections</td>
</tr>
<tr>
<td>A central email and directory service for the NHS</td>
<td>340,000 users</td>
</tr>
<tr>
<td>An individual electronic NHS Care Record for every patient in England</td>
<td>486,000 users registered for access to the Spine</td>
</tr>
<tr>
<td>Electronic booking service offering patients greater choice of hospital or clinic</td>
<td>8,552,000 bookings</td>
</tr>
<tr>
<td>To make prescribing and dispensing safer, easier and more convenient for patients</td>
<td>89,834,000 prescriptions</td>
</tr>
<tr>
<td>Capture, store, display and distribute static and moving digital medical images</td>
<td>640,764,000 images stored</td>
</tr>
<tr>
<td>To support commissioning through Payment by Results in the Sernitary Users Service</td>
<td>1,000,019,000 records created</td>
</tr>
</tbody>
</table>

Image taken from Health Informatics Review DOH (2008)

The Health Information Strategy, DOHC (2004) highlights the need for a cultural change regarding the use of health information and supports the need for a clear and supportive legislative and information governance framework to safeguard privacy and confidentiality of health service users.

**Crucial aspects of an Information Governance Framework**

- Personal Health Information- What information is contained within this, what can be shared and to whom and for what purpose.
- Confidential information-Specific to children, mental health, paternity/maternity issues need full consideration
- EPR Development –national, regional and local and under what standards and protocols
- UHI- What number is chosen, how is it generated and how maintains the accuracy of same.
- Patient Choice, consent and control- Patient role in their own information
- Systems and access-Who has access, for what and where is the information going.
- Information generation, storage, editing, collation and deletion-Who can do this and rules relating to this
Reports relevant for nurses and midwives in relation to health information

- Academy of Medical Sciences (2006) Personal Data for Public Good: Using Health Information in Medical Research
- An Bord Altranais 2000 - Code of Professional Conduct for each Nurse and Midwife
- Data Protection Act 1998/2003
- Department of Health 2008 Health Informatics Review Report NHS (DOH)
- Department of Health and Children 2003 Research Strategy for Nursing And Midwifery in Ireland
- Department of Health and Children 2004 - National Health Information Strategy
- Department of Health and Children 2008 Discussion Paper on the Proposed Health Information Bill
- Department of Health and Children 2008 Audit of Key International Instruments, National Law and Guidelines Relating to Health Information for Ireland and Selected Other Countries.
- Freedom of Information Act 2007
- Government of Ireland 2003 Data Protection Acts 1998 and 2003 and
- HEBE 2003 Embedding the E in Health –An ICT Strategy for Health
- HSE Health Forum 2008 -Towards an Integrated Health Service or More Of The Same?
- NCNM 2003 - Agenda for the Future Professional Development of Nursing and Midwifery
- NCNM 2005 Nursing and Midwifery Research Priorities in Ireland
- NCNM 2007 - Guidance To Nurses and Midwives Regarding Ethical Conduct of Nursing and Midwifery Research
- NWHB (2005) ICON Information Sharing NWHB Framework
- Minister of State, UK 2008 Data Sharing Review Report
- University College London 2008 Summary Care Record Early Adopter Programme -Connecting For Health
Appendix One

A SWOT Analysis is offered on identified technologies in relation to patient care and safety to outline the strengths and weaknesses of each.

**Electronic Patient Record**
An electronic repository of information accessible by multiple users in a standardised format for the purpose of information sharing when it is needed, by whom it is needed.

<table>
<thead>
<tr>
<th>Strengths</th>
<th>Weaknesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Info at the point of care</td>
<td>• Must be of a standardised format for electronic modes</td>
</tr>
<tr>
<td>• Health care professionals have vision on whole care journey</td>
<td>• Security Access Issues- Who is allowed access</td>
</tr>
<tr>
<td>• Holistic care</td>
<td>• Confidentiality can be impaired when scope of access is not well defined</td>
</tr>
<tr>
<td>• Prevents Duplicity of Information seeking and test ordering and undertaking</td>
<td>• Consent issues</td>
</tr>
<tr>
<td>• Drug treatment and medical errors associated with patient identifier issues</td>
<td>• Ability to read, write, edit, remove data by and or for patients</td>
</tr>
<tr>
<td>• Patient has central area with all information accessible (Continuity)</td>
<td>• Accessibility can be restricted in order to comply with privacy rights</td>
</tr>
<tr>
<td></td>
<td>• Stigmatising Illness -information sharing worries for patients.</td>
</tr>
</tbody>
</table>

**Opportunities**

<table>
<thead>
<tr>
<th>Opportunities</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Opens Integration of Care opportunities</td>
</tr>
<tr>
<td>• Mapping of Care Journey across sectors</td>
</tr>
<tr>
<td>• Analysis of Data from a holistic perspective</td>
</tr>
<tr>
<td>• Population Mapping</td>
</tr>
<tr>
<td>• Safety and risk measures can be implemented</td>
</tr>
</tbody>
</table>

**Unique Health Identifier**
A specific number which each person obtains and maintains through their life time which is used across all health care encounters. (PPS Number is a public service unique identifier)

<table>
<thead>
<tr>
<th>Strengths</th>
<th>Weaknesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Each and every person is registered and accounted for</td>
<td>• How is the number generated and by whom?</td>
</tr>
<tr>
<td>• No duplication of records</td>
<td>• Who oversees the generation and maintenance of numbers?</td>
</tr>
<tr>
<td>• Comparability across information requirements-core information the same</td>
<td>• Is the UHI separate to all other numbers such as PPS etc?</td>
</tr>
<tr>
<td>• Linkage of facts to each individual through the UHI</td>
<td>• If PPS number is used what rules govern it’s every day use and sharing</td>
</tr>
<tr>
<td>• Supports care pathway across different health agencies</td>
<td></td>
</tr>
</tbody>
</table>

**Opportunities**

<table>
<thead>
<tr>
<th>Opportunities</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Integration across all episodes of life Healthcare and external-bank, social welfare, passport, work personnel number, id card, garda etc</td>
</tr>
<tr>
<td>• Mapping of Care Journey across sectors- Public and private care working off same identifier allowing information exchange</td>
</tr>
<tr>
<td>• Population Mapping</td>
</tr>
</tbody>
</table>

**Threats**

<table>
<thead>
<tr>
<th>Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Invasion of Privacy</td>
</tr>
<tr>
<td>• Ownership of data an issue</td>
</tr>
<tr>
<td>• Data risk of unlicensed usage</td>
</tr>
<tr>
<td>• Parameters of data exchange -boundaries can get changed</td>
</tr>
<tr>
<td>• Inaccuracies or errors recorded can lead to far reaching consequences</td>
</tr>
<tr>
<td>• Data Ownership</td>
</tr>
<tr>
<td>• Data usage beyond individual control</td>
</tr>
<tr>
<td>• Parameters of data exchange</td>
</tr>
<tr>
<td>• Identify Theft</td>
</tr>
<tr>
<td>• “Big Brother” Concept</td>
</tr>
</tbody>
</table>
### Population Registers and Information Databases

List of persons on a database which identify individuals with a specific condition or disease which can be used for planning purposes such as to plan service provision by population mapping and incidence recording.

<table>
<thead>
<tr>
<th>Strengths</th>
<th>Weaknesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Removes duplicate incidences</td>
<td>• Risk of individual identification with population registers</td>
</tr>
<tr>
<td>• Stops speculation and gives hard evidence</td>
<td>• Determinants for how patients go on a list or come off the list.</td>
</tr>
<tr>
<td>• Supports service planning</td>
<td>• Patient consent to be on list-Mandatory or choice</td>
</tr>
<tr>
<td>• Supports life elongevity through prevention of disease</td>
<td>• Standard across the world or not effective electronically</td>
</tr>
<tr>
<td>• Promotes health through specific health targeting of affected individuals</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Opportunities</th>
<th>Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>• National Screening could begin</td>
<td>• Invasion of Privacy</td>
</tr>
<tr>
<td>• Incidence mapping identifying pockets with possible causes/effects linkages</td>
<td>• Risk of being “boxed” targeted as a person with specific diseases</td>
</tr>
<tr>
<td>• Service provision based on sound projections and occurrences</td>
<td>• Classification may stick with person for life</td>
</tr>
<tr>
<td>• Workforce planning projections possible</td>
<td>• Risk of electronic error</td>
</tr>
<tr>
<td>• Patterns of disease pre mapped, health promotion and prevention</td>
<td></td>
</tr>
<tr>
<td>• Immunisation and Vaccine registers worldwide to eradicate certain diseases</td>
<td></td>
</tr>
</tbody>
</table>

### Use of Information Databases for Research and Education

Provision of information for the purposes of research offering opportunities to map diseases and illnesses and identify cause and effects of occurrences. Education via datasets into disease onset and prevalence is highly beneficial.

<table>
<thead>
<tr>
<th>Strengths</th>
<th>Weaknesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Removes duplicate incidences</td>
<td>• Risk of individual identification with small populations</td>
</tr>
<tr>
<td>• Evidence based on facts provided through population registers and summary data</td>
<td>• Consent issues - Legitimate subject</td>
</tr>
<tr>
<td>• Supports learning from datasets</td>
<td>• Manipulation of data for specific purposes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Opportunities</th>
<th>Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>• National Screening</td>
<td>• Invasion of Privacy</td>
</tr>
<tr>
<td>• Incidence mapping</td>
<td>• Consent issues</td>
</tr>
<tr>
<td>• Population and disease planning</td>
<td>• Information misuse</td>
</tr>
</tbody>
</table>
Appendix Two

Patient Empowerment in Health Record Management

This scenario of client managed health care illustrates a simplex version of health care similar in plan to current practices in financial management undertaken and managed by clients every day.

<table>
<thead>
<tr>
<th>Managing Money</th>
<th>Managing Health –Empowering Health</th>
</tr>
</thead>
<tbody>
<tr>
<td>Book Appointment with Bank Manager/ Accountant</td>
<td>Book appointment with GP or Consultant</td>
</tr>
<tr>
<td>Plan Course of Action with advice- Lodge money/take out loan/invest money</td>
<td>Plan Course of Action with advise-dietary change/medication treatment/ exercise regime/surgical intervention/or further expertise sought.</td>
</tr>
<tr>
<td>Bank Card with details of bank accounts and Access Information</td>
<td>Health Card with health accounts and access to Information from these encounters</td>
</tr>
<tr>
<td>Decide to withdraw cash –Go to Bank or ATM</td>
<td>Book GP appointment and receive change in medication (Documentation of visit entered online by GP to health account of patient)</td>
</tr>
<tr>
<td>Decide to transfer monies between accounts – Online Access and move monies over the Internet</td>
<td>Patient books surgical review on advice of GP. Review takes place organised by patient. Documentation written up by surgical consultant after visit on patient health account.</td>
</tr>
<tr>
<td>Bank Statement and online account access</td>
<td>Patient has online access to health statements, accessed through card or PIN and password or health ATM machines in public spaces and health care settings.</td>
</tr>
<tr>
<td>Take cashback at local shop using chip and pin to access bank account</td>
<td>Collect medication from Pharmacy- Prescription listing in online health account, access using PIN</td>
</tr>
<tr>
<td>When dealing with bank officials or financial advisors, the client decides which accounts to make visible and share with financial consultants in order to progress financial affairs</td>
<td>When dealing with health care professionals, doctors or GP’s, the client decides what information from which transactions of care or all, to share with relevant consultant or HCP</td>
</tr>
</tbody>
</table>
Appendix Three

Extract from CSO – Example of Positive use of Information Databases
Appendix Four

Extract from CSO – Example of Positive use of Information Databases
Appendix Five


This outlines a future view of the electronic information management and the requirements within the NHS to move to a single health electronic information point.

Health Informatics Review Report NHS (DOH 2008)