International Niemann-Pick Disease Registry: Security and Context

Prof. Richard Sinnott
12th January 2014

1. Overview

This document provides an overview of the information governance and security issues surrounding the implementation of the International Niemann-Pick Disease Registry (INPDR – www.inpdr.org) systems. These systems includes the core phenotypic databases for Niemann-Pick types A and B (NP-AB) and for Niemann-Pick type C (NPC) together with the access to and usage of patient-specific information that they contain. This document also outlines processes and models that will be used for (future) biosample management and clinical trials and studies associated with INPDR. These models have been tried and tested in an extensive range of security-oriented health/biomedical projects involving Prof. Sinnott in his roles as Technical Director of the National e-Science Centre at the University of Glasgow (www.nesc.ac.uk) and as the Director of eResearch at the University of Melbourne (www.unimelb.edu.au). Examples of these include ENS@T-CANCER (www.ensat-cancer.eu), EuroWABB (www.euro-wabb.org) and the International Disorders of Sex Development (I-DSD registry - www.i-dsd.org). This is a working document and will be updated over time as the INPDR systems and the studies that they support evolve together with any requested changes to data security policies, patient management and/or collaboration arrangements that may come into place.

2. INPDR Information Governance Context

Throughout the European Union and indeed globally, numerous institutions are involved in clinical service delivery, and hold local registers of clinical cases and associated biological data sets. The EU Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 (along with numerous national initiatives such as the UK Data Protection Act 1998) focuses on the protection of individuals with regard to the processing of personal data and on the movement of such data. These efforts provide an overarching framework for how the collection and sharing of such information between member states for research purposes can be achieved in an individual, privacy-protecting manner. Many countries support further refinements to personal privacy and data usage especially in a clinical context. For example, Section 33 of the UK Data Protection Act 1998 and the Data Protection (Processing of Sensitive Personal Data) Order 2000 allows research to be conducted on non-identifiable data – this needs to be recognized explicitly when dealing with data that is unique and identifying by its very nature, e.g. DNA and especially the more recent advances made possible through whole genome sequencing approaches.

Many of these directives and acts, including the UK Freedom of Information Act 2000 make it clear that subjects that are included on any clinical research systems have a right to know of their inclusion on those systems and a right to access the data. In addition, they have a right to have their data removed from those systems at any time and without question or impacts upon the existing standard of care that they might be receiving. The practice of informing subjects of inclusion on clinical systems varies across the EU. In the UK, a system of opt-out consent is often used. In other countries opt-in models of consent are in place. Contributing sites for INPDR need to ensure that they adhere to nationally defined data sharing policies. Where necessary, applications will be made to relevant authorities, e.g. in the UK to PIAG, and the NHS Security and Confidentiality Advisory Group to enable appropriate access to confidential datasets. Other countries have their own ethics committees that they will apply to so as to ensure that data entry is driven by patient consent and supports ethically focused information governance.

To aid this process, software systems that allow for such exchange of information need to be designed to enforce such checks by contributors. In many cases (including INPDR), the first part of adding a case (patient-specific information) to the registry will be to advise the clinical contributor that they must have written consent to do so, and the final part of completing the addition of a case to the registry confirming that this is in accordance with local and national ethical arrangements regarding data sharing. The onus is very much on the clinician (or their support staff) to ensure that entry of biomedical information/data is strictly aligned with local and national policies on biomedical data sharing.

To comply with the directive 02/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), the INPDR project adheres to the highest standards of data security in the development of the registry. Under the directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, users of the INPDR registry will be allocated specific privileges (roles) depending on their role within the project. These roles are used to restrict access to data and tools that are available. The default model that has been implemented (and always needs to be implemented!) is to deny access to requests that are not fully approved, i.e. only individuals with authentic and valid credentials given as digitally signed credentials recognized by the INPDR system, are able to access and use the registry.

It is important to note that the INPDR system (or more precisely that data model that is realized by the INPDR system) has been designed explicitly so that it does not hold the names or addresses of any patients or any direct information, which can be used to identify an individual patient. Instead cases are identified for the purposes of communication with an automatically generated identifier that is generated by the system and is guaranteed to be unique within the registry as outlined below. Whilst data collected by the participating clinical centres must be shared under the above legal frameworks to select cases and case materials for research by INPDR participants, any research that is carried out on these data or resources is subject to the Declaration of Helsinki, 1964 and the Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine Oviedo, 4.4.1997 and Strasbourg 25.1.2005. As such, it needs to be approved by the ethics committees of the clinical centre that contributes the case and the centres where the case / data is to be researched. As access to the INPDR systems often depends on the nature of the study being performed by a researcher/investigator, the latter will submit a case or requirements including ethics approval status to an INPDR steering committee to determine whether access should be allowed or not. By default all INPDR partners involved in the original INPDR grant are given access to include their own cases (subject to local/national ethics arrangements). A clearly identified process is in place for allocating access to the INPDR systems for new member organisations. This includes the processes for application, review and acceptance (or rejection) of access to the INPDR registry.

In developing IT systems for previous clinical research studies, the consortium partners have had to address a number of important security and data privacy considerations. The project partners have direct experience in working to UK and international standards (including ISO 17799, and US 21 CFR part 11), and have extensive experience of using healthcare data in the context of privacy and data protection legislature (including the Data Protection Act 1998, EU Data Protection Directive 95/46/EC, and the US Health Insurance Portability and Accountability Act [HIPAA] 1996). Such experience is directly shaping the IT security of numerous on-going clinical projects with advanced security at their heart, and we leverage this expertise directly. This includes major on-going European projects in the area of disorders of sex development, rare disease registries and clinical trials in the brain trauma domain amongst numerous others.

It should be emphasised that no data concerning sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction is collected in the INPDR systems and only those data sets directly relevant to research into Niemann-Pick Disease are incorporated. Information regarding past history, presentation, biological parameters, imaging tests and interventions are provided with a unique and non-patient identifying identification number of the biological material. The data sets associated locally with the collection of biological material also include the identification of the depositor and the identification number of the donor, but this information is not to users outside of the given clinical healthcare context. Given the diversity of regulations concerning data protection within the EU as outlined previously, advice

has been taken from numerous places including the Comité National Informatique et Libertés (France), Garante per la Protezione dei Dati Personali (Italy), der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (Germany), and in the UK with the Information Commissioner's Office, to obtain permission to populate and subsequently use the INPDR systems for research purposes.

The physical computer resources that are currently used for the INPDR systems development and support are located at the University of Melbourne, Australia under the direct responsibility of the Director of eResearch, Prof. Richard Sinnott. In addition to the aforementioned ethical and policy frameworks, it should be noted that globally a range of other policies and statutes exist. Given the physical location of the INPDR systems at the University of Melbourne key policies and laws on management and processing of clinical/biomedical data across Australasia also exist. Most pertinent to the INPDR systems are:

- Copyright Act 1968 (Commonwealth) - http://www.comlaw.gov.au/Details/C2012C00482
- Privacy Act 1988 (Commonwealth) - http://www.comlaw.gov.au/Details/C2012C00414
- Electronic Transactions Act 1999 (Commonwealth) - http://www.comlaw.gov.au/Details/C2011C00445
- Australian Code for the Responsible Conduct of Research 2007 (Commonwealth), pp2.1-2.3 - http://www.nhmrc.gov.au/_files_nhmrc/publications/attachments/r39.pdf
- National Statement on Ethical Conduct in Human Research - http://www.nhmrc.gov.au/guidelines/publications/e72
- Public Records Act 1973 (Victoria) - http://www.austlii.edu.au/au/legis/vic/consol_act/pra1973153/
- Information Privacy Act 2000 (Victoria) - http://www.austlii.edu.au/au/legis/vic/consol_act/epa1958361/
- Health Records Act 2001 (Victoria) - http://www.austlii.edu.au/au/legis/vic/consol_act/hra2001144/
- Evidence Act 1958 (Victoria) - http://www.austlii.edu.au/au/legis/vic/consol_act/epa1958361/ and from 01/01/2010 Evidence Act 2008 (Victoria) - http://www.austlii.edu.au/au/legis/vic/consol_act/ea200880/
- Whistleblowers Protection Act 2001 (Victoria) - http://www.austlii.edu.au/au/legis/vic/consol_act/wpa2001322/
- Statute 14.1 - Intellectual Property - http://www.unimelb.edu.au/Statutes/s141.html
- Regulation 17.1.R8 - University Code of Conduct for Research - http://www.unimelb.edu.au/Statutes/r171r8.html

As a general principle, the University of Melbourne is obligated to ensure that research data and records created as part of its research efforts (including data from projects like INPDR) are accurate, complete, authentic and reliable; identifiable, retrievable and available when needed; secure, and compliant with legal obligations and the rules of funding bodies. Research data needs to be retained for a minimum of five years after publication or public release of the work of research. Researchers themselves are obliged to develop appropriate processes for the collection, storage, use, re-use, access and retention of research data and records associated with their research program, including confidential research data and records; to incorporate this information into their research data management plan and to register this information in a local department register. More details on the process by which these legal obligations are adhered to, is described in Annex A.

3. INPDR Security Mechanisms

3.1 Security through Obfuscation of Patient Identity

Given the above, a range of technical solutions and processes has been put into place to ensure adherence to the above policies and legislation. Firstly to ensure that no identifiable information is recorded on the systems a unique and independent identifier is generated through the INPDR systems. This identifier is dissociated from any personal identifiers used for example within a given clinical setting, e.g. hospital numbers or names and date of birth etc. The coding of this identifier includes the country, partner and a generated patient number only, e.g. NOOS-5 for the 5th patient from the Oslo Centre (OS) Norway (NO). Local centres, e.g. Oslo will keep a local track of this record on their own patient management systems and how it relates to an individual patient record in the INPDR systems. At no time will they ever be asked to reveal the identity of individual NOOS-5 to any INPDR researcher or other researcher outside of their

immediate clinical care setting. It is noted that the only real identifier that is associated with a given patient record on the INPDR systems is the email address of the clinician responsible for including the patient onto the system. Here responsible implies that they are the ultimate source of authority to ensure that consent has been obtained from the patient and/or patient family. It is only through the clinician that further information on the patient can be obtained. This can be follow-up information not documented on the INPDR systems and/or the availability and access to/usage of particular biomaterials associated with this patient.

Furthermore registering a patient on the INPDR systems does NOT automatically imply that all biomaterials will be made available at all times, nor does it imply that further information on the patient will be made available. This is entirely discretionary to the clinician involved and is coupled with the level of consent in data sharing agreed to by the patient/their family and their contact clinician.

The linkage between the patient identifiers in the INPDR registries and the identifiers used for biomaterials has been designed to be both distinct and completely separated, i.e. it will never be possible to directly identify (through a given software query or direct observation of a particular software system) that a particular sample comes from a particular patient through use of the registry or other related IT system. To address this, the INPDR systems leverage work from the ENS@T-CANCER project (amongst others) whereby unique identifiers for actual physical biomaterials/genetic samples from individuals are generated by the systems and subsequently used for local storage/identification and data tracking purposes at INPDR related clinical studies. These identifiers include the study information, e.g. NPC-StudyX, the country, center and a unique patient number as well as the biosample type and date. Thus NOOS-5, NPC-StudyX, 20-01-2014, Plasma Sample, indicates a plasma sample for a patient from the Oslo Centre in Norway dated 20th January 2014.

This (aggregated) identifier is used directly on the registry for direct tracking and location of biosamples. However, in some countries it is often the case that further separation of identifiers used on biosamples to identifiers used for collaboration is made. In this case, a unique local identifier needs to be generated (e.g. XYZ123) to associate the biosample identifier with the patient identifier used on the registry (e.g. NOOS-5). Thus a user of the registry would see a patient NOOS-5 with biosamples XYZ123. Only the Norwegian center would be able to establish which particular biosample this refers to through local translation of XYZ123 to the local identifiers used. The VANGUARD system (Sinnott 2009, Stell 2009) has been developed to supports such levels of indirection between identifiers used and their linkages and will be exploited by INPDR where required.

Data existing within the INPDR registry can be edited or deleted by the owner of this data. This may be the person who uploaded the data but can also be a local researcher working on behalf of an INPDR investigator for example. A patient can instigate this deletion if they so wish. Data deletion results in removal of the data from the backend database and any local replicas of this data. We emphasise that the INPDR data model has been specifically defined to not include any identifying information on patients.

All collaborators are fully expected to have signed up to the terms and conditions and standard operating procedures associated with being involved in the project, e.g. regarding obtaining patient consent or guardian assent (as deemed appropriate).

3.2 Technological Aspects of Security in INPDR

Within any clinical/biomedical collaboration system, the technical implementation aspects of security are an essential factor to incorporate. Within INPDR a range of technologies are used to support the development and the associated security mechanisms. The INPDR systems have been developed using Java Server Pages (JSP) server-side scripting hosted in an Apache Tomcat container, running on a virtualized and secure (see below) set of hosts. This system provides secure access to a MySQL database holding the primary datasets for the core components of the INPDR systems. Interfaces to other external clinical trial systems can/will be implemented in due course (once defined by the clinical/biomedical collaborators) – leveraging the body of expertise in development and support of electronic case report forms (eCRFs) and trial-specific study databases (Sinnott 2009, Stell 2009).

Security is a multi-faceted challenge that is more than just the security of the software systems developed through INPDR, but also must accommodate the security of the underlying infrastructure upon which the software systems are deployed and ultimately managed. The INPDR systems have been implemented with these holistic security considerations in mind. Firstly, the security of the applications and their hosted environments needs to be addressed. In this regard, administrative security is implemented on the virtual machines that host the applications. These virtual machines are located in a secure server room where access is physically restricted to a known (small) set of named system administrators employed through the University of Melbourne. These server rooms have swipe card access and are inaccessible to all non-authorized individuals. Access to the INPDR virtual machines is also restricted through software systems and processes to those directly involved in the project. Specifically the servers are locked down through Secure Shell (SSH) logins where access by privileged users is restricted to those with the appropriate public/private key-pairs. The firewalls of these machines are specifically configured in a "default-deny" manner and all non-essential services are turned off, e.g. ftp and telnet. These settings are managed and controlled by the INPDR software developers working for and reporting directly to Prof. Sinnott. All staff members have worked alongside Prof. Sinnott for many years in many security sensitive projects including a range of clinical trials and epidemiological studies in the UK and Australia.

The security of the INPDR applications themselves are protected using advanced web application security methods including "gated" session-based tracking, making use of the Java Server Pages (JSP) notion of session rather than interacting with clients using a given web security context. The header of each INPDR portal web page has a timeout countdown, which logs the user out if the page has been inactive for an extended time period, e.g. 15 minutes. Restrictions are also placed on the application input, for example to ensure that numeric parameters input are indeed numeric, and dropping information that is considered dangerous. This helps to minimize the risks of SQL keywords and/or potential byte-code characters that are unexpected in context (and thereby minimize SQL-injection attacks). The SQL and all inputs use parameterization of predefined query templates, i.e. it is not possible to randomly query the INPDR databases, but only through the vocabulary and query terms given in the INPDR user interface. In each of these situations the system is designed to fail in a manner that is as secure as possible (with "default-deny" logic implemented) rather than in a way that could potentially leave back-end information systems exposed.

As required by the INPDR researchers and their associated ethics bodies, a rich variety of levels of data access and authorization are supported. Contributors are able to add data into the system at three primary levels of data sharing:

- Local centre access only, e.g. only those from a specifically named centre can access the data;
- National level access only, e.g. data is only accessible for researchers from France (assuming the data is from a French contributing centre);
- INPDR partner access, i.e. for those partners involved in the INPDR project (this includes both original members, that is those listed in the original grant, and members who have subsequently joined the project).

The implementation of these types of data access policy are defined both in the user interface (when adding a patient record) and they are subsequently enforced in the associated logic of the security modules in the underlying system implementation. The result of a request for data access can result in one of three outcomes: access is denied, read-only access given, or read/write access is given. The granularity of access level also allows to delineate privileges assigned to certain roles and how these interact, e.g. specific forms in the INPDR systems, e.g. "Laboratory Results" may only be available to users that possess the appropriate participation role (i.e. from the laboratory that has processed the data from the associated patient).

For auditing purposes Google Analytics and Statcounter are used to trace IP addresses, pages visited and the associated profile of utilisation. Regular expression matching in the virtual machine logfiles is supported. For the purposes of more in-depth auditing the software module log4j is used to track every action of every user: all pages accessed and all method calls. The significance of being able to track data provenance is especially important when conducting retrospective monitoring of trials and is something that is supported methodologically. These textual logs are stored into a database that can be more logically searched using more advanced features than string expression matching. (This work is also the focus of a

PhD studentship funded through an INPDR collaboration between the University of Birmingham, UK and the University of Melbourne, as part of a Universitas 21 initiative).

Related to security is the continuity management of the system data in case the systems should ever be compromised or suffer downtime (e.g. power outages). To tackle this, data is periodically stored by running *mysqldump* through a nightly *cron* job. The output file will be copied to a separate machine as part of that *cron* job, and every month a copy encrypted using TrueCrypt will be created and sent to an offsite location (University Hospital Birmingham, UK). Scripts to manage backups and file exports are also run and used to maintain adequate volume space on limited resources.

References

Sinnott R.O., Ajayi O., Stell, A.J., Data Privacy by Design: Digital Infrastructures for Clinical Collaborations. International Conference on Security and Privacy, Orlando, USA, 2009

Stell A.J., Sinnott R.O., Ajayi O., Jiang J., Designing Privacy for a Scalable Electronic Healthcare Linkage System. IEEE International Conference on Information Privacy, Security, Risk and Trust (PASSAT 2009), Vancouver, Canada, 2009.

Stell, A.J., Sinnott, R.O., Jiang, J., Enabling Secure, Distributed Collaborations for Adrenal Tumor Research, HealthGrid conference, Paris, France, June 2010.

Sinnott, R.O., Stell, A.J., Towards a Virtual Research Environment for International Adrenal Cancer Research, Workshop on Biomedical and Bioinformatics Challenges to Computer Science, International Conference on Computational Science, Tsukuba, Japan, June 2011.

Stell, A.J., Sinnott, R.O., The ENSAT Registry: A Digital Repository Supporting Adrenal Cancer Research, Health Informatics Conference (HIC), Sydney, Australia, July 2012.

Annex A: INPDR Confidentiality Policy

A.1. Introduction

1. The Melbourne eResearch Group (MEG) at the University of Melbourne places the highest priority on maintaining the confidentiality of the information that it holds. It is essential that patient identifiable information is handled, processed and released in a strictly controlled manner. This document sets out the University of Melbourne policy for the management of confidential information in general terms and with particular focus on the INPDR project.
2. First and foremost it is emphasised that the INPDR project will not collect patient identifiable information in the central databases and associated Virtual Research Environment (VRE). Nevertheless policies and procedures are essential to define and abide by since the data sets have strict information governance requirements that must be upheld.
3. Overall responsibility for information security rests with the University of Melbourne, Director of eResearch [Prof Richard Sinnott]. All staff are required to be familiar with the contents of this policy and to strictly adhere to it.
4. Any member of staff who at any time has difficulty in understanding the rules or thinks that they are insufficient or are being misapplied has a positive duty to do something about it. In case of doubt, the Director, eResearch or a member of the senior management team should be consulted at the earliest opportunity.
5. Failure to observe these rules may lead to appropriate disciplinary action being taken which, in serious cases, may lead to dismissal.
6. The policy is complimentary to other University of Melbourne policies and should be used in conjunction with them. These include policies and regulations regarding general computing and network facilities (http://www.unimelb.edu.au/ExecServ/Statutes/pdf/r83r2.pdf) at the University of Melbourne as well as associated guidelines related to these policies (http://www.unimelb.edu.au/infostrategy/policies/guidelines.html).
7. The policy shall be reviewed annually.

A.2. Confidentiality measures

1. All staff receiving and using personal information shall be bound by a legal duty of confidence.
2. MEG shall maintain the same standards of confidentiality as customarily apply to the doctor-patient relationship. This obligation extends indefinitely, even after the death of the patient.
3. All staff shall sign a “Confidentiality Undertaking Form” (see Appendix “B”) as part of their contract of employment.
4. The term "Confidential Information" shall apply to any information relating to identifiable individual patients, clinical staff or practitioners held in a document, on microfiche/microfilm or magnetic medium (disc or tape) or other machine readable electronic form.
5. MEG staff may come into contact with confidential information and/or handle a large amount of personal data on patients or clinical staff. All personal data shall be regarded as confidential.
6. If work is contracted to a 3rd party who in the course of their work requires access to confidential or patient identifiable data, the 3rd party will be required to sign the appropriate MEG Confidentiality Agreement for external contractors.

A.3. Compliance with legislative and contractual requirements

MEG has obligations to maintain confidentiality under the following legislation and guidance:
• Copyright Act 1968 (Commonwealth) - http://www.comlaw.gov.au/Details/C2012C00482
• Privacy Act 1988 (Commonwealth) - http://www.comlaw.gov.au/Details/C2012C00414
• Electronic Transactions Act 1999 (Commonwealth) - http://www.comlaw.gov.au/Details/C2011C00445
• Australian Code for the Responsible Conduct of Research 2007 (Commonwealth), pp2.1-2.3 - http://www.nhmrc.gov.au/_files_nhmrc/publications/attachments/r39.pdf
• National Statement on Ethical Conduct in Human Research - http://www.nhmrc.gov.au/guidelines/publications/e72
• Public Records Act 1973 (Victoria) - http://www.austlii.edu.au/au/legis/vic/consol_act/pra1973153/
• Information Privacy Act 2000 (Victoria) - http://www.austlii.edu.au/au/legis/vic/consol_act/epa1958361/
• Health Records Act 2001 (Victoria) -

http://www.austlii.edu.au/au/legis/vic/consol_act/hra2001144/
• Evidence Act 1958 (Victoria) - http://www.austlii.edu.au/au/legis/vic/consol_act/epa1958361/ and from 01/01/2010 Evidence Act 2008 (Victoria) - http://www.austlii.edu.au/au/legis/vic/consol_act/ea200880/
• Whistleblowers Protection Act 2001 (Victoria) - http://www.austlii.edu.au/au/legis/vic/consol_act/wpa2001322/
• Statute 14.1 - Intellectual Property - http://www.unimelb.edu.au/Statutes/s141.html
• Regulation 17.1.R8 - University Code of Conduct for Research - http://www.unimelb.edu.au/Statutes/r171r8.html

Before personal data are held on computer, it is necessary to notify the Office of the Information Commissioner. Copies of MEG registrations are checked regularly to ensure that all uses and especially disclosure of personal data are covered. MEG is covered under the registration for the employing authority, (University of Melbourne). The MEG Director takes overall responsibility for data protection within MEG.

Failure to register personal data or knowingly to use data other than as registered will constitute an offence under the Act, which may result in MEG and/or individual employees being prosecuted and fined. Also, it is essential that the registrations are kept up to date, and the MEG Director is responsible for informing the Data Controller regarding any new uses.

A.3.2. The Melbourne University Human Research Ethics Committee

At the University of Melbourne the Central Human Research Ethics Committee (HREC) has oversight of all matters pertaining to human research. Reporting to the HREC are three Human Ethics Sub-Committees (HESCs) – Health Sciences HESC, Behavioural & Social Sciences HESC, and Humanities & Applied Sciences HESC - which have responsibility for the review and approval of individual research projects. The membership of the HREC and each HESC is in accordance with the National Statement on Ethical Conduct in Human Research (NHMRC, 2007). Human Ethics Advisory Groups (HEAGs) are based in departments, schools or faculties, and provide reviews of all ethics applications and report to HESCs. HEAGs themselves are located in faculties, schools, centres and/or departments and comprise academic staff. They:

- conduct technical and ethical reviews of all projects emanating from a department/school/centre/faculty;
- provide feedback to researchers on their research;
- have delegated authority to approve Minimal Risk applications;
- provide advice to the HESCs.

Projects that present more than low risk must be reviewed by a properly constituted human research ethics committee. Following an initial assessment by the HEAG such projects are referred to one of the University's three discipline-based HESCs for review and approval. The basic principles for conduct of such research and the baseline for good practice:

- Justify the purpose for using confidential information;
- Only use it when absolutely necessary;
- Use the minimum that is required;
- Access should be on a strict need to know basis;
- Everyone must understand his or her responsibilities;
- Understand and comply with the law.

A.3.3. Information flows

There is an annual review of the justification of flows of any patient identifiable information.

A.4. Release of Data

A.4.1. Release of Identifiable Data

Individual records are identifiable if name, address, postcode or national medical numbers are present; any other information is present which, in conjunction with other data held by or disclosed to the recipient, could identify the patient.

A.4.1.1. Controlling the release of identifiable data

The control of the release of identifiable data depends on the circumstances.

- Data subjects (patients) are entitled, under certain conditions, to examine their own records under the provisions of the acts given in section A.3 above.
- Medical practitioners may be given access to data on patients for whom they are responsible.
- This would normally mean that they have diagnosed or treated the condition which has been registered.
- Designated individuals in organisations providing care for the patient at any point in the clinical journey.
- Designated individuals for the purposes of audit and monitoring.
- Regional Directors of Public Health, Strategic Health Authority Directors of Public Health for the purpose of investigating specific public health concerns about service quality.

All other requests for patient identifiable data including all new requests for identifiable data for research require either patient consent or exemption under the Health & Social Care Act (2001).

A.4.1.2. Release of 'potentially' patient identifiable data

Aggregate data may also be identifiable in practice if linked formally or informally with other information, for example in small communities. As a general rule, the following categories should be regarded as being potentially identifiable data:

- Individual records even if they do not include variables, such as names, full postcodes, and dates of birth which would make them obviously identifiable
- Tabular data, based on small geographic areas, with cell counts of fewer than five cases/events (or where counts of less than five can be inferred by simple arithmetic)
- Tabular data containing cells that have underlying population denominators of less than 1,000
- As a general rule, the following categories should be regarded as potentially identifiable data for small geographic areas:
- Those areas where the total denominator population is less than that of a hospital, e.g. wards or aggregations of wards.
- Any geographic area (e.g. local authority) which, when released, may provide information regarding small population non-contiguous areas (“slivers”) when combined with other information, e.g. hospital data. These should be regarded in the same way as ward level data.

A.4.2. Requests for identifiable data

All releases of data must be approved by the MEG Director and the INPDR management committee and shall be requested in writing. Releases of both identifiable and potentially identifiable data are governed by the following principles:

- the intended use(s) of the data should be stated clearly in writing
- the use(s) of the data should be justified and the data should not be used for any other purpose(s)
- the VRE should not release data that are more detailed than necessary to fulfil the stated purpose
- the data should not be passed on to other third parties or released into the public domain
- the data should be kept securely for the period of time that can be justified by the stated purpose, and then destroyed
- no attempt should be made to identify information pertaining to particular individuals or to contact individuals (unless patient consent has been obtained via the patient’s clinician)
- no attempt should be made to link the data to other data sets, unless agreed with the data providers
- any public domain reports or papers resulting from analyses of the provided data should be shared prior to publication with the VRE supplying the information.
- recipients of data should be aware of their responsibilities, and should sign an agreement to this effect prior to the release of data by the VRE.

Publication of data on a website and in unrestricted circulations of reports or documents containing data should be regarded as being in the public domain.

A.4.3. Conditions for the release of identifiable data for research

The release of identifiable data for research purposes shall normally be subject to the following conditions:

- The researcher shall have the consent of the individual patients or approval from a local/national

Patient Information Advisory Group (PIAG).

- Approval shall be obtained from the relevant local/national Multi-Centre Research Ethics Committee (MREC) or Local Research Ethics Committee (LREC).
- Copies of MREC, LREC or PIAG approval letters or equivalent bodies in local countries should be provided to MEG.
- Consent of the clinical practitioner responsible for the patient shall be obtained. Where consultant permission cannot be sought – e.g. consultant unknown – the GP's permission shall be sought.
- A registered medical practitioner or health professional shall take responsibility for the security and use of the data;

In addition the requester shall:

- Agree in writing to observe the same principles of confidentiality as a registered medical practitioner or health professional and shall take responsibility for the security and use of the data.
- Agree to use the data only for the purpose outlined in the request.
- Not contact the registered person except where written authorisation is received by the treating clinician and Ethics Committee approval has been given.
- Ensure that publication of results will not enable any individual to be identified.
- Return or appropriately destroy all data once no longer required.
- Give due acknowledgement to the VRE for provision of the data.

A.4.4. Release of aggregated data

Aggregated data is released to requestors provided that a written request is submitted and that there is no possibility of indirectly identifying an individual from the data due to small numbers.

A.5. Deletion of Data

A.5.1. Technical Aspects of Deletion

Upon request by a patient to have their data removed/deleted from the registry, the database and all local copies of the data will be permanently removed using appropriate secure deletion technologies. This process recognizes that simply removing a file from a database or file system does not permanently remove it and technologies exist to recover data. The MEG will periodically explore the technologies that they adopt for permanent file removal. Many of these are explored and benchmarked in [Priya, 2015].

A.4.6. Transmission of information

A.4.5.1. Use of telephone and fax

No individual identifiable data shall be issued over the telephone or via facsimile.

A.4.6.2. Post and courier services

All data issued (paper, disk or other electronic methods) shall have an accompanying letter sent, quoting the number of pages or records in the report or on the disk and must be clearly marked "Private & Confidential" and sent to a named person. Paper copies shall be enclosed and sealed in double envelopes, with the internal envelope marked confidential.

A.4.6.3. Electronic transmission

Confidential information shall be transmitted by a secure method. Confidential information shall be encrypted prior to transmission over the Internet. If the data are encrypted and password protected, a separate letter or email shall be sent asking the recipient to telephone the MEG for the password.

A.4.7. Recording of Patient Identifiable Information Requests

All completed patient identifiable information requests, e.g. concerning genetic counselling shall be held in a locked cabinet under the responsibility of the INPDR VRE Manager (Prof. Richard Sinnott). Similarly, all electronic copies of summary replies shall be stored on a secure folder accessible only to (Prof Richard Sinnott).

A.8. Responsibilities

Access to patient identifiable information held electronically or in paper format is controlled; staff and managers have appropriate designated levels of access to electronic information, and working practices

and physical security restrict access to paper records to a 'need to know basis'. There will be an annual update related to confidentiality given to all staff.

A.8.1. Management responsibilities

Managers shall ensure that:

1. staff are aware of this policy and understand their responsibilities under it;
2. staff are following the policy;
3. any adverse incidents are reported to the MEG Director or a member of the senior management team.

A.8.2. Staff responsibilities

Staff shall ensure that:

1. they make themselves aware of the policy and follow it.
2. they never examine or handle in any way personal data, except in the course of their work. If they are required to read personal data as part of their work, this data shall never be disclosed to any person not directly concerned with that work.
3. the data they are working on are not read or handled by anyone who has no reason to do so.
4. if they believe that someone is deliberately attempting to read or handle personal data not within their official duties, the facts must be reported immediately to their manager, or the MEG Director or a member of the senior management team.
5. if they are working with personal data and they have to leave the room they must either lock the data away or ask another member to be responsible for the data until they return.
6. if they are the only member left in charge of personal data and they have to leave, the data must be locked away, the room locked and the windows closed.
7. confidential information is never left unlocked in an unattended room; it must be kept in secure locked cupboards or cabinets or in a secure filing room when not in use, and must not be taken out of the MEG premises except for specified purposes authorised by the MEG Director.
8. if it is ever discovered or even suspected that confidential information has been lost, their manager must be informed immediately; he/she shall investigate and report to the MEG Director without delay.
9. keys to cupboards holding confidential information are locked away or kept on the person when not in use.
10. they always "log out" of their PCs when leaving the building or leaving the office empty, and 'lock' their PC screen when leaving their desk/ office.
11. visitors to the MEG are accompanied at all times.
12. person identifiable data is never left visible on an unattended terminal/PC screen.

A9. References

- Data Protection Act (1998)
- Caldicott Committee Report (1997)
- Health and Social Care Reform Act (2001)
- The Health Service (Control of Patient Information) Regulations 2002
- Health and Social Care Act 2001 (www.hmso.gov.uk/acts/acts2001/20010015.htm)
- Statutory Instrument 2002 No. 1438. The Health Service (Control of Patient Information)
- Regulations 2002 (www.legislation.hmso.gov.uk/si/si2002/20021438.htm)
- Guidance notes. Section 60 of the Health and Social Care Act 2001 (www.advisorybodies.doh.gov.uk/piag/s60guidancenotes.PDF)
- Use and disclosure of health data. Guidance on the application of the data protection act 1998.
- May 2002. Information Commissioner. (www.dataprotection.gov.uk)
- National Statement on Ethical Conduct in Human Research (2007), http://www.nhmrc.gov.au/
- Priya, B., (2015) *Secure deletion of data on the Cloud*, Masters Dissertation, University of Melbourne, November 2015.

Appendix B: MEG Confidentiality Agreement

Confidentiality Undertaking for MEG Staff

I, the undersigned, understand that, in the course of my work, I may come into contact with, or have access to, a wide range of confidential data relating to individual patients, various members of staff, confidential reports and other sensitive information. I understand that misuse of this information, especially its disclosure to people or agencies not authorised to receive it, would constitute a serious breach of confidentiality. Any breach of confidence will lead to disciplinary action, which may involve dismissal. I also understand that the use and security of personal information is subject to the provisions of the following acts and policies:

- Copyright Act 1968 (Commonwealth) - http://www.comlaw.gov.au/Details/C2012C00482
- Privacy Act 1988 (Commonwealth) - http://www.comlaw.gov.au/Details/C2012C00414
- Electronic Transactions Act 1999 (Commonwealth) - http://www.comlaw.gov.au/Details/C2011C00445
- Australian Code for the Responsible Conduct of Research 2007 (Commonwealth), pp2.1-2.3 -
- http://www.nhmrc.gov.au/_files_nhmrc/publications/attachments/r39.pdf
- National Statement on Ethical Conduct in Human Research - http://www.nhmrc.gov.au/guidelines/publications/e72
- Public Records Act 1973 (Victoria) - http://www.austlii.edu.au/au/legis/vic/consol_act/pra1973153/
- Information Privacy Act 2000 (Victoria) - http://www.austlii.edu.au/au/legis/vic/consol_act/epa1958361/
- Health Records Act 2001 (Victoria) - http://www.austlii.edu.au/au/legis/vic/consol_act/hra2001144/
- Evidence Act 1958 (Victoria) - http://www.austlii.edu.au/au/legis/vic/consol_act/epa1958361/ and from 01/01/2010 Evidence Act 2008 (Victoria) - http://www.austlii.edu.au/au/legis/vic/consol_act/ea200880/
- Whistleblowers Protection Act 2001 (Victoria) - http://www.austlii.edu.au/au/legis/vic/consol_act/wpa2001322/
- Statute 14.1 - Intellectual Property - http://www.unimelb.edu.au/Statutes/s141.html
- Regulation 17.1.R8 - University Code of Conduct for Research - http://www.unimelb.edu.au/Statutes/r171r8.html

I recognise that unauthorised disclosure of personal information is an offence under these Acts.

I confirm that I have been made aware of the of MEG Confidentiality policy which deals with the handling of confidential information in the MEG, and the Information Security Policy, which is concerned with rules and procedures governing access to cancer data, and that I have read and understood the requirements of the document.

Signed .....
Name .....
Date .....
Witnessed .....

PLEASE RETURN THIS DOCUMENT WHEN SIGNED TO THE INPDR MANAGER