

# Georgia Department of Human Resources Division of Aging Services

## Section 90 State Agency Operations, Guidelines and Procedures

### §96 Technology and Data Management

June 2004

#### §96.1 Purpose

This chapter establishes policies and guidelines for implementing and managing technology systems and data management activities at the Division of Aging Services, Area Agency on Aging and provider organization levels of the statewide aging network. The fundamental purpose of the policies and guidelines is to protect the State's stored information about consumers who are receive services through the aging network's programs.

#### §96.2 Background and Scope

The Department of Human Resources Division of Aging Services operates in a data-driven environment, which will become only more extensive, pervasive and complex in the future. The Division is responsible for creating, managing, supporting and maintaining a statewide centralized database, the Aging Information Management System (AIMS). AIMS is the mechanism used to track, account for and report service delivery and financial data. Area Agencies on Aging use the AIMS to create individual client records; enter individual client assessment data; create area plans; establish administrative and service budgets; comply with Federal and State reporting requirements; generate reports used for program management; obtain reimbursement for services rendered; and evaluate and improve the quality of the service delivery system. The AIMS is designed and intended to be implemented and used at both the Area Agency and service provider organization levels. Service providers are authorized to establish client records, establish service delivery logs, enter service data and generate reports related to their clients, sites and services. Technical information regarding how to use the system is provided in the AIMS Manual, which may be accessed at [http://www.aims.dhr.state.ga.us/aimsbook/HCBS%20Web%20Service%20Log%20Manual Revised 2 24 04.pdf](http://www.aims.dhr.state.ga.us/aimsbook/HCBS%20Web%20Service%20Log%20Manual%20Revised%202%2024%2004.pdf)

These policies and guidelines, and related authorities, apply to the Division of Aging Services; allied federal and state agencies; contractors, Regional Development Centers and/or Area Agencies on Aging; and subcontractor agencies and vendors, including private non-profit organizations, proprietary organizations, and city and county governments.

### §96.3 Authorities

Code of Federal Regulations, Title 45, part 1321, *Grants to State and Community Programs on Aging, Subpart B, State Agency Responsibilities, §51, Confidentiality and Disclosure of Information*

42 U.S.C. 1301 et seq., Public Law 104-191, Health Insurance Portability And Accountability Act of 1996

Code of Federal Regulations, Title 45, part 160, *General Administrative Requirements*, and part 164, *Security and Privacy( HIPAA)*

The Georgia Computer Systems Protection Act (OCGA § 16-9-90 et seq.)

### §96.4 Definitions

For purposes of these policies and guidelines the following definitions are provided:

- (a) Access: To instruct, communicate with, cause input to or output from, cause data processing or otherwise make use of any resources of a computer, information system, or information network.
- (b) Authorized User: One who has been verified as having valid rights to and who has been granted rights of access to an information technology system based on that person's responsibilities within an organization and his/her need for access to the system.
- (c) Computer: An internally programmed automated device that performs data processing or telephone switching.
- (d) Computer system: At least one computer together with a set of related, connected or unconnected peripheral devices.<sup>1</sup>
- (e) Electronic document: A structured data file, most commonly created in a word processing or spreadsheet application, but possibly in other personal computer applications, such as desktop publishing or presentation software, and the like. An electronic document remains a document only until it is transmitted electronically or physically to another person or persons or store of information.
- (f) Electronic record: A document or other type file that is transmitted or submitted electronically or physically.

---

<sup>1</sup> Peripheral devices are electronic equipment connected by cable to the Central Processing Unit (CPU) of a computer; for example disk drives, printers, external fax machines.

- (g) System: An assembly of components (hardware, software, procedures, human functions, and other resources) connected by some form of regulated interaction to form an organized whole. A group of related processes.

**§96.5 Objectives.**

The objectives of these policies and guidelines are:

- (a) to assure that all entities that are part of the regional and statewide aging services network have appropriate and adequate access to both the data entry and reporting functions of AIMS, based on their organizational capabilities, expressed in terms of budget, staffing and technical capacities;
- (b) to establish the authority given by the Division to the Area Agency on Aging to grant to their staff and provider agencies appropriate access to AIMS with necessary security protections;
- (c) to assure that the documentation related to reporting client or other programmatic activity through electronic or other means to the Department is maintained accurately, completely and in a timely fashion;
- (d) to assure that data collected, stored and reported in and by the state system are managed in a secure fashion which protects the privacy and confidentiality of applicants and consumers;
- (e) to provide credible, timely data which are used to support management decision-making and program administration;
- (f) to provide general guidelines for disposal of electronic documents related to program administration and other purposes, maintained outside the AIMS.

**§96.6 General Policy Statements**

- (a) It is the intent of the Division of Aging Services that Area Agencies assess the staffing and technological capacity of the service provider network, provide technical assistance and training to providers, and deploy AIMS to providers who demonstrate the capacity to perform adequately the essential data management functions, including but not limited to data entry, data validation, and report generation.

- (b) The State's information is to be handled in such a manner to protect it from unauthorized or accidental disclosure, inappropriate modification or loss. The integrity of the State's information resources must be protected.
- (c) The State, in processing confidential information, must have adequate controls over users' access to the AIMS.
- (d) Confidentiality is determined in accordance with federal laws, rules and regulations and any applicable state laws, rules and regulations. (See §96.4, "Authorities")

### §96.7 Data Management

Activities associated with data management include:

- (a) data verification and validation, in general;
- (b) entry of required participant and/or activity data into AIMS;
- (c) monthly service delivery reporting into AIMS;
- (d) generation, analysis and timely<sup>2</sup> submission of programmatic and fiscal reports, and reports yielding data about client and service characteristics;
- (e) maintenance of resource databases or other directories;
- (f) retention of, safeguarding, and appropriate disposal of the records of participants, including information generated at intake, screening and at the assessment and service delivery levels.

### §96.8 Conventional Participant Records

Regarding conventional, non-electronic forms of participant records --

- (a) Area Agencies/providers (as applicable) shall establish, organize and maintain for each participant a record that is protected from damage, theft, and unauthorized inspection, and made available for monitoring and audit purposes. At a minimum, records shall contain the following information<sup>3</sup>:

---

<sup>2</sup> Report submission cycles vary from monthly to quarterly to annually. Other reports may be produced on an *ad hoc* basis in response to special inquiries or for research and evaluation purposes. Please note that some reporting, data analysis and management activities are conducted independently of the AIMS.

<sup>3</sup> Refer to DAS HCBS Manual Chapter 114, "Guidelines for Client Assessment," for information on the core assessment instruments, the DON-R and NSI-D Checklist. Copies of these instruments, as required for individual services, will be retained in conventional files to document each initial screening, assessment and successive reassessments.

- (1) intake and screening information, collected/documented at the AAA and transmitted to a case manager/provider either associated with the AAA or with a subcontract agency;
  - (2) documentation of initial eligibility status, ongoing eligibility status and assessment and reassessment findings;
  - (3) contact information and procedures for emergency care; and
  - (4) any other information, such as service/care plans, service schedules, notes on client contacts, supervisory notes, etc. as may be required by an individual service or program, according to the DAS Manual for Non-Medicaid Home and Community Based Services.
- (b) AAAs/providers shall develop and implement written procedures to be followed for obtaining the written consent of the participant for release of confidential information to other service providers when referrals are made.

#### **§96.9 Electronic Participant Records**

Area Agencies/providers may establish electronic participant records *in lieu of* conventional files.

- (a) Area Agencies electing to implement electronic participant file systems shall establish and implement protocols which provide for shared access to client records in AIMS on a need-to-know basis among their staff, staff of case management agencies, and provider agencies, as applicable in their planning and service areas.
- (b) The state and federal government and the Department/Division shall have full and complete access to all consumer/ customer/client records, administrative records, financial records, pertinent books, documents, papers, correspondence, including e-mails, management reports, memoranda, and any other records of the Area Agency and subcontractors for the purpose of conducting or reviewing audit examinations, excerpts, and transcripts.
- (c) Area Agencies will establish protocols for monitoring electronic files, including providing required access, with or without notice, to such files by authorized DAS staff, staff of any state or federal funding agency, auditors, and/or staff of the Office of Inspector General.

**§96.10 Security and Access Management**

It is the policy of the Division of Aging Services that Area Agencies on Aging manage the security of and access to the individual computers and network servers used in the respective offices and facilities used by the Area agency and provider organizations to record and report client, programmatic and fiscal data.

- (a) The AAA is responsible for verifying for each staff member at the AAA and provider level, his/her need for access to AIMS and to which functions within AIMS users have need of access. Authorized users may access the system only while actively employed or providing volunteer staff service. AAAs/providers may provide appropriate system access to contract employees, for the term of the contract agreement.
- (b) The AAA is responsible for assuring that authorized users have and use individual passwords to access the system. Passwords are not shared.
- (c) The AAA will develop and implement procedures for disabling passwords and discontinuing access to the system whenever staff at the AAA or provider agencies, including contract staff and volunteers, terminate employment or volunteer service for any reason.
- (d) Owners of data at each level of the network are ultimately responsible for ensuring that adequate controls exist to protect their transactions. The type and degree of protection shall be commensurate with the nature of the information, the operating environment, the potential for exposures resulting from the loss, misuse or unauthorized access to or modification of the information.
- (e) Each Area Agency must evaluate its business needs and the associated risks for its local information systems in conjunction with its management of data handling. (See Appendix 96-A, "Recommended Guidelines for Handling Data.")

**§96.11 Monitoring.**

- (a) Area Agencies will conduct periodic reviews of participants' records maintained at the AAA/provider level, whether maintained in conventional or electronic format, to verify that eligibility criteria for services are met and required documentation is maintained, based on a review of assessment and reassessment documentation and documentation of service plans and service delivery activities. The area agency shall comply with the Division's requirements in HCBS Manual §102.6, relating to Area Agency on Aging Administrative Requirements and monitoring of subcontractors.
- (b) The Department/Division reserves the right to monitor and inspect the operations of the Regional Development Center/Area Agency on Aging and any subcontractor for compliance with the provisions of contracts with the Department and all applicable federal and state laws and regulations and Department policy, with or without notice, at anytime during the term of this Contract. Monitoring and inspection activities may include, without limitation, on-site health and safety inspections; financial and service delivery audits; review of any records developed directly or indirectly as a result of the contract; review of management systems, policies and procedures; review of service authorization and utilization activities; review of any other areas, activities or materials relevant to or pertaining to the contract; and requirements to maintain on file with the Department such records as the Department may require to demonstrate compliance with the provisions of the contract. The Department will provide the contractor/subcontractor with a report of any findings and recommendations and may require the development of corrective action plans as appropriate.

**§96.12 Disposal of Electronic Documents**

Area Agencies and contractors are required to comply with state record retention requirements, which currently call for conventional documents to be retained for a period of 6 (six) years or until all outstanding claims or litigation are resolved. Data entered into and stored in the centralized AIMS database are managed by the Department of Human Resources Office of Information Technology. However, Area Agencies and subcontractors may be retaining certain other business related data in electronic formats. Please see Appendix 96-B for suggested guidelines for disposing of electronic documents, including email.

**§96.13 Technology Planning** As a part of the larger strategic planning process, Area Agencies periodically will assess the technology needs of both their own organizations and assist subcontractors to identify their technology needs. Technology needs assessments are used to identify barriers to compliance with minimum technology standards<sup>4</sup> implemented by the Department of Human Resources Division of Aging Services. Area Agencies will assure the availability of adequate and sufficient resources to develop, implement and maintain technology infrastructure, equipment and staffing to stay abreast of changes in standards and requirements.

**Effective Date:** Upon Issuance. Area Agencies shall have a reasonable amount of time in which to conduct assessments of technical capability, develop protocols and establish necessary procedures for data management activities.

**Review Date:** Annually or at any such time that there are changes in law or regulations which affect this policy.

---

<sup>4</sup> Standards for operating systems, hardware and software are developed by the DHR Office of Information Technology. Current standards are found on the AIMS website at [http://www.aims.dhr.state.ga.us/Info\\_Tips\\_howto/checklist\\_for\\_hardware.htm](http://www.aims.dhr.state.ga.us/Info_Tips_howto/checklist_for_hardware.htm)

**Appendix 96-A**  
**Recommended Guidelines for Data Handling**

### **Recommended Guidelines** <sup>5</sup>

Following are guidelines based for data management and handling standards and best practices:

- The originator of a telephone call, a facsimile transmission, an E-mail, a computer transaction, or any other telecommunications transmission, should be aware of the possibility of compromise of confidentiality, integrity or availability of the information transmitted, and determine whether the information requires additional protection and handling.
- Agencies should provide special protection and handling to information that is covered by statutes, including, for example, confidential information, financial information, protected health information.
- Owners of confidential information should authorize access on a strict "need to know" basis in conformance with legal requirements for allowable access.
- Agency personnel should have access to confidential information only for the performance of their duties.
- An agency that receives/uses confidential information from another agency shall observe and maintain the confidentiality conditions imposed by the providing agency.

---

<sup>5</sup> Adapted from the State of North Carolina's Information Resource Management Commission Guidelines

**Appendix 96-B**

**Checklist for Disposal of Electronic Documents**

### **Checklist for Disposal of Electronic Documents<sup>6</sup>**

**Follow these steps and answer the questions:**

1. Does the message or document grant some kind of approval under a delegated authority, for example, authorize the expenditure of funds?

If Yes, print the message, have it signed by the authorizing officer and file in a designated place.

(All such messages should indicate where a signed copy will be filed.)

2. Does the document:
  - signify a change in policy?
  - create a precedent?
  - relate to the substantive business of the work unit, section or organization?
  - include legal advice?
  - involve negotiations on behalf of the organization?

If Yes to any of the above, print and file in a central file location

3. Is this a formal communication between contracting authorities or their delegates?

If Yes, print and file in work unit or central file location.

4. Is the document used to initiate, continue or complete an organizational activity?

If Yes, print and file in work unit or central file location.

5. Does the document have ongoing value to others in the work unit?

If Yes, print and file in the work unit.

6. Does anyone external to the work unit need to be aware of, or refer to, this document in the future?

If Yes, print and file in central file location.

7. Are there other documents on this matter, such as questions, answers and responses, and other prior documents?

If Yes, evaluate all documents together.

---

<sup>6</sup> Adapted from *Managing Electronic Documents and Folders*, University of Melbourne, Australia, 2002

**Document Disposal continued--**

8. Is the document of information only value, that is, an information copy?  
If Yes, delete the document.
  
9. Does the document comprise draft information leading to a final version?  
If Yes, delete the document.
  
10. Is the document of short term, facilitative value, for example related to arranging a meeting?  
If Yes, delete the document.
  
11. Does a paper copy or copy in another storage medium (floppy disk, zip drive, or CD) already exist?  
If Yes, delete the document.