

Chapter:	Three	Section:	Four
Policy No.	03-04-01		
Policy:	Registry Data – Release of Data and/or Information and Result Reporting Policy		
Issued:	January 2002	Revised:	April 2008

General:

Data collected by disease registries is directly related to the health care of the patients. This data collected on a hospital/national level is for research purposes available for researchers/doctors without disclosing patient's identification. Anyone interested in the registry data for research purposes has to submit their research project proposal for approval to the Office of Research Affairs (ORA) of King Faisal Specialist Hospital and Research Center. Once ORA approve the research project, the data can be made available by the registrar to the requestor after necessary documentation.

Statement:

1. Responsibility of Reporting the descriptive statistics based on the yearly collection of data in the form of an Annual Report rests upon the registrar of the relevant registry.
2. Any request for release of information / data for research or other purposes should be processed by the Registrar who is responsible for documenting the request and informing the Registry Committee regarding the release of data from the registry. The data export facility from the web-database software will allow the registrar to furnish the data request. It should be made certain that the whole procedure is in conformity to the RCF Confidentiality Policy. Registrar is also responsible for maintaining the log of all such releases of information.

Policy Objective:

- To safeguard against unauthorized release of registry information.
- To provide a smooth mechanism for the provision of registry data/information to authorized individuals.

Application / Scope:

All registries under RCF.

Monitoring:

Annual

References

RCF IPP # 03-05-01 Confidentiality Policy

Chapter:	Three	Section:	Five
Policy No.	03-05-01		
Policy:	Confidentiality Policy		
Issued:	January 2002	Revised:	April 2008

General:

Since a disease registry requires the review of significant amounts of data there is normally a very thorough review of each patient's medical record. All information obtained on patients shall be considered extremely confidential. The actual medical record is the property of the hospital and is kept to document the course of a patient's care and provide communication between all health care professionals for both current and future care of the patient. The actual information contained within the medical record is the patient's property and cannot be released to anyone without proper authorization from the patient, a subpoena or court order. It is important to stress the strictest confidentiality, as new employees are hired as well as periodic reminders for other employees. RCF members have an obligation to safeguard the confidentiality of personal information maintained in the disease registries. This is governed by ethical and professional codes of conduct. Because of the rapid development of electronic processing of information making sensitive data widely available it is required by the users of sensitive data to ensure they also use common sense when handling data. Different professional and ethical considerations apply depending on the purpose for which the information is used.

Policy Definition:**Confidentiality**

Whilst RCF accepts that great benefits can be made from the information it has collected through disease registries and that medical professionals and hospital management should have ready access to the information they need, it is also important that personal information is kept confidential and that privacy is respected. Disciplinary action may result from a breach of confidentiality, where a breach of contract can be proved.

Principles of Confidentiality

- a. The purpose for which data collected by the registry are to be used should be clearly defined.
- b. All disease registries in the RCF must 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.
- c. Identifiable data may be provided to a clinician for use in the treatment of a particular disease / patient observing that only the data necessary for the stated purpose are released. Access to patient identifiable information should be on a strict need to know basis. Only those individuals who need access to patient identifiable information should have access to it, and they should only have access to the information items that they need to see. Use the minimum necessary patient identifiable information.
- d. The scope of confidentiality extends not only to identifiable data about data subjects and data suppliers, but also to others directly or indirectly identifiable data stored in or provided to the registry.
- e. Data on deceased persons should subject to the same procedures for confidentiality as data on living persons.

- f. Don't use patient identifiable information unless it is absolutely necessary. Patient identifiable items should only be used if there is no alternative.
- g. Everyone should be aware of their responsibilities. Action should be taken to ensure that those handling patient identifiable information, both clinical and non-clinical staff, are aware of their responsibilities and obligations to respect patient confidentiality.
- h. Guidelines for confidentiality apply to all data regardless of storage or transmission media.

Policy Statement:

1. Registrar of each registry is responsible for assuring the confidentiality and security of registry data.
2. The RCF staff should sign, as part of their contract of employment, a declaration that they will not release confidential information to unauthorized persons. The declaration should remain in force after cessation of employment. They are also given a copy of the statement. It is essential that the requirements and responsibilities for people working with all the registries, record and databases maintained by Registries Core Facility (RCF) are clearly defined and understood. This policy outlines the steps that registry database users must adopt. 'Users' are authorized personnel to access any database. The policy also includes those staff members who are charged with the responsibility of creation, maintenance and development of registry databases and relevant software in Biostatistics, Epidemiology and Scientific Computing Department.
3. Suitable control of access to the registry, both physical and electronic, and a list of persons, authorized to enter the registry should be maintained by the Registrar.
4. The Registrar should maintain a list of staff members indicating the nature and extent of their access to registry data.
5. Notices reminding staff of the need to maintain confidentiality should be promptly displayed.
6. Registries at RCF should provide proof of identity to staff engaged in active patient registration.
7. Identifiable data should not be transmitted by any means (post, telephone or electronic) without explicit authority from the Head, RCF or staff member to whom such authority has been delegated. Transmission by telephone should in general be avoided.
8. Registries should consider the use of courier services for confidential data, as well as separating names from other data for transmission.
9. Precautions should be taken for both physical and electronic security of confidential data sent on magnetic, optical or electronic media. This could be done by separating identifying information or via encryption of the identification.
10. Use of computer for confidential data should be controlled for electronic and if possible physical measures to enhance the security of the data, including use of separate room, passwords, different levels of access to data, automatic logging of all attempts to enter the system, and automatic closure of sessions after a period of inactivity.
11. Demonstration of the computer system / database management software should be performed with separate and fictitious or anonymous data sets.
12. Special precautions should be taken for the physical security of electronic backup media.

13. Expert advice on security against unauthorized remote electronic access should be sought if necessary.
14. Measures should be taken to ensure the physical security of confidential records held on paper or any other media and to protect such data from corruption.
15. A policy should be developed for the safe disposal of confidential waste.
16. Security procedures should be reviewed at suitable intervals, and consideration should be given to obtaining specialist advice.
17. Any unauthorized release of patient information will be punishable as stated in "Oath of Confidentiality".

Release of Data

- a. Release of registry data for research and for healthcare planning is central to the utility of a registry. The registry should develop procedures for data release that ensures the maintenance of confidentiality.
- b. The registrar is made responsible to present the request for identifiable data to the Registry Committee and make recommendations to the committee that the particular request meets the requirement of the law and the registry guidelines on confidentiality.
- c. In the absence of written consent from data subjects a registry should not release identifiable data on data subjects for the purpose other than research and statistics. National legislation with respect to confidential data should be observed.
- d. Physicians should be given access to data needed for the management of their patients if identified as such and if in accordance with national / institutional regulations.
- e. Enquiries from the press should be directed to the Chairman of the relevant Registry Committee or to a staff member nominated for this purpose.
- f. Requests for identifiable data to be used for research should include a detailed justification with a commitment to adhere to the registry's guidelines on confidentiality.
- g. Registries should provide a document describing their procedures and criteria for the release of data especially identifiable data to researchers who request access to the data.
- h. If allowed by the institutional and/or national regulations, cross-border transfer of identifiable individual data should only be carried out if required for the conduct of a research project and if the level of protection is satisfactory.

Policy Objective:

- The need for a code of conduct in the maintenance of confidentiality in disease registries and the definition of what should be considered confidential.
- The principles of confidentiality including measures to maintain and survey security procedures.
- Guidelines for the preservation of confidentiality and for the use and release of registry data in accordance with these principles.

Application / Scope:

All registries under RCF