100.03.04B RELEASE OF PROGRAM INFORMATION

No Medicaid data regarding recipients, providers or services may be released without prior approval of the Executive Director, unless an established exception applies. The following program information constitutes the only established exceptions which do not require prior approval of the Executive Director:

- The annual report of the Division of Medicaid, published pursuant to state law, containing the total number of recipients, the total amount paid for medical assistance and care; the total number of applications, the total number of applications approved and denied, and similar data.
- Pamphlets, brochures and other documents prepared for distribution to the public.
- Information exchanged with other state or federal agencies pursuant to a contract or written agreement.

If requests for information are received, including requests for large quantities of pamphlets, brochures and other public information, the regional office should forward them to the Bureau of Enrollment for further action. Requests will be considered pursuant to the Access to Public Records Act, as applicable.

100.03.04C SAFEGUARDING CONFIDENTIAL INFORMATION

The privacy rule protects electronic records, paper records and oral communication. Therefore, employees of the agency are responsible for safeguarding the confidentiality of recipient information in all forms to prevent unauthorized disclosure. In practical terms, this includes:

- Following password and other security procedures for systems;
- Securing cases in filing cabinets rather than leaving them in open view when not in use; and
- Discussing cases or recipients only as necessary for legitimate job-related purposes and in confidential office settings.

SAFEGUARDING CONFIDENTIAL INFORMATION (Continued)

Failure to abide by the policies and procedures regarding confidentiality of recipient and applicant information, either intentionally or unintentionally can result in disciplinary action. Group offenses are discussed in the DOM Employee Manual under Discipline and Grievance Policies. In addition, any violation of privacy and security policies and procedures may be referred to state or federal agencies for prosecution.

100.03.04D SAFEGUARD AWARENESS TRAINING

Training on the security standards for data provided by the Internal Revenue Service (IRS) and Social Security Administration (SSA) must be conducted annually for eligibility staff in each regional office. During the training employees are instructed in office security procedures to ensure security of the data and are issued a copy of the federal penalties for unauthorized disclosure of IRS and SSA information.

A confidentiality statement for each type of data is signed by employees. The person providing the training signs and dates the confidentiality statements to certify security training for each agency's data. The signed and certified statements are forwarded to state office, where they are maintained to document compliance with IRS and SSA safeguard training requirements.