

**The Register**

**and its**

**CODE OF PRACTICE**

**CONFIDENTIALITY, SECURITY**

**& DISCLOSURE OF PATIENT INFORMATION**

Mrs Rosie Thompson MSc  
Project Manager

Mr Tim Overton  
Clinical Lead  
Consultant in Fetal Medicine

South West Congenital Anomaly Register  
Institute of Child Health  
UBHT Education Centre  
Upper Maudlin Street  
BRISTOL BS2 8AE

Telephone: 0117 342 0195/0158

Fax: 0117 342 0178

Email: [rosie.thompson@ubht.swest.nhs.uk](mailto:rosie.thompson@ubht.swest.nhs.uk)

[tim.overton@ubht.swest.nhs.uk](mailto:tim.overton@ubht.swest.nhs.uk)

## *Contents*

### Acknowledgements

#### Part One The Register

1.	Background .....	4
2.	Aims & Objectives .....	5
3.	Sources of data .....	6
4.	Nature of data .....	8
5.	Information routes & pathways .....	10
6.	Method of notification .....	11
7.	Registration of notification .....	12
8.	Reporting from the register .....	12
9.	Operation of the register .....	13

#### Part Two Confidentiality, Ethics & Disclosure of Patient Information

1.	Introduction .....	16
2.	Basic Principles .....	16

#### Part Three IT Security Policy

1.	Overview .....	20
2.	Statement of Authority and Scope .....	21
3.	Statement of Responsibilities .....	21
4.	The Computing Environment .....	22
5.	Computer Access .....	23
6.	Physical Security .....	24
7.	General Computing .....	25
8.	Internet Access .....	26
9.	Intranet (Campus) Access .....	26
10.	Remote Access .....	27
11.	Email .....	27
12.	World Wide Web Server .....	28
13.	Departmental File Server/Store .....	28
14.	Backups .....	29
15.	Anti Virus Security .....	30
16.	Contingency Planning .....	30

## Appendices

Appendix 1	List of exclusions	Appendix 7	List of Steering Committee Members
Appendix 2	Good Practice Guidelines	Appendix 8	Terms of Reference for Steering Committee
Appendix 3	Declaration by Members of Register Staff	Appendix 9	Information Sheet
Appendix 4	Guidance for Staff Providing Data	Appendix 10	PIAG letter for Section 60 support
Appendix 5	Warning Card	Appendix 11	MREC Approval
Appendix 6	Data Form	Appendix 12	Paediatric Form
		Appendix 13	BINOCAR Application

### *Acknowledgements*

Thanks to Mrs Nicky Henderson RN for her work in creating our original Code of Practice upon which this is based.

## ***Part One - The Register***

### ***1. Background***

In the South West Health Region there was no regional registration for children with congenital anomalies until funding from the Regional Specialist Commissioning Group enabled the monitoring to begin in January 2002. There were, however, registers for specific conditions e.g. Cleft Lip and Palate and some local unit based monitoring of babies with specific abnormalities eg fetal medicine. A regional congenital anomaly register enables benchmarking within a regional clinical service and an understanding of the types and numbers of anomalies occurring in a geographical boundary that is currently not reliably accessible elsewhere.

In addition to local monitoring, there is a national notification scheme of reporting to the National Congenital Anomaly System via the Office for National Statistics (ONS). However, there is an acknowledged under-reporting with correspondingly low anomaly rates for this region. The national scheme does not collect data for elective terminations of pregnancy on babies with anomalies, or spontaneous loss before 24 weeks gestation that is collected by this Register.

In pursuit of best clinical practice Government initiatives included the establishment of a National Institute for Clinical Excellence (NICE), the aim being to provide clarity for practitioners of the most effective and cost-effective interventions, for patient's benefit. Screening programmes are amongst the issues that fall under the remit of NICE. In order to assess the effectiveness of, for example screening for a specified congenital anomaly, it is necessary to monitor the reported rates for a population. An anomaly register for the South West Region is an essential first step to meet this objective. (A First Class Service, Quality in the new NHS 13823 NHS 20k 3P Sep 98). A register can also provide information for effective planning of health care resources by providing accurate numbers of babies with anomalies occurring who will need treatment and/or corrective surgery eg paediatric cardiology, paediatric surgery. Responding to local needs as set out in the Government's White paper 'Keeping the NHS Local' that requires hospitals to know what specific services for their particular population are and can be provided by accurate information on their childhood population.

It has been the experience of other regional anomaly registers that their operation leads in a short period of time to improved quality and quantity of reported babies with anomalies. (Budd J & Cook L, Trent CAR/ONS Data Exchange. Paper presented to the 2<sup>nd</sup> Annual Study Day on Congenital Anomaly Registers, Newcastle, March 1998).

Public concerns about possible increases in rates of a congenital anomaly and the development of a cluster of cases may only be allayed by the presentation of accurate data. The operation of a regional register will be able to show true geographical patterns of location once sufficient data has been collected. It would be hard to provide such information at present and such environmental questions have been raised.

### ***2. Aims and Objective of SWCAR***

#### ***Aims***

SWCAR aims by accurate, timely and complete collection of data to:

- describe the pattern of congenital anomalies in the South West NHS Region
- disseminate data and information as appropriate to healthcare professionals
- report notifications to ONS via National Congenital Anomaly System so that accurate increased rates can be passed to local Public Health Offices indicating possible anomaly clusters.

- provide baseline population data for use in assessing effectiveness of interventions to detect and prevent anomalies.
- provide more specific and better healthcare services.

### *Objectives*

- Establish a Project Team to ensure the Register achieves its aims, within budget and time constraints.
- Inform and educate the individual units and departments providing data. This will initially comprise information about the register and how it operates followed by feedback from the Register.
- Data will be collected from any department where babies/children/fetuses with an anomaly are suspected or detected. Either a notification card or form will be completed and sent to the central registry.
- The data will be checked and then entered onto a database where further updating can occur as information is submitted.
- Regular, monthly reports of anomalies will be sent to ONS for cross checking with their reporting.
- Checking with other registers e.g. Confidential Enquiry into Maternal & Child Health (CEMACH), neighbouring regional anomalies registers.
- Issue of bi-annual newsletter to those providing data. This will include detection rates and trends. There will also be information on the progress on any research project. Planned education sessions will be publicised and presented for those working in this field.
- Register will respond to individual requests for non-identified information.
- Production of annual report to assess the progress of the Register and any research projects.
- Provide data and support to research project.

### **3. Sources of Data**

#### **All maternity units in the Region :-**

Gloucester Royal Hospital  
Cheltenham General Hospital  
Stroud Maternity Hospital  
Southmead Hospital - Bristol  
St. Michael's Hospital - Bristol  
Weston-super-Mare General Hospital  
Taunton & Somerset Hospital  
Yeovil District Hospital  
Royal Devon & Exeter Hospital  
Honiton District Hospital  
Tiverton & District Hospital  
Okehampton District General Hospital  
Royal Cornwall Hospital  
St. Mary's Hospital, Isles of Scilly  
St. Austell Community Hospital  
North Devon District Hospital  
Torbay Hospital  
Derriford Hospital - Plymouth  
Salisbury District Hospital  
Great Western Hospital – Swindon  
Royal United Hospital – Bath  
Dorset County Hospital – Dorchester  
Royal Bournemouth Hospital  
Poole Hospital

#### **Wiltshire Healthcare NHS Trust – Community Units**

Malmesbury Community Hospital  
Chippenham Community Hospital and Greenways CMU  
Trowbridge Community Hospital and CMU  
Devizes Community Hospital and CMU  
Frome Community Hospital and CMU  
Paulton Community Maternity Unit  
St. Peters Community Maternity Unit

All associated diagnostic departments attached to the above.

#### **Paediatric Units – (which treat pre-school children)**

Gloucester Royal Hospital  
Cheltenham General Hospital  
Southmead Hospital - Bristol  
Frenchay Hospital - Bristol  
Royal Hospital for Children – Bristol  
Weston-super-Mare General Hospital  
Taunton & Somerset Hospital  
Yeovil District Hospital  
Royal Devon & Exeter Hospital  
North Devon District Hospital – Barnstaple  
Torbay Hospital  
Derriford Hospital - Plymouth  
Royal Cornwall Hospital – Truro  
Salisbury District Hospital  
Great Western Hospital – Swindon  
Royal United Hospital – Bath  
Dorset County Hospital  
Royal Bournemouth Hospital  
Poole Hospital

### **Neo-natal Units (15)**

St. Paul's Wing – Cheltenham General Hospital  
SCBU The Women's Hospital – Yeovil  
Gloucestershire Royal Hospital  
North Devon District Hospital – Barnstaple  
Poole Hospital  
Royal Cornwall Hospital – Truro  
Royal Devon & Exeter Hospital  
Royal United Hospital – Bath  
Salisbury District Hospital  
Torbay Hospital  
Southmead Hospital - Bristol  
Great Western Hospital – Swindon  
Taunton & Somerset Hospital  
St. Michael's Hospital, Bristol  
Dorset County Hospital – Dorchester

### **Clinical Genetics Departments**

SW Clinical Genetics Service  
Peninsula Clinical Genetics Service  
Wessex Clinical Genetics Service

### **Neighbouring Abnormality Registers**

Congenital Anomaly Register & Information Service – Wales  
West Midlands Congenital Abnormality Register  
Congenital Anomaly Register for Oxford, Berkshire & Buckinghamshire (CAROBB)  
Wessex Clinical Genetics Service Register of Antenatally Diagnosed Congenital Malformations (WANDA)

### **National Speciality Registers**

e.g. National Downs Cytogenetics Register  
CRANE Cranio-facial Abnormalities Register

### **Local Audit Schemes**

e.g. Paediatric Surgery, Fetal Medicine, Paediatric Cardiology

### **Office for National Statistics (ONS) and the National Congenital Anomaly System**

## ***4. Nature of Data***

Registrable data may come from any baby, child or fetus with a congenital anomaly whether suspected or confirmed and whose mother is resident in the South West Health Region. NHS numbers of mother and child, hospital numbers and postcode will be recorded to enable individual mothers and children to be identified. In addition each reported case would have a SWCAR identity code number allocated.

### **Type**

The anomaly will be of a structural, metabolic, endocrine or genetic nature with the excluded conditions used in the ONS reporting system as revised for local considerations (Appendix 1).

### **Distribution**

The distribution of anomalies will be shown both geographically within the Region and the different elements of the local health services (eg PCT). The mother's postcode at the time the pregnancy ends will indicate the unitary authority and allow for investigation of cluster queries. Identification of the hospital where the pregnancy ends will allow feedback to Trusts for audit purposes. The mother's General Practitioner will be able to trace cases of anomalies amongst their patient population.

### **Incidence Rate**

The Register will provide incidence figures for a calendar year. Rarely occurring abnormalities may need to be monitored over a longer time span.

As the Register will record details on anomalies detected up to the age of 16, this will include babies diagnosed following delivery or in early childhood and beyond. The incidence rates per calendar year will be possible once the Register has recorded notifications for 2 years or when the data are considered complete enough to describe the incidence of some anomalies.

It will be possible on the database to record both babies with anomalies and the total number of anomalies. Further information on the presence of a syndrome can be recorded identifying syndromes that otherwise would have been missed.

The incidence rate will be calculated by comparison with the denominator data of total live births, total stillbirths and termination of pregnancy rates per annum.

### **Risk Factors**

Factors associated with the development of anomalies will be categorized as:

- maternal age at birth
- maternal ethnic origin (self reported)
- maternal occupation (self reported)
- maternal medical history including diabetes, epilepsy, DXR/cytotoxic therapy
- exposure to smoking, alcohol, non-therapeutic drugs, prescribed medication
- paternal age and occupation
- family history of congenital anomaly
- previous obstetric history
- use of assisted conception techniques
- multiple or single pregnancy

### **Outcome**

The outcome of the pregnancy includes live birth and death, which will include categories such as legal abortion, spontaneous miscarriage or stillbirth.

### **Diagnosis**

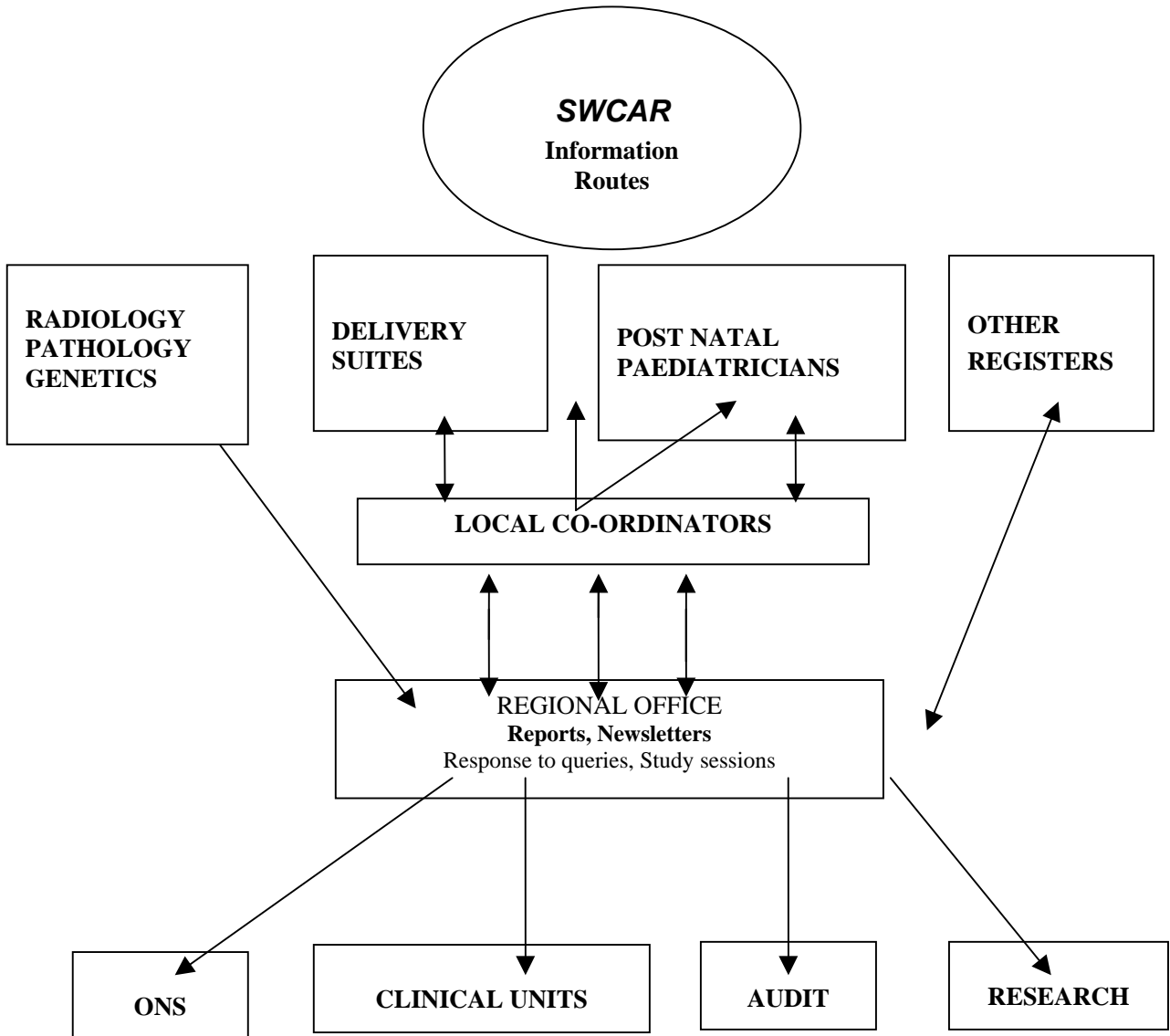
The method of detection of the anomaly will be categorized and its date to indicate gestational age. This will include:

- antenatal ultrasound
- serum screening
- karyotype – amniocentesis, CVS, cordocentesis and infant blood sampling
- examination of the new-born
- heel prick test
- x-ray

- cardiac studies
- postnatal ultrasound

In addition details of any post-mortem performed will be recorded.

## 5. Information Routes and Pathways



## ***6. Method of Notification***

### **Manual Reporting**

All cases will be reported locally and sent to the central registry for addition to the database. A two-tier system of reporting will allow for notification of both suspected and confirmed anomalies. Examples of the early warning card and notification form are included as Appendix 5 & 6 respectively. Notification of children with newly identified anomalies has shown that the A4 notification forms were not appropriate for paediatricians, mainly because they did not have the information on the mother to hand. The Register has now created an A4 paediatric form (Appendix 12) that concentrates on the anomaly and the child rather than the obstetric information. The procedure of posting these forms is outlined in Part Two of the Code of Practice to minimize the risk of confidential information becoming publicized.

### **Local Co-ordinators**

It will be preferable if the person caring for the expectant mother or parent and child completes the notification. Within each unit or department providing data to the Registry there will be a local co-ordinator. This individual will act as a source of clarification for queries about notification and for the Registry to check forms submitted. As well as providing information sheets for patients and ensuring posters are displayed in all relevant clinical areas.

### **Multiple Reporting**

It is to be expected that some cases of reported anomaly will be duplicated with notifications from a range of diagnostic departments. The database can be updated without distorting the overall incidence rate.

As consistent electronic reporting systems become available, they may replace the postal notification procedure. Care will need to be taken to protect the confidentiality of the data subjects.

### **Follow-up on suspected abnormalities**

Suspected anomalies will either be confirmed by receipt of further notifications or can be checked by the central registry once the Estimated Date of Delivery has passed.

### **Electronic reporting**

The long-term plan for notifying the Register of anomalies is to be by electronic reporting. The project team have been working on setting up a SWCAR reporting form on the STORK Maternity System available at the majority of maternity hospitals in the South West. The system went 'live' in September 2004 that enables the completed A4 notification forms to be printed out automatically.

## ***7. Registration of Notification***

### **Technology**

The software package used by the anomaly register in Wales has been adapted to meet the needs of this register. 'Visual' Basic is a relational database using 'Access' and produces reports using 'Business Objects'.

There will be a postcode checking facility to search for duplicate reports and verify accuracy of notifications. The Register also checks notifications against National Strategic Tracing System to get the NHS number and to check for the correct GP details. It is also planned to check notifications against the GP information systems and the Local Child Health Registers.

### **Quality of data**

There will be a target set of 95% for completeness of data items (fields) and 100% for accuracy. The success of any future research project is dependant on the highest quality data. Validation will take place as an on-going process to ensure the data set for each pregnancy/child is correct eg stillborn infant must be  $\geq 24$  weeks gestation. Where information is scanty, a minimum dataset has been agreed so that a limited amount of information can be put on the Register anything less than the agreed dataset is not put on the Register. Missing information is researched using local co-ordinators, remote access to maternity systems or by accessing patient records.

The experience of other anomaly registers is that audit departments and the SW Public Health Observatory will make use of the register. They will also require high quality data to assess their quality assurance programmes.

### **Ascertainment**

To ensure the Register is notified of as many anomalies as possible, the Project Team have set up a cross checking system with local hospital downloads from the patient administration systems searching for specific codes, as well as post-mortem reports, and regional cytogenetics.

## ***8. Reporting from the Register***

***Provision of an annual report and regional/local meetings.*** This would provide an opportunity for an education session for those with an interest in the field of congenital anomalies.

***Reporting to ONS with monthly incidence figures.*** With the agreement of the Directors of Public Health this will replace the current system of SD56 form completion. Completion of a single form may aid willingness to support the Register, particularly if the quality of data available is improved.

***Response to individual requests for data.*** This will most readily be achieved with anonymised data. However individual requests for identifiable data may be processed with the consent of the representative of the Data Controller once a separate MREC approval had been agreed for these requested data.

## ***9. Operation of the Congenital Anomaly Register***

SWCAR has been in operation since 1<sup>st</sup> January 2002 with support and advice being given by the SWCAR Steering Committee. All relevant specialties and the majority of hospitals in the South West are represented on the committee (list of members – Appendix 7). The committee meets at least twice a year or when deemed necessary. Their Terms of Reference are presented in Appendix 8. In addition, an executive group meets more frequently to address problems as they arise and includes the Clinical Lead, Project Manager plus one or more clinical staff depending on the identified problem.

The Project Manager reviews the Register's Code of Practice annually and the SWCAR Steering Committee supports any changes. The movement of all data collected and released for the SWCAR must adhere to the policies outlined in Part Two (Confidentiality & Disclosure of Patient Information) & Part Three (Department of Clinical Science South Bristol IT Policy document). In addition, all staff employed by this Register are required to read and comply with these policies

and to sign a confidentiality statement on employment making the employee open to disciplinary procedures if there is proven non-compliance with this Code of Practice.

The following states the basic responsibilities of the Register with supporting information and details documented in Parts Two and Three:

- Ensure staff are aware of their responsibility to maintain confidentiality and security and adhere to the *SWCAR Code of Practice – Confidentiality, Security, Ethics and Disclosure of Patient Information* in relation to both general work activities and operation of the register in particular – signed declarations of understanding of this commitment and periodic reviews of the Code of Practice and work practice.
- Ensure all staff adhere to the Leaving Procedure – whenever a member of staff leaves, any relevant security system should be changed and all keys, swipe cards etc should be handed in. The leaving procedure, including the network leaver’s form, must be worked through, completed and signed. All network access will be revoked. Further details are available in the Department IT Security Policy.
- Ensure confidentiality is maintained when collecting, transmitting (by any method), storing, checking and disclosing data both within the register and externally.
- Limit access to the information stored on the database by:
  - User identification and password access only
  - Passwords and user keys not visible on the VDU
  - Issue all staff with identification badges
- Record all forms and documents sent to or from the central register office
- Limit the output of identifiable information by
  - Demonstrations of the database to use fictitious data
  - Tables and other information provided in routine reports to be devised with appropriate levels of detail to minimize the risk of identification
- Disposal by burning or shredding, of confidential material that is no longer required
- Requests for identifiable information to be passed via the data controller or designated representative
- Research requests for information must be in writing – stating the exact purpose for which data is required, the nature of the information, declaration as to its security and the duration for which the information is required along with disposal provisions.
- Transmission of information to or from the register to be controlled in the following ways:
  - (i) Postal:
  - (a) Completion of notification forms

Use of plain, sealed envelopes, not internal transit envelopes. Use of envelopes for forms, marked 'private and confidential'. Suspected abnormality notification cards to be sealed and marked 'confidential'

(b) Information from the register

Written and anonymous or pseudonymous information sent from the register to be marked 'confidential' and for personal addressee only.

(ii) Computer:

Identifiable information to be separated from other information during transmission from the register. Use of passwords for access. Storage of data should be on a stand-alone server (virtual private network). SWCAR is planning to set up a VPN.

(iii) Oral Transmission

No identifiable or confidential information to be transmitted via the telephone, any such requests to be put in writing to the data controller or deputy. There should be a designated person to handle any requests for information from the press or general public.

**Security**

- All confidential paper data including notification forms to be kept securely locked when not in use.
- Disposal of confidential information that is no longer required.

**Policies**

- Named lead for confidential & security policies – Mrs Rosie Thompson, Project Manager
- Date of review for Code of Practice – Confidentiality, Security, Ethics and Disclosure of Patient Information – October 2005

## ***Part Two – Confidentiality & Disclosure of Patient Information***

### ***1. Introduction***

This Code of Practice is based on current standards and practice; however, this document will be updated over time as and when these standards and practices are changed. A relevant web address for each principle has been given to aid the reader.

Healthcare clinicians are advised to supply data and to support congenital abnormality registers to help them provide an efficient and cost effective service. However, the healthcare clinicians and the Register's staff need to ensure that during this process the confidentiality of the patient is protected.

#### **Duty of Confidence**

**Confidentiality: NHS Code of Practice** guidance from the Department of Health, July 2003. (<http://www.doh.gov.uk/ipu/confiden/protect.htm>)

**The Data Protection Act 1998: An Introduction** from the Data Protection Registrar, October 1998 (<http://www.hmsa.gov.uk/acts/acts1998/19980029.htm> or <http://www.informationcommissioner.gov.uk>)

**Health & Social Care Act 2001** (<http://www.doh.gov.uk/ipu/confiden/act/s60bg.htm>)

**The Caldicott Committee:** Report on the Review of Patient Identifiable Information, December 1997 (<http://www.doh.gov.uk/confiden/crep.htm>)

**Duties of a Doctor:** Guidance from the General Medical Council, October 1995 (<http://www.gmc-uk.org/standards/doad.htm>)

### ***2. Basic Principles***

#### **The Duty of Confidence**

There is a long established common law principle whereby any personal information given or received in confidence for one purpose may not be used for a different purpose or passed to anyone else without the consent of the provider. All employees who handle such information are bound by this principle and form the basis on how the NHS will develop a patient centred service where information is shared between all those involved in delivering or developing care. The Government has made it clear that informed consent is the fundamental principle governing the use of patient identifiable information by any part of the NHS or research community. The NHS is 'committed to the delivery of a first class confidential service'. This means ensuring that all 'patient information is processed fairly, lawfully and as transparently as possible'. The Department of Health has established guidelines on Confidentiality with a Code of Practice for those working in and allied to the NHS.

Fixed on the foundations of a duty of confidence are legal obligations such the Data Protection Act 1998, Human Rights Act 1998 and Health & Social Care Act 2001 Section 60 that are incorporated in the NHS Code of Practice. These Acts of Parliament are in place to ensure that confidential information is treated correctly.

#### **Data Protection Act 1998**

The Data Protection Act 1998 provides a framework that governs the processing of information that identifies living individuals. Processing includes holding, obtaining, recording, using and disclosing information and the Act applies to all forms of media, including paper and images. The Act is based on a principle of openness between the sources of the information and the user(s) and personal data should be obtained fairly and lawfully. Each user(s) must be registered as a Data Controller, a legal person, who determines the purpose for which data is processed. All registered data users must comply with the data protection principles in relation to the data they hold. To satisfy Data Protection Act 1998 the data controller should satisfy one condition in each schedule.

SWCAR is covered under schedule 2 (public function and legitimate interests of data controller) and schedule 3 (medical purposes). Second principle: SWCAR are registered under the DPA to use data for medical and research purposes and data uses are limited to those purposes. Third principle: Identifiable data are required for the core purposes of congenital anomaly registration but the uses and releases are rigorously controlled. Fourth principle: Considerable effort is invested in the quality assurance of the data to ensure accuracy. Fifth principle: The nature of congenital anomaly registration is such that the data collected now and in the past increases in relevance and usefulness over time. The purpose of the registration process is to monitor congenital anomaly prevalence, detection and outcomes over time in addition to monitoring changing environmental risks. For this reason data are retained indefinitely. Sixth principle: Procedures are in place to satisfy the rights of data subjects within the DPA and in line with Department of Health guidelines. Seventh principle: Rigorous policies and procedures are in place to protect against unauthorised or unlawful processing of data. Details of the confidentiality and security policies implemented within congenital anomalies registers are provided in Parts Two and Three of this Code of Practice. Eighth principle: Identifiable information is not transferred outside the EEA. SWCAR complies with NHS standards of Security and Confidentiality.

The SWCAR processes information in pursuit of legitimate interests – medical purposes and therefore does not seek explicit consent. The Register provides Information Sheets (appendix 9) and Posters for Clinic Users to satisfy ‘fairness’ so that the data subject can identify who holds their personal information, what it will be used for and the likely disclosures. The data collection process is considered lawful with support from PIAG and Section 60 of the Health & Social Care Act 2001 that makes it lawful to disclose and use patient information in specified circumstances.

### **Health & Social Care Act 2001**

For the NHS to improve care by sharing patient information posed a problem as informed consent could not always be obtained. Section 60 of the Health & Social Care Act 2001 provides a power to ensure that patient identifiable information needed to support essential NHS activity can be used without the consent of patients. The power can only be used to support medical purposes that are in the interests of patients or the wider public, where consent is not a practicable alternative and where anonymised information will not suffice.

SWCAR obtained Section 60 support in July 2002 (Appendix 10) through an umbrella application from the British Isles Network of Congenital Anomaly Registers (BINOCAR), which means it is lawful for healthcare professionals to share patient information with the SWCAR. The application (Appendix 13) was made to the independent statutory Patient Information Advisory Group (PIAG) who on behalf of the Secretary of State for Health gives support for patient identifiable information to be collected without consent if good reason is given. The arguments given for the application are detailed in Appendix 13.

### **General Medical Council**

In addition to the NHS confidentiality guidelines, Doctors and other health professionals are governed by their own professional rules of conduct. Patients have a right to expect that you will not disclose any personal information which you learn during the course of your professional

duties, unless they give permission. Without assurances about confidentiality patients may be reluctant to give doctors the information they need in order to provide good care.' (GMC Guidelines, Oct. 1995). These guidelines are now considered out of date as they do not take into account the Section 60 support now available and therefore contradicts the lawful collection of personal data without consent. GMC Guidelines are in the process of being updated in *Confidentiality: Protecting and Providing Information 2003* where it is proposed that in the situation of a doctor providing information for a disease register or for epidemiology studies the following guidance will be given:

“First, it is important to remember that professional organisations and government regulatory Bodies, which monitor the public health or the safety of medicines or devices, rely on information from patients’ records for their effectiveness in safeguarding the public health. You must provide relevant information wherever possible. Law requires the notification of some communicable diseases.

In other cases, you should provide information in anonymised form, where this is practicable, and anonymised data will serve the purpose. Where this is not the case you should seek express consent to disclosures, if that is practicable.

In England and Wales, Section 60 of the Health and Social Care Act 2001 provides for Regulations to be made allowing for the disclosure of information for specified purposes, without consent, but without breaching common law requirements of confidentiality. Regulations are made where, following consideration by the Patient Information Advisory Group (PIAG), it has been decided that there is a significant potential benefit from the research, and that it will not usually be practicable to seek consent from patients, or to anonymise the data. For this reason, where a Regulation has been made, you may rely on the PIAG assessment that it is not practicable to seek consent to disclosures.

In all circumstances you must inform patients about the disclosure and their right to object (or be satisfied that such information has been provided), wherever that is practicable. You must respect objections wherever that is practicable, or explain to patients why it is not practicable for you to do so.”

### **Ethics**

Recently it has been suggested that MREC approval should be sought for all congenital anomaly registers in England to ensure that data are collected and used for ethical reasons. BINOCAR submitted an MREC application for all registers in May 2004 and was given MREC approval in July 2004 (Appendix 11). All LRECs have been notified of this approval, although as there is no local investigator this was done for LREC’s information only. R&D Registration for each Trust in the South West is currently being sought. Any application for MREC using SWCAR data should be sent to the Trent MREC.

### **Caldicott Principles**

Disclosure of patient identifiable information should also comply with the principles outlined in The Caldicott Report (December 1997). Both users and providers of patient identifiable information should be aware of their ethical, professional and legal responsibilities. All Caldicott Guardians have been contacted and informed of this register.

### **Disclosure**

In addition to the principle of confidentiality, disclosure implies specific consideration for the security of the personal data and prevention of unauthorized access. For anomaly registers providing baseline information for clinical research projects, the guidelines provided for Local Research Ethics Committees (LREC) are relevant. (HSG (91) 5). These relate to storage of data and prevention of unauthorized disclosure of identifiable information. The aim of the register is primarily to improve healthcare in the South West; however, data will be available for research

projects. For any future research project, the SWCAR will only disclose data with LREC or MREC approval.

In conclusion, Part Two of the SWCAR Code of Practice demonstrates that SWCAR has statutory as well as ethical support to collect patient identifiable information without consent. Collecting confidential data in keeping with statute and guidelines has to be supported by a robust IT security Policy. Part Three gives details of how data are stored within the Institute of Child Life & Health, University of Bristol.

## ***Part Three – IT Security***

### ***1. Overview***

The purpose of this IT Security policy is to define a framework on how to protect the Departmental computer systems, network and all data contained within, or accessible on or via these computer systems from all threats whether internal, external, deliberate or accidental. This policy recognises that the Department's work involves management of data that is of the utmost sensitivity to subjects, research and funding partners, staff and students. With reference to ISO 17799, this policy is designed to proactively meet and exceed standard security policies.

#### **Departmental policy**

It is the policy of the Department to ensure that:

- All computer systems and information contained within them will be protected against unauthorised access.
- All computer systems and information contained within them will be protected against systems failure.
- All members of the Department are aware of their responsibility to adhere to this policy.
- All members of the Department will fulfil their responsibilities to adhering to, implement and promote this policy within their areas.
- The integrity of all computer systems, the confidentiality of any information contained within or accessible on or via these systems is the responsibility of the Caldicott guardian/Departmental data protection Officer or representative.
- The Department will meet all regulatory and legislative requirements regarding computer security and information confidentiality and integrity.
- All breaches of security will be reported to and investigated by the Departmental Technical Manager.
- All entrusted offices will proactively promote, review and implement enhanced security features.
- All data is protected by a monitored backup system and comprehensive recovery plan.
- The primary role of the Department regarding education and research is not hindered but is advanced by adhering to this security policy.

## ***2. Statement of Authority and Scope***

This policy is intended to detail the rules of conduct for all users given authority to use the computing and network facilities run by the Department.

Users must also abide by University of Bristol's Computing Service's Regulations and code of conduct for the use of computing facilities:

<http://www.bris.ac.uk/Depts/Secretary/regscomp.htm>

<http://www.bris.ac.uk/is/selfhelp/documentation/code-g1/code-g1.html>

Users must also abide by the Departmental policies additionally implemented so as to proactively promote good security practices.

Users will promote good security practices in accordance with this policy and as set out in the Departmental guidelines.

### **Compliance**

This document is made with reference to ISO 1779. The Department complies with and adheres to all its current legal responsibilities including Data Protection 1998, Electronic Communication and Human Rights, Computer Misuse, Copyright and Intellectual Property.

## ***3. Statement of Responsibilities***

### **Users**

Every user of the Departmental computer services has a duty to ensure the security and integrity of information in the system and must understand the responsibilities for this. They must:

- Be conversant with all security orders and instructions issued for use with the system, e.g. this policy.
- Use the appropriate built-in security features of the system, e.g. passwords.
- Ensure that all computer account information pertinent to individuals, e.g. accounts and passwords, are managed accordingly, are not shared, written down or generally misused.
- Not store data on local hard drives.
- Report promptly any incidents that may have security significance to the Departmental Technical Manager.

The Department Technical Manager is responsible for providing central security measures to protect the Department's computer systems and networks from external threats. This includes assessment of threats, provision of advice to departments, provision of tools and software (e.g. virus scanners) and implementation of any security systems (e.g. firewalls and virus scanners).

The Department Technical Manager is responsible for liaising with the University's Computing Services to promote and implement the University's security policies. Supplementary to this, The Department Technical Manager will be responsible to the Head of Department for providing enhanced security measure that will protect the Department's unique data resources. The Department Technical Manager will proactively pursue this policy.

The Department Technical Manager will ensure that the Department is invested with the necessary skills and expertise to carry out this policy

#### ***4. The Computing Environment***

The Departmental Computing Services plan, support, maintain and operate a range of central computing servers, core network switches, backup systems, and the overall network infrastructure connecting these systems to The University Campus network.

The computing environment is defined as all computing resources and network infrastructure managed and overseen by Departmental Computing Services and all computing devices that can physically connect, and have been authorised to connect, to this environment. All are covered by this policy, including computing hardware and software, any related data residing on these machines or accessible from these machines within the campus network environment and any media such as CD-ROMs, DVD-ROMs and backup tapes that may at times be accessible.

##### **Non-managed resources**

The Departmental Computing Services also considers all temporary and permanent connections via the University network, casual laptop docking points and RAS modem pools to be subject to the provisions of this policy. Computing resources not managed by the University or the Department will not be connected to the network without the express permission of the Head of Department. On receiving consent, such resources will be accessed by The Department Technical Manager. The Department Technical Manager will ensure compliance with University Computing policies in general, and the Department's security policies in particular.

##### **Monitoring**

As a function of this policy, the Department is required to monitor, log, collect and analyse the content of transmissions on networks maintained by The Department at any time deemed necessary for security purposes. Any network monitoring will be performed in accordance with the relevant national and international legislation.

##### **Internal Integrity**

The internal integrity of the Departmental computing system will be ensured by the enforcement of security policies enforced through:

- Good practice.
- Physical security.
- System security.
- Integral password and user name policy.
- Programs of end-user education.

All computers will be set up and installed under the supervision of the Department Technical Manager in accordance with this document.

Only application software supported by the University Computing Services or the Department will be installed on Desktops.

Only operating systems fully supported by the Department will be installed on Servers.

No resource sharing services will be activated other than those approved by University Computing Services or the Department.

##### **Support**

The Department Technical Manager will be responsible for the provision of adequate user and system support. This will be directed to ensuring the maximum efficiency and security of the Departmental computing systems.

End-user Support will be provided between 08:00 to 16:00. This will be accessible via telephone, email and open surgery.

## ***5. Computer Access***

### **Accounts**

Valid user accounts are only issued by University Computing Services for individual use. These accounts are only valid on central systems and will not be duplicated elsewhere. Accounts should not be shared, given away or offered for use to anybody else. User accounts issued by University Computing Services are for the sole use of the individual to which they were issued. Accounts will be deleted when the user leaves the Department, in accordance with the Department's Leaving Policy.

### **Contact**

The Department Technical Manager is the initial contact point for users who wish to obtain new accounts and receive training and documentation in the use of Departmental computing systems.

### **Induction**

All new users will undertake an induction given by the Departmental Technical Manager who will be appropriately qualified.

### **Access to Departmental resources**

To gain access to the appropriate Departmental computer resources a request must be made to the Department Technical Manager. Where the user is not a member of the Department, the permission of the Head of Department will be required.

### **Levels of access**

An assessment will be made by the Department Technical Manager, in consultation with the appropriate line manager, upon individual access requirements. This will be based upon a policy of least need. The Department does not permit open access to Departmental Computing systems.

### **Personal storage space**

All users will be provided with appropriate protected personal file store. Users may additionally be provided access to protected shared resources, as requested by their line manager.

### **Password policy**

All machine-generated passwords will be changed immediately. Passwords may be subject to a checking program, to ensure acceptance users must follow the following password policy:

- Passwords must not be dictionary words.
- Passwords should not use proper names.
- Passwords must be a minimum length of six alphanumeric characters
- Passwords will not be disclosed to any third party including computer officers and line managers

- To request a password reset users will contact the Department Technical Manager who has the sole responsibility to request a reset.

## ***6. Physical Security***

### **Servers**

The Department Technical Manager provides a secure server room with UPS and controlled environment. Access is restricted to The Head of Department and the Department Technical Manager. Access to secure room and securable chassis keys will be restricted to the Department Technical Manager and Head of Department.

### **Desktops**

All Desktop machines will be sited in secure rooms and sections and be secured by logon password protection that can only be activated by unique username and password combination. All users will either lock or log off unattended desktop machines and lock their room on exit

### **Laptops**

Laptops will always be secured in a locked cupboard within a locked room. Laptops will not to be left in unattended vehicles. No data is allowed to be stored on local hard drives of laptops, unless encrypted using a mechanism installed by the Department Technical Manager.

### **Network**

The network will be regularly inspected for unauthorised attachment or tapping. Access to the network will only be activated by unique username and password combination. Network devices such as switches and hubs will be physically secured.

The short-term plan is for the SWCAR Register to sit on a virtual private network accessible only by the SWCAR team.

### **Data storage**

All data will be stored on the secured network file stores and will only be activated by unique username and password combination. No data is allowed to be stored on local hard drives.

### **Keys**

The Department Technical Manager will secure all keys. Duplicate keys will be placed in a sealed envelope and secured by the Departmental administrator. These can only be released by consent of the Head of Department

### **External doors**

The Department employs card access security systems and CCTV to all external entry doors.

## ***7. General Computing***

### **Use of resources**

All users will ensure the proper use of the Department's computing resources through:

- Proper management of accounts & passwords.
  - Proper management of login sessions eg proper signoff
  - Respect of software copyrights and licence restrictions. In general software and datasets should not be used for commercial purposes unless specifically licensed for such use.
  - Proper management of sensitive information:
  - All users will be instructed in their data protection duties.
  - No data is allowed to be stored on local hard drives.
- 
- Users will be directed to familiarise themselves with the University Computer Services code of conduct.

### **Data protection**

All users will ensure their compliance to relevant national and international legislation when handling data. They will familiarise themselves with both University and supplementary Departmental data protection policies.

## ***8. Internet Access***

### **Janet**

The Departmental network is connected to the Internet via the Joint Academic Network (JANET) through the University's campus network. All users, subject to adherence to policies referred to in elsewhere in this document, may access the Internet.

### **Responsibilities**

All users will abide by the University's Computing Service's regulations and code of practice:

<http://www.bris.ac.uk/Depts/Secretary/regscomp.htm>

<http://www.bris.ac.uk/is/selfhelp/documentation/code-g1/code-g1.html>

### **External boundary**

The campus network interconnects with JANET through University Computing Services managed routers. These protect the University's network and systems from unauthorised or illegal access or attack from the external environment. Traffic or connections initiated from the campus network are generally not restricted unless identified as unacceptable by University Computing Services.

## ***9. Intranet (Campus) Access***

### **Connection policy**

The majority of Departmental computers will need to connect to the campus LAN. Individuals are not allowed to connect to any machine to the LAN. The Department adheres to The University's University Computing Services connection policy.

### **Restrictions**

Access to Departmental resources from outside of the Department will be generally restricted based upon IP monitoring. Unsecured FTP access to Departmental resources will be disabled except in extraordinary cases after consultation with the Departmental Technical Manager. In these cases a different username/password pair must be used and the FTP server must be a dedicated FTP server, physically separate from the Departmental Data servers.

## ***10. Remote access***

### **Policy**

All server resources are hidden from general browsing and external access. Users connected to the network via any remote access mechanism are subject to the same rules and regulations, policies and practices just as if they were physically within the Department. University facilitates remote access via dialup (Ascend) and/or Nomadic for broadband users.

### **Service**

Remote access will be granted to users only after consultation with the Departmental Technical Manager. Each user will receive the minimal access required for their work.

## ***11. Email***

### **Policy**

All users with valid accounts may send and receive email. Users will not in any way forge electronic mail or otherwise misrepresent themselves, other individuals or the University in any electronic communication. All email accounts have quota limits placed on them. The University Computer Service backs up all email accounts to tape on a regular basis.

### **Responsibilities**

All users will abide by the University's electronic mail policies.

### **Sending confidential data**

Confidential data will not be sent by email unless:

- Permission has been sought from the user's line manager.
- The Departmental data protection adviser is consulted.
- Approved encryption mechanisms are employed, eg PGP. (Word and Excel password protection is not appropriate!)
- The recipient is known
- The recipient can confirm receipt immediately

## ***12. World Wide Web Server***

### **Policy**

The Departmental web server will run minimum services that supports only web serving. The operating system and platform will run a secured operating system.

## **Services**

The Department web server will only run web sessions. No mail, printing or other such services will be run.

## **Users**

All users have the right to publish their own WWW pages on the Departmental web server. They must request an account from the Department Technical Manager.

Individual users will be responsible for content in these areas and the University reserves the right to remove access to any material which it deems inappropriate, illegal or offensive. Users should not in any way use personal WWW space for commercial purposes.

Users shall not in any way use personal web space to publish material, which deliberately undermines IT security at the University or elsewhere. Users shall not publish any information regarding open accounts, passwords, PINs, illegally obtained software licences, hacking tools, common security exploits or similar unless there are specific and legitimate reasons to do so.

## ***13. Departmental File Server / Store***

### **Policy**

All file servers will be protected with UPS and will run minimum services that support only their specific function. Servers will not be allowed to cross mount directories and FTP and Telnet services will be explicitly removed. Where practical access to shares and services will be limited to the Departmental subnet. All file stores will be regularly and routinely backed up using industry standard software and non- proprietary media.

### **Access to resources**

All users will have access to a secured home directory, and as requested by line-managers, necessary project resources. The will be secured by a unique username password combination. Logging monitoring will be initiated.

All shares will be hidden, except a common directory to support teaching.

Accounts that are removed will have their files archived. Ghost accounts will be removed. Unless specifically requested no other archiving takes place. The Departmental file servers will not broadcast personal, project or administrative shares.

### **Passwords**

Only the Department Technical Manager shall have full access to server passwords. If the password has been forgotten the Department Technical Manager can reset a new password.

### **Security and error logging.**

The Departmental file stores will be audited for security and error logging. All the following will be reported to the Chair of the Departmental IT strategy group.

- Failure of the backup service.
- Failure of file store services.
- Discovery of security vulnerabilities.
- Failure of server hardware.
- Failure of Server software.

### **Virus scanning**

All files are scanned for viruses as they are transferred to and from the server. It is the responsibility of the Department Technical Manager to ensure that up to date virus signatures are maintained.

## ***14. Backups***

### **Policy**

All file partitions across the Department's Computing system will be backed up once a week during a Thursday night using industry standard backup software and open systems devices and media.

### **Storage**

The Department Technical Manager will securely maintain system backups off site. A full backup archive of the system is put aside and stored separately at the beginning of each year.

### **Audit**

All Backup media will be audited and checked for defects and errors and secured by a password. A minimum of three weeks backups will be stored securely off-site under the supervision of the Department Technical Manager.

Any user can request a restoration of data. The Department Technical Manager will maintain logs of the backup routines, and immediately report any issues to Chair of the IT Strategy Group.

## ***15. Anti Virus Security***

### **Policy**

The University Computing Services provide means by which all open files on client machines will automatically be scanned for viruses. Virus signature updates will be handled automatically. If a machine is detected behaving abnormally due to a possible viral infection it will be disconnected from the network until deemed safe.

### **Services**

The Department Technical Manager will ensure that, where appropriate the file stores are protected by an independent and up to date virus checker.

### **Infection procedure**

If any user suspects viral infection on their machine, they will contact the Department Technical Manager immediately.

## ***16. Contingency planning***

## **Policy**

The Department Technical Manager will ensure that the Department can recover from any degree of Central systems failure, from single hard disk failure through to catastrophic systems failure. This will be achieved by ensuring that complete data reconstruction is possible across the whole system. Recovery will permit roll back to the last integral backup cycle. The Department Technical Manager will ensure that the Department is invested with the skills and proficiency to support this policy.

## **Threats**

The main identified threats are:

- Power failure
  - Hacking
  - Hardware failure
  - Software failure
  - User error at all levels
  - Measures implemented
  - UPS protection of all critical components.
  - Controlled server room environment.
  - Fully automated and audited backup regime.
  - Rolling maintenance plan.
  - Stocking of critical components.
  - Support training program.
  - Implementation of open systems policy.
  - Use of off-shelf components.
  - Recovery priority
- 
- Departmental File service
  - Departmental Unix service
  - Departmental Printer service
  - Departmental Web service
  - Departmental RAS service

## **Maximum Recovery times**

- Software or hardware failure: next day arrangement with the University's Computing Service if parts are in stock.
- Utility Services failure: 14 hours  
Assumes 12 hour utility downtime and 2 hour recovery program
- Facilities failure: 7 days

## **Recovery Media**

The Departmental Computer Officer will be responsible for the storage of three weeks of contemporary backup media off site. This will include all operating system installation media and drivers. The Department Technical Manager will lodge a contact number with the Departmental administrator

## **Hardware**

All hardware will be regularly inspected and serviced as appropriate under the supervision of the Department Technical Manager. All system critical components will be under extended warranty where appropriate.

### **Fail over storage capacity**

Sufficient storage capacity will always be available so as to support the failure of one file store. This will be measured as capable of supporting all user home directories and project shares.

### **Fail over processing capacity**

Sufficient processing capacity will always be available so as to replace the complete failure of the main Departmental file server.

Appendix 1

### **Minor defects that need not be reported**

The following minor defects are excluded from registration unless occurring in combination with other anomalies. If there is any doubt in a particular case, please report it.

#### **Anomalies of eye**

- Stenosis or stricture of lacrimal duct

#### **Anomalies of ear**

- Minor or unspecified anomaly of ear
- Preauricular appendage, tag or lobule
- Other appendage, tag or lobule

#### **Cardiovascular system**

- Functional or unspecified cardiac murmur
- Absence or hypoplasia of umbilical artery, single umbilical artery
- Patent ductus arteriosus (in babies <37 weeks or <2500 gms))

#### **Digestive system**

- Tongue-tie

#### **External genitalia**

- Congenital hydrocele or hydrocele of testis
- Phimosis

#### **Limbs**

- Clicking hips
- Clubfoot of postural origin/positional talipes (**DO** notify if ongoing care)
- Postural or unspecified metatarsus varus or metatarsus adductus
- Postural or unspecified talipes calcaneovalgus or pes calcaneovalgus
- Minor or unspecified anomalies of toe such as hallux valgus, hallus varus, or “orteil an marteau”

#### **Other musculoskeletal anomalies and anomalies of the integument**

- Spina Bifada occulta uncomplicated
- Pectus excavatum
- Minor or unspecified anomaly of nose
- Minor or unspecified deformity of face
- Minor anomaly of nipple
- Accessory or ectopic nipple
- Congenital umbilical hernia, para umbilical, ventral or incisional hernia
- Abnormal palmar crease
- Skin tag with surface less than 4cm<sup>2</sup> ; skin tag, angioma, glomus tumour, lymphangioma, birthmark
- Naevus (**DO** notify if naevus subaceous or port-wine stain)
- Haemangioma (**DO** notify if giant haemangioma)
- Sacral dimple

**Confidentiality and Security  
Guidelines for good practice**

With the current climate of sensitivity and concern surrounding the handling of identifiable patient information, the FSID research unit has decided to create the following guidelines for good practice. The guidelines cover the processing and holding of personal identifiable data collected by staff of the FSID Research Unit plus accessing and working within a secure department. This document sets out the guidelines for good practice in the area of confidentiality and security, although it is not an exhaustive list, each individual has a responsibility to ensure they behave in a manner, which would be deemed acceptable when processing these data.

Please ensure you read these guidelines as well as the Department IT Security Policy, and sign the bottom to indicate that you have read and understood what is required of staff in the FSID Research Unit.

1. All members of staff processing patient information should be aware that it is a disciplinary offence to jeopardise or breach the confidentiality and security of these data.
2. Individual security passes should not be lent or given to other members of staff to enable that member of staff to access different areas within the UBHT and University. This would be considered a disciplinary offence.
3. All members of staff should safeguard access to secure areas by:

Checking security passes of those people trying to gain access to a secure area. Do not let anyone into the building or department or other department within the UBHT or University when accessing a secure area eg NICU, PICU. For example if anyone is following you into a secure area either check their security pass or make sure the door is closed behind you so that they have to use their pass to enter.

If no security pass is available, they should be signed in and escorted to the people they are seeing or telephoned for that person to escort/greet them

Stopping any individual unknown to you who may have already gained access to check if they should be there.

If possible, do not use the security code when other people are in the lift. Wait until they have left the lift then use the code.

Do not give the department lift access code to an unknown person.

If you are uncomfortable about someone found in the department or other secure area, report this to another member of staff.

4. Processing of identifiable patient information:

All paperwork containing identifiable patient information should be stored securely overnight or when away from your desk. All such paperwork should routinely be placed on your desk upside down so that the casual passer-by cannot read the information.

Any identifiable patient information on a computer should be double password protected, the first when gaining access to the computer and then when gaining access to the database. These passwords should not be given to any staff outside the FSID Research Unit.

Screensavers should be used that are enabled if the computer is idle for more than 5 minutes.

No identifiable patient information should be faxed or emailed. Information should be anonymised before faxing/emailing and the identification of the individual should be given directly over the telephone to the person receiving the fax/email. A fax header should be used at all times giving instructions to those receiving the fax what to do if pages are missing or if received by mistake. If an email is received by mistake specific instructions should be given routinely at the beginning or end of an email.

Names and addresses of patients should not be routinely discussed over the telephone. If this has to be carried out you should ensure you are speaking to a known individual and that there is no one eavesdropping your conversation.

All paperwork with identifiable patient information should not be routinely posted. This should be sent anonymously if possible. If this is not possible this information must be sent in a sealed plain envelopes marked 'to be opened by addressee only' plus 'confidential'.

5. Disposal of identifiable patient information

All identifiable and anonymised patient information should be shredded and put for 'confidential waste' when not required anymore. No other form of disposal is acceptable.

Paperwork should be anonymised for archiving.

All archived paperwork should be stored securely in locked filing cabinets in a locked/secured area.

6. Passing on of identifiable patient information

Routinely, this should not take place. Any verbal requests for identifiable patient information should be supported by a written request and sent to the Project Manager.

No information should be routinely given out over the telephone/email/fax etc. Anonymised aggregated regional information may be given out upon formal request rather than any local information, as that may still be identifiable, even though it is anonymised.

7. All members of staff will complete a confidentiality statement for their particular study.

Signed: .....

Printed name: .....

Date: .....

Please sign and date, and then photocopy when completed to keep for your records. If there is anything in the above you do not understand, please discuss with the Project Manager.

Specimen Declaration by Staff

SW CONGENITAL ANOMALY REGISTER

Name:

Position

Workbase and contact number:

I confirm that I have read and fully understand the confidentiality and security document title 'Code of Practice – Confidentiality, Security, Ethics and Disclosure of Patient Information'.

I recognize that I am required to keep identifiable information confidential. There should be no passing of such information without either the permission of the Chair of the SWCAR Steering Committee, Professor Peter Fleming, Professor of Infant Health and Developmental Physiology, or the data subject.

Any requests for information from outside the Register should be directed to the SWCAR Steering Committee or the Project Manager.

I am required to keep my personal identification password private no others are able to use it. Any loss of this password needs to be notified to the Technical/IT Security Manager, Mr Jason Merrick, so that it can be erased and a substitute password issued.

Failure to respect the confidential nature of the data constitutes a breach of my employment contract and may lead to dismissal.

I understand that further guidance about confidentiality may be obtained from the University of Bristol's Data Controller Co-ordinator.

Signature:

Date:

Appendix 4

INSTITUTE OF CHILD LIFE & HEALTH

---

**INFORMATION SHEET FOR HEALTH PROFESSIONALS**

**THE SOUTH WEST CONGENITAL ANOMALY REGISTER**

The South West Congenital Anomaly Register (SWCAR) has been set up to prospectively collect all birth anomalies that have been identified at any stage of development *in utero*, including at delivery and later in life, normally up to 16 years of age. **Notify all newly identified abnormalities as from 1<sup>st</sup> January 2002** exclude abnormalities diagnosed before this date.

### ***A5 warning card***

**PLEASE COMPLETE AND RETURN A CARD FOR ANY CONGENITAL ABNORMALITY YOU ENCOUNTER. WE WOULD RATHER RECEIVE SEVERAL CARDS ON ONE PATIENT THAN MISS A PATIENT.**

As a healthcareer you should complete the A5 notification card (warning card) if you suspect there is an anomaly or if there is a confirmed anomaly. The A5 notification card should be completed, sealed and sent to the regional office with as much information as possible. At this stage please ensure the NHS Number is noted if you know it; otherwise ensure the postcode is given. This warning card should be completed if you have identified an anomaly for the first time, or if you do not know if the A5 warning card has already been sent. The regional office is expecting to be notified of a baby with one or more anomalies by more than one person in the majority of cases. If in doubt complete a card and send it to the regional office. If you know an A5 card has been completed, please complete the A4 forms now that you have more information.

### ***A4 notification forms***

The A4 notification forms are for when the anomaly or abnormalities are confirmed and/or when more information is available. If you do not know if one has already been completed, please complete this form and return it.

### ***Paediatric form***

A new form has been produced to collect anomalies diagnosed later in childhood. The form concentrates on the anomaly and how it was confirmed rather than the obstetric records; these would be collected separately from the hospital maternity system. Please complete this form and return to this office.

### ***Information Sheet***

The register is not seeking consent from the patient and the Information Sheet should be given to the patient or patient's parent/guardian at the time of a suspected anomaly or when an anomaly is identified. This information sheet is provided to satisfy the Data Protection Act 1998 only and provides details of what information is kept on the patient, where it is kept and how they can obtain a copy of this information. **Please seek advice on this if you are unsure.**

### **Posters**

To satisfy Data Protection Act 1998 it is advisable that each diagnostic department within a Trust who routinely provide data for the SWCAR, should display a poster for clinic users to inform them that it is the policy of your Trust to provide data on congenital abnormalities to the SWCAR. These posters are available from the SWCAR regional office.

### ***Trust Co-ordinator***

Your local SWCAR Trust co-ordinator is:

The remit of the Trust Co-ordinator is to provide additional cards and forms, help with completion of forms and to cross check that forms have been received.



## South West Congenital Anomaly Register (SWCAR)

### *Steering Committee*

Professor Peter Fleming (Chair) Professor of Infant Health & Developmental Physiology	St Michaels Hospital Bristol
Mr Tim Overton (Clinical Lead) Consultant in Fetal Medicine	St Michaels Hospital Bristol
Mrs Rosie Thompson (Project Manager)	Institute of Child Health UBHT Education Centre Bristol
Ms Maggie Brooks Midwife	Antenatal Clinic Co-ordinator Cheltenham General Hospital
Dr Peter Turpenny Consultant Clinical Geneticist	Royal Devon & Exeter Hospital Exeter
Mr Dominic Byrne Consultant in Fetal Medicine	Royal Cornwall Hospital Truro
Mrs Julia Drury Midwife	North Devon District Hospital Barnstaple
Professor Alan Emond Professor of Child Health	Hampton House Bristol
Ms Jenny Ford Midwife	St Michaels Hospital Bristol
Miss Melanie Robson Consultant Obstetrician	Taunton & Somerset Hospital
Ms Chrissie Hammonds Midwife Sonographer	Southmead Hospital Bristol
Mrs Cath King Genetic Nurse Specialist	Royal United Hospital Bath
Dr John Madar Consultant Neonatologist	Derriford Hospital Plymouth
Dr Rob Martin Consultant Cardiologist	Royal Hospital for Children Bristol
Mr L Osoba Consultant Obstetrician	Yeovil District Hospital
Ms Alison Phillips Sonographer	Torbay Hospital
Mr Steve Savage Sonographer	Yeovil District Hospital
Dr Consolato Sergi Consultant Paediatric Pathologist	St Michaels Hospital Bristol
Mr Richard Spicer Consultant Paediatric Surgery	Royal Hospital for Children Bristol
Dr Julia Verne Consultant in Public Health	South West Public Health Observatory Bristol

# South West Congenital Anomaly Register (SWCAR)

## *Steering Committee*

### Terms of Reference

The purpose of the SWCAR Steering Group is to support and actively promote the implementation of the Congenital Abnormality Register into hospitals in the South West Region in the first instance. Secondly, to monitor and evaluate the Register once established, give advice on tackling specific issues and to support the project management of this Register.

The SWCAR Steering Committee shall consist of a chair, lead clinician, project manager, clinicians from the relevant specialties, plus additional relevant experts. In the long term it is expected that each hospital in the South West will be represented on this committee. The composition and size of the group shall be considered further at the inaugural meeting.

The Chair of the Steering Committee shall be Professor Peter Fleming, as fund holder. The SWCAR Steering Committee at their inaugural meeting shall decide the job description, process of appointment and term of office for the lead clinician. In addition the Committee shall give authority for the lead clinician and project manager to have overall responsibility for the SWCAR project. This authority will include the power to form *ad hoc* executive groups to manage clinical or specific issues during the development period of this Register, and in the long-term eg annual report, annual meetings, and research projects. The executive steering group shall consist of the lead clinician, project manager and representation from the relevant specialty or expertise. Changes may need to be made from time to time as the register develops, these changes affecting the 'project plan' and 'code of practice' will be agreed through the SWCAR Steering Committee, by a majority vote.

The SW Steering Committee members shall:

- Share the aims and objectives of the SWCAR
- Have commitment to the SW Steering Committee
- Have an acceptance of group values and norms to achieve an effective group
- Have a feeling of mutual trust and dependency
- Participate fully and accept that decision-making shall be by consensus
- Enter into free flow of information and communications
- Exhibit an open expression of feelings and disagreements
- Resolve conflict between another group member, themselves

The overall aim of the SWCAR is to collect good quality data about congenital abnormalities, which can then be used to reach the following objectives:

- ❖ Describe the pattern of congenital abnormalities in the South West Region
- ❖ Disseminate data and information
- ❖ Report the notifications to ONS
- ❖ Provide baseline population data
- ❖ Provide more specific and better healthcare services

The Steering Committee shall meet on a regular basis, the minimum being three times a year, but when specific needs arise meetings shall be convened if it is considered appropriate. The meetings shall take place in or around Taunton, unless the origin of majority of attendees makes this an unsuitable venue. The Executive Steering Group shall meet when and where appropriate.

Dated: 1<sup>st</sup> July 2002