NCDIR POLICY ON DATA PROCESSING AND DISCLOSURE 2017

National Centre for Disease Informatics and Research

Indian Council of Medical Research (ICMR), Bengaluru

CONTENTS

Members involved in drafting and review of the documents

National Centre for Disease Informatics and Research, Bengaluru
Dr.Prashant Mathur *Director*
Dr.A.Nandakumar *Former Scientist G and Director-in-charge*
Dr.R.Sukanya *Scientist-D (Medical)*
Dr.Meesha Chaturvedi *Scientist –C (Medical)*
Ms. Roselind F.S. *Scientist-D (Programmer)*
Ms.Priyanka Das *Scientist-C (Programmer)*

Dr. Visweswara R.N. *Consultant-Pathologist, P.D.Hinduja Sindhi Hospital, Bengaluru*
Prof (Dr.) Shamnad Basheer *Honorary Research Chair, Professor of IP Law, Nirma University* *Visiting Professor of Law, National Law School, Bengaluru*
Dr. Sarasu Esther Thomas *Associate Professor,National Law School of India University (NLSIU), Bengaluru*
Dr. Manjulika Vaz *Lecturer, St. John's Research Institute, Bengaluru*
Dr. Janet Parameshwara *Head, Department of Social Welfare,Kidwai Memorial Institute of Oncology, Bengaluru*
Dr. Sanjay A Pai *Consultant Pathologist and Head of Lab,Columbia Asia Referral Hospital, Bengaluru*
Dr. Elizabeth Vallikad *Professor and Head, Department of Gynaecologic Oncology,* *St.John's MedicalCollege,Bengaluru*
Dr. Vishal Rao U S *In-charge of Head & Neck Services, Dept of Surgical Oncology,* *Healthcare Global Cancer Centre (HCG), Bengaluru* *Member, High Power Committee for Tobacco Control, Government of Karnataka*
Dr. Shashank Garg *Principal Architect, IIMB Digital Innovation Lab, Indian Institute of Management, Bengaluru*
Mr. B. S. Kumar *Director,IT Centre, Bengaluru*

PREAMBLE

The mandate of the National Centre for Disease Informatics and Research (NCDIR) of Indian Council of Medical Research (ICMR), is to sustain and develop a national research data-base on cancer, diabetes, CVD and stroke through recent advances in electronic information technology with a national collaborative network, so as to undertake aetiological, epidemiological, clinical and control research in these areas.

The National Cancer Registry Programme (NCRP) was initiated by the ICMR in 1981 to collect information on cancer cases and is housed under the NCDIR. NCRP provides established datasets from 29 population based registries (till date) for analysis and has scope for expansion. The NCRP produces periodic reports to explain the magnitude of cancer burden and highlight the priority areas of cancer research and control in India.

Registry data collation and compilation is unique as it involves data collection from multiple participating institutions that provide data to the Population based and Hospital based cancer Registries. NCDIR has the responsibility to maintain the trust bestowed by the institutions in the NCRP network to be a custodian of data. The highest ethical standards to safeguard patient confidentiality and privacy, and to maintain data protection and security, are the utmost priority for this Centre, in order to build a national database with international standards.

In view of this responsibility, the Institutional Ethics Committee (IEC) and the Research Area Panel on Cancer of NCDIR recommended having a detailed document on the ethical aspects in handling datasets that includes guidelines on data sharing of cancer registry data. NCDIR has developed the ‘NCDIR policy on data processing and disclosure’ and the ‘Guidelines for sharing of NCRP data-Terms and conditions; Guidelines on data confidentiality and protection; and Guidelines on data security’. Feedback from stakeholders across the NCRP has been taken in preparing the documents.

The IEC has reviewed and approved the documents that will ensure a stable, reliable, ethical and legally compliant framework for data collection, use and dissemination by the NCDIR for the NCRP and for future registries or any long term mechanism for continous data collection on other diseases. The documents are a guide to a framework of data sharing by NCDIR to further scientific research and facilitate resources for training and education. This will strengthen the discussion on ethical aspects of data use and data sharing in India and will be a dynamic document responding to the needs of the future.

1.NCDIR Policy on Data Processing and Disclosure

I. INTRODUCTION

The National Centre for Disease Informatics and Research (NCDIR) was set up by the Indian Council of Medical Research (ICMR) as a permanent institute, to develop and maintain a national research database on cancer, diabetes, CVD and stroke, so as to facilitate aetiological, epidemiological, clinical and control research in these areas. In this regard, it has developed and implements a national level programme of cancer surveillance involving the collection and analysis of reliable data on the magnitude and patterns of cancer.

The purpose of this policy is to ensure a stable, reliable, ethical and legally compliant framework for data collection, use and dissemination by the National Cancer Registry Programme (NCRP) of ICMR-NCDIR, which follows international best practices on cancer registries, as best as possible. Similarly, this document would apply to other disease based registries implemented by ICMR-NCDIR, Bengaluru.

The framework for this policy is broadly based on the guidelines on confidentiality for Cancer Registries, drafted by the IARC,[1] and on the national privacy principles enumerated by the Report of the Group of Experts on Privacy (the Justice Shah Report).[2]

This policy has been formulated, keeping in mind that in the near future, there may be a statutory mandate for hospitals and other sources to supply such data to the ICMR-NCDIR on cancer, cardiovascular diseases (CVD), diabetes, stroke and any other mandated activity.

II. DEFINITIONS

1. 'Chief Data Controller' shall be the Director, ICMR-NCDIR or anyone appointed by him/her.
2. 'Controllers' shall collectively mean the Chief Data Controller and all Data Controllers at the various Registries.
3. 'Data' shall mean any representation of information, knowledge, facts, concepts or instructions relating to a data subject who has been diagnosed with cancer which are being prepared or have been prepared in a formalized manner, and is intended to be processed by the NCRP or any person/body authorized by the NCRP for the purpose of maintaining a Registry.
4. 'Data Controller' shall mean the Principal Investigator (PI) at any of the Registries tasked with supervising the collection of cancer data.

[1] *http://www.iacr.com.fr/images/doc/confidentiality2004.pdf.*

[2] *http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf.*

5. 'Data Subject' means the identifiable natural person whose cancer data is processed by the Registry and ICMR-NCDIR.
6. 'Personal Information' or 'Personal Data' means any information that relates to a natural person, which, either directly or indirectly, in combination with other information, is capable of identifying such person. Personal information shall include all "sensitive personal information" as defined under the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 to mean "physical, physiological and mental health condition; sexual orientation; medical records and history and Biometric information".
7. 'Processing of Data' denotes any and all operations performed upon data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, analysis and reporting, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking and erasure.
8. 'Registry' refers to the Population Based Cancer Registries and the Hospital Based Cancer Registries set up under the National Cancer Registry Programme by the Indian Council of Medical Research.
9. Source of Registration refers to a hospital, clinic, physician, pathology laboratory or any other body which directly collects data from the data subject.
10. 'Third Party' refers to any natural or legal person, public authority, agency or any other body than the Data Subject, the Source of Registration, the Registry, ICMR-NCDIR, the Chief/Data Controller or any person authorized by the Data Controller.

III. DATA COLLECTION

A. AUTHORISATION AND INFORMED CONSENT

1. The Controllers (Chief Data Controller and all Data Controllers) shall ensure, as best as possible, that all institutions and persons involved in the processing of data under this policy are authorised to collect and transfer such data in consonance with the broad framework of this policy.
2. Each Data Controller shall, under the broad supervision of the Chief Data Controller ensure that:
   i) The data subject has provided their informed consent in writing for the processing of data and the usage of such data in accordance with the broad terms of this policy. Informed consent may be taken to mean any freely given, specific and informed indication of the wishes of the data subject by which the data subject signifies his or her agreement to personal data relating to him or her being collected, stored, processed and transferred for the broad purposes of the registry related work of the NCDIR.
   ii) Clause (1) should be followed as far as practicable. However, the requirement of notice and/or consent may be derogated from in the following circumstances:
      a. Where the data has already been collected in the past

b. The data subjects cannot be informed (deceased persons, etc); or
c. Where procuring consent from the data subject entails a disproportionate deployment of resources; or

In the last instance mentioned above (c), the hospital or other site from where data is collected shall ensure, at the very least, that a notice is prominently displayed stating the data from potential data subjects is likely to be collected and processed in furtherance of the ICMR-NCDIR mission and in accordance with this policy.

B. PURPOSE, RELEVANCE AND RETENTION

1. ICMR-NCDIR and/or registries shall only collect information from the data subject which is commensurate to the purpose for which the ICMR-NCDIR registry is maintained.
2. The purposes for which ICMR-NCDIR may collect data include, but not limited to:
   - To generate reliable data on the magnitude, type and patterns of cancer;
   - Undertake epidemiological studies based on results of registry data;
   - Help in designing, planning, monitoring and evaluation of cancer control activities and patient care under the relevant programmes;
   - Develop training programmes in cancer registration and epidemiology;
   - Offer such data to third party researchers who in turn would use such data for the greater public good.
3. ICMR-NCDIR shall retain personal information that is required for the purposes for which the information may lawfully be used.
4. The Controllers shall put in place quality control mechanisms to ensure that the data collected is accurate and reliable.

IV. DATA DISCLOSURE TO THIRD PARTIES

1. Personal data shall not be disclosed to any third party except in accordance with the terms of this policy.
2. In all other cases, the consent of the data subject is to be procured, except where required under any relevant law for the time being in force. Where such disclosure is necessitated by any law/ regulatory / statutory requirement for the time being in force, the data subject shall be immediately notified of the disclosure.
3. Release of aggregate or anonymised data does not breach the duty of confidentiality.
4. Any third party desiring access to data held by ICMR-NCDIR in a format other than is made available through open publications (including those available on its website) shall make a written request to ICMR-NCDIR. Such request shall include all particulars relevant to such request including the following:

   a. The name and full details of the third party applicant

b. Its constitution including any foreign shareholding or participation in its management
c. The nature and format of data required by it
d. The reason for so desiring the data, including details of any project in furtherance of which the data is sought to be acquired, processed and used currently and any further use of such data
e. The intended use of the data including the identity of any partners or collaborators that would have access to such data, once made available to the third party
f. The identity of any organisation who is partnering, collaborating and/or funding the project, in furtherance of which the data is so requested

5. Provided that any such request for sharing of data shall not be granted by ICMR-NCDIR/ 'Chief Data Controller' without the prior permission of the Data Controllers, from whose custody the said data was procured in the first place by ICMR-NCDIR.
6. Every request for data sharing as above shall be carefully scrutinised by the Chief Data Controller who shall, prior to the grant of any permission, consult with and procure clearance from the relevant Research Area Panels, the Scientific Advisory Committee and the Ethics Committee of the ICMR-NCDIR.
7. No primary data shall be available to a third party unless three years have elapsed from the date of publication of the relevant ICMR-NCDIR report.
8. The third party shall ensure the following:

   a. The third party shall use the data strictly in compliance with the terms of this policy, and cannot further share/transfer the data with anyother individual or organization within or outside India.
   b. Prior to submitting the results of any "relevant research" for publication, the said results and the format, methodology and all other particularly surrounding the intended publications shall be made available to the ICMR-NCDIR. ICMR-NCDIR shall carefully evaluate the methodology and the research results to ensure that they comport with the best academic standards. Only after ICMR-NCDIR approval shall this research be released for publication. Provided however that if ICMR-NCDIR does not respond within three months of the request, it shall be presumed that ICMR-NCDIR has given permission.

V. DATA SECURITY

1. Unauthorized access to data shall be prevented. The Controllers shall maintain a list of authorized individuals with access to the registry, both physical and through other means. Access to the data should be provided only to the extent necessary for the fulfillment of a defined purpose or objective.
2. The Controllers shall ensure that the registry and the storage/tranmission of data complies with international best practices and procedures in maintaining data

security, so long as such measures can be implemeted without undue cost or burden to ICMR-NCDIR.

3. The Controllers shall permit the data subject, as and when requested by them, to review the information they had provided and ensure that any personal information found to be inaccurate or deficient shall be corrected or amended as feasible.

VI. BINDING NOTICE AND GRIEVANCE REDRESSAL

1. The Controllers shall be responsible for ensuring that the terms of this policy are complied with by all employees and others working under their supervision, who shall be bound by the said terms (particularly the need to maintain confidentiality of data) even after the termination of their employment/engagement.
2. The Chief Data Controller shall take steps to ensure that this policy shall be made publicly accessible online.
3. The Controllers shall ensure an adequate mechanism for the reporting of grievances by data subjects.

VII. OTHER LAWS/GUIDELINES

To the extent applicable, the Controllers shall ensure compliance with all relevant laws and policies including:

1. Norms relating to data processing, storage and transfer including the Sensitive Personal Data (Reasonable Security Practices) Rules, 2011, under the Information Technology Act.
2. ICMR guidelines pertaining to research on human subjects and collection of consequent information/data.

2. Guidelines for Sharing of NCRP Data – Terms and Conditions

Preamble

With accumulation of data over the years there is a need to have a vision of data sharing with a view to promoting open scientific inquiry. It would also allow others in the field or outside to have a different approach towards analysis and interpretation. Opening up of data to be used by other researchers would also quickly identify co-researchers and help explore topics not envisioned by the initial investigators. However, there are challenges before this process could be streamlined and all stakeholders are taken on board.

Registry data are different from data collated for specific studies. Multiple hospitals, laboratories and other sources are involved in contributing data to a registry. ICMR-NCDIR by itself does not collect individual patient information from any source and coordinates data processing adhering to internationally (WHO) accepted standards for collating, checking, analyzing and reporting cancer registry data. Ethical considerations include patient privacy and confidentiality, and the doctor–patient trust. Other aspects include intellectual property rights and ownership of data sets by registries.

The ICMR - NCDIR is guided by the 'Policy on data processing and disclosure' to ensure a stable, reliable, ethical and legally compliant framework for data collection, use and dissemination by the NCRP-NCDIR, which follows international best practices on cancer registries, as best as possible. The guidelines that allow for data access and disclosure to a third party by ICMR-NCDIR will be guided by the following terms of reference in accordance with the 'ICMR-NCDIR policy on data processing and disclosure'.

General

1. Access to data held by the NCRP shall be allowed "for the purposes of medical/public health research or the administration of cancer related public health programs".
2. ICMR-NCDIR will facilitate access to data for projects that meet appropriate standards of scientific merit or public health importance / interest as determined by the ICMR-NCDIR Research Area Panels, Scientific Advisory Committee (SAC), and Institutional Ethics Committee (IEC), who will approve the same.
3. Any non-research activity/ purpose /commercial interest in relevance only to the mandate of the applicant will not be entertained.
4. Any request for data access and disclosure should be in 'public interest' and for 'public good'. The impact of the research proposal on furthering 'public good or public interest' has to be considered.

5. The guidelines will be applicable to data held by the ICMR-NCDIR in a format other than is made available through open publications (including those available on its website) -
   i) anonymised data ;
   ii) customized aggregated data other than that is publicly available in the NCRP reports; and
   iii) anonymised data access at the ICMR-NCDIR, Bengaluru.

   Anonymised data is that "data from which individual identifiers have been removed and personal identification is not possible through direct identifiers (name, address) and indirect identifiers (identification number, registration number, parents names, source of registration, cultural group)".
   The items of information from the cancer registry data base that would include such anonymised data are: Age Group, Sex, year of diagnosis, ICD, primary and secondary site of tumour (PSTT & SST), morphology of primary and secondary (PHM&MOM), date of death

6. Personal data shall not be disclosed to any third party except in accordance with the terms of the ICMR-NCDIR policy.

Scientific Merit

1. Terms of Reference for considering the Scientific merit of the data request

   Scientific merit will be judged on the following:
   - To have articulated a worthwhile question or hypothesis,
   - To have described a study design appropriate to the question,
   - To have provided a feasible research plan,
   - To have provided calculations of statistical power required to address the question,
   - To have provided an analysis plan,
   - To have provided an information dissemination plan,
   - To have provided a data disposal plan,
   - To have addressed issues of ethics and confidentiality consistent with the ICMR guidelines, in particular the chapter on datasets and bio-banking, and the ICMR-NCDIR policy on data processing and disclosure, and guidelines on data confidentiality, protection, security, storage.
   - To have demonstrated that the researchers have the expertise or access to appropriate supervision required to conduct the research, and
   - To have provided information about funding source(s) along with evidence that sufficient fund will be available to complete the research project.
   - To review if there is need of anonymised data in order to fulfill the uses identified in the research proposal submitted with the data request.

2. The SAC/RAP/IEC will review the scientific merit of each proposal and has the final authority to decide if the research study question can be answered with already available aggregate data published in the NCRP reports and whether there is need of anonymised data.

Justification of Outcome vis-à-vis mandate of NCDIR-NCRP

1. The SAC and IEC will review the competing interests in approving data disclosure for answering similar research questions by one or more organizations given that the NCDIR is collecting data for the purposes mentioned in the ICMR-NCDIR policy.
2. The issue of benefits to ICMR-NCDIR and participating institutions contributing data to the NCRP has to be taken into consideration while review of any data request.
3. If the SAC and/or IEC feel that a discussion with the requesting party is deemed necessary before arriving at a decision, then the concerned person will have to attend and justify the proposal and the request.
4. ICMR-NCDIR is mandated to provide the patterns and burden of cancer of India. No primary data shall be available to a third party unless three years have elapsed from the date of publication of the relevant ICMR-NCDIR report.
5. Prior to submitting the results of any “relevant research” for publication, the said results and the format, methodology and all other particularly surrounding the intended publications shall be made available to ICMR-NCDIR. ICMR-NCDIR shall carefully evaluate the methodology and the research results to ensure that they comport with the best academic standards. Only after ICMR-NCDIR approval shall this research be released for publication. If the ICMR-NCDIR does not respond within three months of the request, it shall be presumed that ICMR-NCDIR has given permission.
6. Decisions on co-authorship for publications/ acknowledgment of source of data etc. should be arrived by mutual consent. Researchers at ICMR-NCDIR and relevant researchers of the registries could be the Co-Principal investigators in the project for which data is being shared.

Terms of reference with Participating Institutions

1. Custodian of data: Cancer registry data collation and compilation is unique and a completely different exercise. The registry data is from multiple hospitals, laboratories etc., and primarily extracted from medical records, pathology reports, radiotherapy charts etc. collected throughout the year for several years. Thus it is not necessarily collected from individual subject/patient or populations which data of most other studies are; ICMR-NCDIR by itself does not collect individual patient information from any source; ICMR-NCDIR or its staff is not the PI or Co-PI of any registry; ICMR-NCDIR is essentially a coordinating centre for all registries. ICMR-NCDIR is a custodian and has only the legal rights and responsibilities of a custodian. Accordingly, the ICMR-NCDIR has no legal right

to transfer the data to a third party without the permission of the Principal Investigator of the respective registry.

2. ICMR-NCDIR and the participating institutions shall ensure, as best as possible, through legally binding instruments that all institutions and persons involved in the processing of data are authorisedto collect and transfer such data in consonance with the broad framework of the ICMR-NCDIR policy.

   A. The major sources of registration of PBCRs should:
      a. Incorporate items listed in the consent form of the patient regarding data extraction (Appendix 1) for the National Cancer Registry Programme
      b. Sign the MOU/T&C (Appendix 2) with the respective PBCR

   B. The institution housing the PBCR should:
      c. Incorporate the items listed into the consent form of the patient registered/diagnosed in their institution;
      d. Sign the MOU/T&C with the major sources of registration feeding the PBCR;
      e. Sign the MOU/TC with NCDIR (Appendix 3);
      f. Have the respective State Government to issue an administrative order incorporating the points mentioned (Appendix 4).
      g. Get clearance from their institution's IEC.

   C. The ICMR-NCDIR should observe the following guidelines:
      h. Ensure that the items listed in A & B above are followed and executed by the respective PBCRs. The process should be facilitated by ICMR-NCDIR.

3. Any request for sharing of data shall not be granted without the prior permission of the Principal Investigators (or Data Controllers as referred to in the ICMR-NCDIR policy), from whose custody the said data was procured in the first place by ICMR-NCDIR. The Principal Investigator should be informed of the credentials and of the third party that is requesting the data.

Terms of reference with third party requesting data

1. 'Third Party' refers to any natural or legal person, public authority, agency or any other body than the Data Subject/patient, the Source of Registration, the Registry, ICMR-NCDIR, the Chief (NCDIR) /Data Controller (PBCR) or any person authorized by the Data Controller.
2. The data request by a third party shall include all particulars relevant to such request including the following:
   a. The name and full details of the third party applicant
   b. Its constitution including any foreign shareholding or participation in its management
   c. The nature and format of data required by it

d. The reason for so desiring the data, including details of any project in furtherance of which the data is sought to be acquired, processed and used.
e. The intended use of the data including the identity of any partners or collaborators that would have access to such data, once made available to the third party
f. The identity of any organisation who is partnering, collaborating and/or funding the project, in furtherance of which the data is so requested.

3. The third party shall use the data strictly in compliance with the terms of this policy, and cannot further share/transfer the data with any other individual or organization within or outside India.

4. To this effect, the third party, who has been granted access to use of NCRP data will sign a Memorandum of Understanding and/or Agreements on Material Transfer with NCDIR-ICMR. These should, according to the requirements of case under consideration, include items pertaining to identification of the collaborating or sending/receiving parties, background, the data to be released /transferred and its quantities (number of years/ registries), purpose of data use, the research to be carried out using the data, moratorium on data access, data confidentiality and data security, reporting, publication rights, intellectual property rights, filling of patents, arrangements for future commercial exploitation, monetary payment for data use, termination of agreement, assignation or transfer of agreement/rights ; audit mechanisms to be observed, qualified user information, materials transfer agreement and any other matter that may be relevant.

All of the above guidelines will apply to registries or any other mechanism of large scale, continous ongoing data collection on any other diseases undertaken by ICMR-NCDIR.

Appendix 1:

Items to be included in consent form of the patient regarding data extraction for the National Cancer Registry Programme

- *I hereby give my consent for clinical information (including identifying, diagnostic and treatment related information) relating to my case to be used for scientific compilation for social/public health purposes.*
- *I understand that my name and initials will not be published and that efforts will be made to conceal my identity, in any scientific analysis / publication, safeguarding my right to privacy.*
- *I believe that no part of my Identifying information will be revealed to any other organization other than the Hospital / Laboratory involved in Public Health Research (Cancer Registration / Control / Stage / Treatment based survival etc.) and the National Cancer Registry Programme(NCRP) coordinated by the National Centre for Disease Informatics (NCDIR) of the Indian Council of Medical Research (ICMR).*
- *I understand that this Institution and the ICMR-NCDIR shall not transfer the data to a third party without the permission of the Ethics Committee of the respective organizations, and further that ethical guidelines in data confidentiality and sharing will be followed, and data protection maintained with adequate security measures.*
- *I understand that the material may be published in a journal, Web site or other form of publication by ICMR-NCDIR as it has the right to publish any scientific information that may be derived from such data,without disclosing my identity.*

-Name of the patient / patient's attendant

-Patient's date of birth / Age:

-Signature of patient / patient's attendant

***Appendix 2*:**

Items to be incorporated in the MOU/Terms and Conditions between the Sources of Registration (SOR) and the respective PBCR

1. *It is understood that the Population based Cancer Registries or PBCRs collect data that is based on goodwill, trust, practice of good scientific ethics and clinical neutrality to generate reliable data on the magnitude and patterns of cancer for the public good.*
2. *It is believed that the patients are well informed of the consent regarding sharing of their data for the abovementioned purpose and the terms relating to its use and their identity is protected.*
3. *In public and national interest for research on cancer, this organization agrees to provide the Anonymised Data (AD), Identifiable Data (ID) and Clinical and treatment related Data (CTD) of all cancer patients registered (diagnosis / treatment) to the PBCR centre, with an understanding that this information would be further forwarded to ICMR – NCRP/NCDIR.*
4. *It is understood that confidentiality guidelines of the data will be maintained at all levels. It is also comprehended that the registries function with an understanding that primary data would not be shared by any individual PBCR / HBCRs with a third party- third party including any party other than registry and ICMR-NCDIR / NCRP. This not only includes patient's identity, but also that of the diagnosing/treating physician and where necessary, that of the hospital.*
5. *ICMR-NCDIR being the only custodian of data, it is deduced that it has no individual right to share the data with any third party except in accordance to the ICMR-NCDIR policy on data processing and disclosure and Guidelines on data sharing, confidentiality and security.*
6. *If a need may arise for betterment in research, on the basis of discussions with ICMR –NCRP / NCDIR, the data may then be shared with a third party for public good and benefit specifying the purpose of data use, and then only the AD will be shared. This will be done after approval by the Ethical Committees at the Hospital/Institution where PBCR is located and that of ICMR-NCDIR.*
7. *The research is allowed with an understanding that the access to the data will be curtailed by the ICMR-NCDIR after the completion of the research study.*
8. *All registries are operating and contributing data based on the understanding that such data is shared only to NCDIR-NCRP and not to a third party.*
9. *It is recognized that ICMR-NCDIR has no legal right to transfer the data to a third party without the approval of the Research Area Panel, Scientific Advisory Committee and the Institutional Ethics Committee, which will ensure that the research application is in compliance with the relevant laws and guidelines.*

10. *It is believed that that the time interval between date of report on data and date on which data would be available for sharing would be a minimum of three years to the date of subsequent report.*

11. *It is strongly believed that protection of patient and physician privacy will be safeguarded by adequate data security measures, and under no circumstances shall the ID or CTD be released to any third party.*

Appendix 3:

Items to be incorporated in the MOU/Terms and Conditions between the respective PBCR and ICMR-NCDIR/NCRP

1. *It is understood that the Population based Cancer Registries or PBCRs collect data that is based on goodwill, trust, practice of good scientific ethics and clinical neutrality to generate reliable data on the magnitude and patterns of cancer for the public good.*
2. *It is believed that the patients are well informed of the consent regarding sharing of their data for the above mentioned purpose and the terms relating to its use and their identity is protected. This will be inclusive for all patients registered / diagnosed / consulted in this centre/hospital, thus covering the Hospital Based Cancer Registry component also.*
3. *In public and national interest for research on cancer, this organization agrees to provide the Anonymised Data (AD), Identifiable Data (ID) and Clinical and treatment related Data (CTD) of all cancer patients registered (diagnosis / treatment) to ICMR–NCRP/NCDIR. The above includes the basic information on broad types of treatment. However, the details of treatment etc. for specific sites of cancer will be provided under separate project heads on Patterns of Care and Survival Studies.*
4. *It is understood that ID will be used only for the purposes of duplicate elimination and data cleaning by NCDIR-NCRP.*
5. *It is understood that confidentiality guidelines of the data will be maintained at all levels. It is also comprehended that the registries function with an understanding that primary data would not be shared by any individual PBCR / HBCRs with a third party- third party includes any party other than registry and NCDIR / NCRP. This not only includes patient's identity, but also that of the diagnosing / treating physician and where necessary, that of the hospital.*
6. *ICMR-NCDIR being the only custodian of data, it is deduced that it has no individual right to share the data with another third party except in accordance to the ICMR-NCDIR policy on data processing and disclosure and Guidelines on data sharing, confidentiality and security.*
7. *If a need may arise for betterment in research, on the basis of discussions with ICMR –NCRP / NCDIR, the data may then be shared with a third party for public good and benefit specifying the purpose of data use, and then only the AD will be shared. This will be done after approval by the Ethical Committees at the Hospital/Institution where PBCR is located and the approval of the Research Area Panel, Scientific Advisory Committee and the Institutional Ethics Committee of ICMR–NCDIR.*

8. *The research is allowed with an understanding that the access to the data will be curtailed by the ICMR-NCDIR after the completion of the research study.*
9. *All registries are operating and contributing data based on the understanding that such data is shared only to NCDIR-NCRP and not to a third party. It is further believed that once ethical guidelines for sharing data are set in place, they will be adhered to.*
10. *It is recognized that ICMR-NCDIR has no legal right to transfer the data to a third party without the approval of the Research Area Panel, Scientific Advisory Committee and the Institutional Ethics Committee, which will ensure that the research application is in compliance with the relevant laws and guidelines.*
11. *It is believed that that the time interval between date of report on data and date on which data would be available for sharing would be a minimum of three years to the date of subsequent report.*
12. *It is strongly believed that protection of patient and physician privacy will be safeguarded by adequate data security measures, and under no circumstances shall the ID or CTD be released to any third party.*

Appendix 4:

The items listed below are to be incorporated in the Administrative order issued by the respective State Governments

1. *In keeping the importance of cancer registration for public good in terms of understanding magnitude and patterns of cancer, the State Government acknowledges the lead taken by ICMR -NCDIR(NCRP)towards this.*
2. *Accordingly, this order is issued for compliance by all medical institutions - government and private hospitals, nursing homes, clinics, pathology laboratories, hospices or any facility diagnosing/treating or attending to cancer patients.*
3. *In public and national interest for research on cancer, the institutions listed above should provide or facilitate to provide (in the standardized specified format) the Anonymised Data (AD), Identifiable Data (ID) and Clinical and treatment related Data (CTD) of all cancer patients registered (diagnosis / treatment) to the PBCR centre (where the PBCR is housed) who in turn would provide the same to ICMR – NCDIR (NCRP) as above.*
4. *It is understood that confidentiality guidelines of the data will be maintained at all levels. This not only includes patient's identity, but also that of the diagnosing/treating physician and where necessary that of the hospital.*
5. *No part of the three components (viz., patient, physician, hospital) of ID would be revealed to any other organization other than that listed above.*
6. *If a need (in the form of research proposals) arises based on discussions with ICMR –NCDIR (NCRP), then the data may have to be shared with a third party for public good – benefit / research, then, only the AD will be shared. This will be done after approval by the Ethical Committees of the Hospital / Institution that houses the PBCR and that of ICMR –NCDIR.*
7. *Under no circumstances will the ID and / or CTD be shared, with any third party.*
8. *Protection of patient / physician privacy will be safeguarded / maintained by adequate data security measures*
9. *Ethical guidelines in handling data will be followed as specified by ICMR –NCDIR.*
10. *The State Government or its authorized parties shall have the right to access the entire dataset on cancer for public good use / policy / planning / program purposes.*

3. Guidelines on Data Confidentiality and Protection

1. Confidentiality Issues in Cancer Registration and other activities.

   Confidentiality could be that of patient, physician and hospital/pathology laboratory or any other medical institution. The material - patient data could be in paper (hand written and / or print outs) or electronic format. It could be in the desktop computer, local or external – web server and on the net during transmission.

   The patient details comprise identifying information or anonymised data, diagnostic and / or treatment / survival parameters. In all permutations and combinations of the above individuals involved in collating, abstracting and handling the different formats and types of data have to follow strict guidelines and procedures so as not breach confidentiality. Such guidelines are well documented in the article published by the European Network of Cancer Registries and the International Agency for Research on Cancer given in Appendix 5. The NCDIR-NCRP along with the institutions under this network may by and large adopt these guidelines.

2. The staff of the ICMR-NCDIR and that of all collaborating registries/institutions shall have to individually sign an undertaking the format of which is given in Appendix 6(A) and Appendix 6(B). The undertaking will be to protect both confidential information in all its formats and types listed above as well as data protection issues outlined below.

3. General physical arrangements by institutions (ICMR-NCDIR and others):
   a. The physical premises must be secured from fire and other natural disasters. Appropriate plans for combating such emergency responses should be part of the institution's policy.
   b. Physical access to data stored in a registry must be secured. Documents need to be stored in areas specifically designated for this purpose with appropriate locking facility. Access to the data files /documents is limited to authorized Registry personnel.
   c. The arrangements for security and confidentiality within each hospital must be strictly observed. Medical records should not be taken from areas assigned to them without the specific permission of a responsible hospital authority.
   d. Only authorized persons (data entry operator / social worker / statistician / software development staff / doctor / scientist) identified in each respective Institution can access the data entry portal for entry, edit, save, delete, quality control check functions, etc.
   e. Data gathered/received from other sources in physical – paper must be kept in secure storage until used and then appropriately disposed so that information there-in cannot be retrieved.

Appendix: 5

Guidelines on Confidentiality and ethics for population-based cancer registration and linkedactivities in Europe by European Network of Cancer Registries and International Agency for Research on Cancer

http://www.eurocourse.org/mm_files/do_944/D2.2.pdf

Appendix 6(A):

Staff Undertaking at ICMR-NCDIR

I, ..., employee of ICMR-NCDIR/....., engaged as Medical / Statistics / Computer Science Scientist, Programmer / Technical Officer Technical Assistant / Data entry Operator

undertake to protect the confidentiality of all personal and medical information held by the National Cancer Registry Programme (NCRP) of ICMR or brought to my attention in my line of work of the NCRP in my employment in ICMR-NCDIR.

I undertake that I will not disclose any such information (personal or medical items) to any person who is not directly involved with the NCRP and ICMR-NCDIR, or to any unauthorized person or institution, except as permitted by the guidelines of data handling of the ICMR-NCDIR.

I also undertake that I have read and will follow the 'Guidelines on Data Confidentiality and, Protection and Guidelines on Data Security' to maintain confidentiality of patient information and registry data, and to maintain measures of data security and protection.

I also undertake that I have to maintain the above even after leaving the current employment with ICMR-NCDIR.
I understand that any breach of this undertaking could result in a disciplinary action by the Institution.

Signature:.....

Date:..... *Place:.....*

Appendix 6(B):

Staff Undertaking –Registry

I, ..., employee of ..... (Institution name) /....., engaged as Principal Investigator/Co- Principal Investigator/ Senior Scientist/Statistician/Medical Social Worker/Data Entry Operator/.....,

undertake to protect the confidentiality of all personal and medical information held by the National Cancer Registry Programme (NCRP) of ICMR or brought to my attention in my line of work with the NCRP in my employment in.....(Institution name).

I undertake that I will not disclose any such information (personal or medical items) to any person who is not directly involved with the NCRP and ICMR-NCDIR, or to any unauthorized person or institution, except as permitted by the guidelines of data handling of the ICMR-NCDIR.

I also undertake that I have read and will follow the 'Guidelines on Data Confidentiality and Protection, and Guidelines on Data Security' to maintain confidentiality of patient information and registry data, and to maintain measures of data security and protection.

I also undertake that I have to maintain the above even after leaving the current employment with ……..... (Institution Name).

I understand that any breach of this undertaking could result in a disciplinary action by the Institution.

Signature:.....

Date:..... *Place:.....*

4. Guidelines for data security at ICMR-NCDIR

The guidelines on data security are based on the Information data security policies existent in India.

Basic principles

1. Al employees of ICMR-NCDIR who are involved in the collection, processing, analyses and outputs of the National Cancer Registry Programme have to maintain confidentiality of the data and maintain measures to ensure data security and protection.
2. To this effect, the concerned staff have to read, agree and sign an undertaking to observe rules necessary to maintain confidentiality and security of data of the NCDIR-NCRP.
3. This undertaking will be renewed annually, or as and when required by the Head of the Institution (NCDIR/PBCR/HBCR).
4. This undertaking protects patient data (identifiable and non–identifiable) from disclosure to any third party through any means directly and indirectly.

1. Identifying Assets

1. Inventory of the servers, desktops, laptops, printers, etc. is maintained.
2. Licenses of system and application software, antivirus are well maintained.
3. In-house developed software modules are identified and maintained in centralised server.
4. Databases containing HBCRs, PBCRs, Cancer Atlas, POCSS and other independent modules are identified and maintained.

2. Access Control

a. Local Network

i. Servers (Domain, Application and data) is protected by secure passwords and only authorised employees are allowed access.
ii. Only System Administrator is allowed to access all the system to perform installation of software from removable media or from the internet thus restricting the use of third party software which may compromise data security.
iii. Each employee is assigned with a unique user id and password to access their desktop and NCDIR LAN.
iv. Database and applications that contain sensitive information be accessible to authorized employees with valid credentials only.
v. Only the shared drive of each system is visible to the other users in the network.
vi. Databases are accessible to authorised users having valid credentials.

vii. The software codes are stored in licensed Configuration Management software, password protected and onlyprogrammers have access to the source codes relevant to their projects.
viii. Databases / documents containing identifying information are being accessed by only analysts/researchers who need complete information to process the data. Each team member requiring complete access under each project is identified to create an access control list.
ix. Records containing personal (identifying) and medical information of registered cases available in several formats (SQL Server DB/ MS Excel/ MS Word / CSV files / any other) are stored in allocated network folders and are password protected. Only authorized staff of ICMR-NCDIR processing the data is given access to the same.

b. Web Server

i. Web databases can be accessed only by NCDIR's IP address.
ii. Databases are accessed by authorised users having valid credentials only.
iii. The control panel to access the web server to upload/download pages, create databases, backup data be available to identified programmers entrusted to do this work.

3. Data security measure for online transmission and storage

1. Hosting of the web server in an ISO 27001 certified data centre in India
2. SSL certification for all the NCDIR domains.
3. The sensitive data residing online (web server) is stored in encrypted format following standard encryption algorithm.
4. Loaded with antivirus and updated with the latest virus definitions.
5. Automatically provide backup of database and web pages.
6. Control panel rights to ICMR-NCDIR for uploading and downloading of data, web pages and maintenance.
7. Disaster Recovery Plan to mitigate any human induced/ natural disaster.

4. Physical Security

1. The server room can be accessed by authorized employees.
2. The servers are password protected.
3. CCTV surveillance is implemented to keep track of intrusions in server room and different locations of the office premises.

5. Back-up

1. When there is a major update in the data, back up of the database is taken and stored in a designated folder in the server.
2. Back up of the SQL database in the Web Server is done once a month.

3. Regular backup of all software codes, databases and documents (MS Excel/ MS Word/ CSV files/ any other) is taken monthly in external hard disk drive.
4. Back up of data will be kept in a external hard disk drive.

6. Personnel

On termination and change of employment, revoking of access privileges, such as User-IDs and passwords, to system, data resources and server room is done. All hardware, software, data, access control items, and documentation issued to or otherwise in the possession of the data user being relieved is retrieved.

7. Keep software up to date

System and application software, antivirus software are upgraded with latest versions as per the requirement.

8. Encryption

The identifying data rsesiding online (web server) is stored in encrypted format.

9. Real Time Monitoring

1. Firewall is in place to protect unauthorised access, blocking irrelevant websites, monitoring internet traffic and block of spams in emails.
2. Log in activities of the centres are monitored and working hours are recorded.
3. Audit trail is maintained whenever there is an updation or deletion of data/records.
4. An official internet connection is used by all terminals to access internet.

10. Remove Data Securely

Before condemnation, the hard disks are formatted and information is wiped out and verified.

11. Disposal of confidential waste – Some measures include:

1. Paper records will be shredded
2. Electronic records, storage devices are formatted and information wiped out
3. DVDs/CDs be cut up and disposed as per paper waste
4. The confidential waste bags will be kept secure and separate from any other waste whilst waiting to be disposed.

Guidelines for data security at registry sites

1. Local Server/ Desktop – backups of SQL Server database and documents (SQL Server DB/ MS Excel/ MS Word/ CSV files/ any other) has to be taken every month.
2. Licensed versions of operating system and application software, antivirus software have to be used and updated regularly.
3. The passwords to the SQL Server (for offline software) and NCDIR software being used for capturing data is not shared with any unauthorized personnel.
4. All folders in the network shared drives where identifying information on patient's data is available (SQL Server DB/ MS Excel/ MS Word/ CSV files/ any other) should be password protected.
5. Only team members involved in processing of the data is given access to the folders and files with identifying information.
6. When an employee ceases to be associated with the registry work, ICMR-NCDIR is to be intimated so that old credentials are disabled and fresh credentials for data entry would be provided.
7. Disposal of confidential waste – Some measures include:
   i. Paper records will be shredded
   ii. Electronic records, storage devices are formatted and information wiped out
   iii. DVDs/CDs be cut up and disposed as per paper waste