



## **Confidentiality Policy and Plan**

CIMRO has developed the following policies, procedures and processes that meet the confidentiality and disclosure requirements set forth in Section 1160 of the Social Security Act and implementing regulations at 42 CFR 476 and 42 CFR 480; the Alcohol, Drug Abuse and Mental Health Administration (ADAMHA) Reorganization Act (42 USC 290dd-2); as well as State-specific and/or any other applicable regulations, including, without limitation, the Final HIPAA Privacy and Security Rules.

Two areas of major concern must be considered in reference to confidentiality of medical information. These are the security of the data and the responsibility of personnel to hold sensitive information in confidence and be accountable for any breach of that responsibility.

### **Designation of Responsible Individual**

The CIMRO Board of Directors has designated the Chief Executive Officer of CIMRO to oversee and be ultimately responsible for strict adherence to this Confidentiality Policy.

### **Responsibilities of CIMRO Employees and Consultants, Independent Contractors, Vendors and Service Providers**

CIMRO instructs all new employees and consultants of their responsibility to maintain confidentiality of information and of legal penalties for unauthorized disclosure. All employees and consultants are required to sign a *Statement of Confidentiality Employee Certification and Acceptance* form, indicating that he/she accepts responsibility to hold confidential data and information in strict confidence and is aware of CIMRO's dismissal policy, as well as the legal liabilities and penalties for unauthorized disclosure of data and information. This form is maintained in each employee and consultant file. In addition, all CIMRO staff and consultants receive an annual *CIMRO Confidentiality Requirements Reminder* statement.

Similarly, all other Independent Contractors, Vendors and Service Providers that have access to confidential medical information or confidential proprietary information of CIMRO are required to abide by the Confidentiality Policy and to execute an appropriate Certificate and Acceptance form regarding the same.

### **Destroying of Confidential Medical Information**

Medical information which is maintained in any form and is identifiable as to individual patients, physicians and/or providers will be destroyed, if feasible, consistent with legal record retention or contractual requirements, by authorized CIMRO staff when the information has served the specific purpose for which it was generated.

## **Notification and Specific Access**

Any individual patient who is the subject of data in the system will be allowed access to pertinent file data in order to ascertain the accuracy of that data. Requests for access must be made in writing to CIMRO and receive written approval of the CIMRO Board or its authorized designee.

CIMRO will notify the physician of record in writing at least fifteen (15) days prior to allowing an individual to access the file. The physician or his/her designee may be present at the review and clarify contents of the record. All involved parties must sign statements agreeing that no information will be removed from the CIMRO offices. Coded data will be interpreted by CIMRO staff to facilitate the review. If existing data is demonstrably incorrect, CIMRO will permit such data to be corrected or amended. Should an unresolved disagreement occur regarding the accuracy of the data, CIMRO will, upon written request, provide for submission of the contested data to arbitration. Any costs of arbitration shall be borne by the requesting party.

## **Dissemination and Disclosure of Confidential Data**

All QIO Medicare, Medicaid, and private review data and information is strictly confidential and may not be disseminated except in accordance with the provisions hereof and applicable laws and regulations.

The following are also strictly confidential and may not be disseminated without the prior written consent of CIMRO:

- CIMRO's proprietary information, methodology and technology
- CIMRO's know-how and trade secrets and/or derivatives, including but not limited to those relating to computer programs and technologies developed, enhanced or improved by CIMRO
- CIMRO's review processes and methodology used in performing its services. However, general terms regarding the nature and extent of these may be disclosed for the sole purpose of reasonably apprising the medical community of the nature of the review process and its potential applications to any provider of medical care or services.

Any development, enhancements or improvements to any of the above shall be conclusively deemed to be work done for hire and for all purposes be deemed to be the exclusive property of CIMRO.

Data obtained from any contracts will not be released, disclosed or published except in de-identified form. Any comparative data, including utilization data, will be released in de-identified aggregate form only. Any non-confidential, de-identified data which results from an activity funded by CIMRO must be approved by CIMRO in writing prior to publication. Except as provided herein, no patient or physician identified data will be released to anyone other than the responsible government agency, company, insurer or re-insurer with a contractual right and need to know for purposes of their adjudication of a claim for reimbursement, or serious quality problems and/or substantial quality patterns of care and related quality improvement activities or for their approval of recommended case management by CIMRO unless ordered by a court of competent jurisdiction. Identified data may be released pursuant to notification described under "Notification and Specific Access".

## **Data Subcontractors**

Any data subcontractor which stores, maintains or processes confidential data collected for utilization or quality review, peer review and evaluation purposes must agree to abide by CIMRO's confidentiality policies and procedures. Data subcontracts must minimally assure that:

- the computer data bank limits the output of any confidential information to those persons duly authorized by CIMRO
- individually identifiable data will not be transferred to another system or corporation without specifying requirements for security of the data, including limitations of access
- the conditions of the transfer will provide the required security

In addition, express written approval must be obtained from the CIMRO Board of Directors or its designee prior to the release of any such information. Once the data is no longer required for purposes of review, appeals, program monitoring and/or evaluation, CIMRO will direct, and the data subcontractor will perform, the purge of personal identifiers from the data files.

## **Legal Requests for Information**

In the event of the issuance of a subpoena or other discovery demand for any confidential information, or for a representative of CIMRO to testify concerning any patient, practitioner, physician reviewer, or institution, the court's attention will be called, through proper channels, to all applicable legislated and Department of Health and Human Services (DHHS) regulated QIO confidentiality provisions against disclosure of information or other applicable disclosure limitations.

## **Adherence to Contractual or Regulatory or Statutory Confidentiality Requirements**

The CIMRO Board, CIMRO committees and staff are additionally obligated to strictly adhere to any additional confidentiality requirements applicable by virtue of contract, regulations or laws that may, from time to time, be applicable.

## **DATA SECURITY PROCEDURES**

### **A. Overview**

The CIMRO Confidentiality Policy and related procedures are applicable to the data management process. These procedures deal with both the release or disclosure of confidential information and the physical security of this information.

The following confidentiality procedures related to CIMRO employees and physician consultants deal primarily with the physical security of data. However, all employees and physician consultants are informed that provisions of the CIMRO Confidentiality Policy which deal with the release of confidential information are also fully applicable.

For the purpose of this procedure manual, confidential materials are defined to include:

1. Patient medical records and all related review worksheet documentation, provider and physician responses.
2. Computer reports which are physician and/or patient specific.
3. Related working materials, drafts and copies of all the above which contain identifying information.
4. Physician license numbers, Medicare/Medicaid provider numbers.
5. CIMRO data access codes.

The major areas of concern with regard to these materials involve their:

1. Storage/use.
2. Transportation.
3. Release or disclosure.
4. Destruction.

### **B. Procedures**

#### 1. Storage/Use of Confidential Materials

##### a. CIMRO Facilities

- 1) Confidential materials will be stored in a secure area when not in use. Keys to the storage room and locked files will be kept by the Senior Vice President or designee in a separate locked file.
- 2) The storage area is only accessible when under the direct supervision of designated staff. Access to the storage area by other staff or members of the Board of Directors will be only with the prior knowledge and approval of the Senior Vice President or the Chief Executive Officer.
- 3) Access to the storage area by individuals other than staff or members of the Board of Directors will only be with the prior knowledge and approval of the Senior Vice President or Chief Executive Officer and any such visit will be accompanied by the Senior Vice President or the Chief Executive Officer.
- 4) In general, other work involving confidential materials - such as the preparation or use of profile reports - will be performed within the CIMRO corporate office. Materials related to any such work will be removed from the

corporate office only with the prior knowledge of the Chief Executive Officer as to the materials concerned, purpose and involved staff.

b. Hospitals or Other Facilities

- 1) In all hospitals or other facilities where CIMRO performs review or other functions, the same principles of security will be observed. Confidential material will, when not in use, be stored in a separate area to which CIMRO and appropriate hospital/facility personnel have sole access.
- 2) All confidential materials will be secured by hospital/facility personnel when not under the direct supervision of CIMRO personnel.
- 3) Under no circumstances will confidential materials be left unsupervised by CIMRO personnel in the hospital/facility.
- 4) Routine work utilizing confidential materials will only be performed in the hospital or other facilities.

c. The CIMRO Technology System

- 1) Only authorized CIMRO personnel will have access to the technology system.
- 2) The access codes assigned to each person will be restricted to various levels of system access so that overall system access will be controlled. An electronic copy of these codes is maintained in the system and is accessible only by the Chief Financial Officer and Manager, Information Technology.
- 3) On an annual basis or more frequently, if appropriate, these accessing codes will be changed. In the event of an employee termination, the CFO/Manager, IT are immediately notified and the terminated employee's access to the system is restricted.
- 4) The accessing code will be entered in a manner which conceals the code on subsequent printed reports.

2. Transportation of Confidential Materials

- a. Routine transportation of confidential materials between CIMRO and contractors may be accomplished by First Class mail, United Parcel Service, or similar commercial carrier. Confidential materials will be transported to and from CIMRO staff and physician consultants using United Parcel Service or similar commercial carrier call tag system. The confidentiality of all medical records and related information must be safeguarded at all times. Due care must be exercised in assuring the integrity of the packaging materials utilized, as well as appropriate, legible addressing to provide safe delivery.
- b. On a special basis, confidential material may be hand delivered. However, this will only be with the knowledge of the Senior Vice President. It will involve the direct delivery of materials involved and will occur during the normal working day. Confidential materials which are hand delivered must be under the direct supervision of CIMRO staff at all times while in transit.

- c. Only duly authorized personnel having a signed Certification & Acceptance document may prepare for shipment or receive confidential materials. Duly authorized recipients of confidential material accept responsibility of personal receipt or must have instructed other individuals receiving such materials to place these materials unopened, in a safe place for later inspection by the authorized recipient.
  - d. Knowledge of the whereabouts of all confidential materials will be maintained by either a computerized program of logging materials in and out or by manual logs. Time frames for return of confidential materials are likewise maintained and appropriate follow-up initiated when unexplained delays in return occur.
3. Release/Disclosure
- a. Release or disclosure of any confidential materials is prohibited by the CIMRO Confidentiality Policy except as herein provided.
  - b. Release of physician identifier codes to any party, including the concerned physician, will only be done with the knowledge and approval of the CIMRO Board of Directors or designee.
  - c. This policy applies primarily to the release of material to individuals other than CIMRO employees or members of the CIMRO Board of Directors. However, it also prohibits the release of confidential materials to other staff or members of the Board of Directors who are not directly involved in the use of these materials and/or who do not have a "need to know".
4. Destruction or Return of Confidential Materials
- a. Destruction of any confidential materials will be at the discretion of the Chief Executive Officer, Senior Vice President or designated personnel and pursuant to the provisions of the CIMRO Confidentiality Policy.
  - b. Once designated for destruction, confidential materials will be immediately shredded by the designated personnel or bonded shredder service.
  - c. Return of medical records to the hospital or other health care facility instead of destruction will be in accordance with the specific provider's request.
  - d. Deletion and storage of electronic confidential information will only be accomplished under the supervision of the CFO or designated IT personnel. Once confidential data is removed from the CIMRO server, it is only accessible from tapes, which are stored in a locked room in the media server, or in a secure offsite storage (i.e., bank vault). Tapes containing PHI are marked "Confidential - PHI - this tape must be safeguarded from unauthorized use." Only the CFO and designated IT personnel have access to the tapes and server, and destruction will be in accordance with applicable federal (including but not limited to HIPAA) and state regulations, as well as contract requirements.