III. Records Management

A. Record Retention and Disposition

[Table of Contents]

1. Definitions

   Unless the context clearly specifies otherwise, the following terms are defined as follows:

   1.1 "Agency" means Division of Aging and Adult Services, Area Agencies on Aging, or community service provider.

   1.2 "Client" means any applicant for, or recipient of, services administered under the auspices of the Division of Aging and Adult Services.

   1.3 "Client information" or "client record" means any information, whether recorded or not, including information stored in computer data banks or files, relating to a client which was received in connection with the performance of any function of the agency.

   1.4 "Public record" or "public records" shall mean all documents, papers, letters, maps, books, photographs, films, sound recordings, magnetic or other tapes, electronic data-processing records, artifacts, or other documentary material, regardless of physical form or characteristics, made or received pursuant to law or ordinance in connection with the transaction of public business by any agency of North Carolina government or its subdivisions. [NC General Statutes 132-1]

   1.5 "Community service provider" means any public or private agency from which Division of Aging and Adult Services funded services are purchased or authorized.

2. Accountability

   The records covered by these policies are in the custody of the Area Agencies on Aging or their funded subrecipients, including county governments and the community service providers designated by the county for delivering services under the funding sources subject to these policies. Records are maintained for agency use in delivering services or in documenting agency operations. They include but are not limited to all financial and programmatic records, supporting documents, statistical records and other records of grantees and contractors, as well as their subcontractors.

   It is the responsibility of all Area Agencies on Aging, community service providers, and contractors/subcontractors to assure effective records management so that legal record keeping requirements are met. All contracts/grants related to the expenditure of funds subject to these policies must include the requirement that records will be maintained in accordance with federal or state policies, whichever is more restrictive, and include a provision that allows DHHS, DAAS, and/or the AAA to access persons and records relevant to the implementation of the contracts/grants.

3. Records Impacted

   Chapters 121 and 132 of the N.C. General Statutes govern the retention and disposition of public records, e.g., documents, papers, electronic records, or other materials regardless of format (including electronic mail), that are made or received in connection with the transaction of official business.

   All public records as defined by N.C.G.S. §132-1 are covered by this policy. This includes both confidential and non-confidential records. Classification of records as confidential will warrant different treatment when processing records as discussed in Sec. III B below. Nothing in this chapter

should be construed to require or authorize an agency to disclose confidential information as part of a public record.

4. Retention Period

Record retention schedules and purge dates are maintained by the DHHS Controllers' Office for records related to federal funding grants and maintained by the NC Department of Natural and Cultural Resources, Office of Archives and History, for other types of records that are common to most agencies (e.g., personnel records, program records, financial records, etc.). This policy is intended to complement the use of approved record retention and disposition schedules, not replace or supersede them. This policy does not authorize agencies to destroy or dispose of unscheduled records. **Agencies may not destroy or otherwise dispose of contract/grant records prior to the purge dates listed in the DHHS record retention schedule or the agency-specific schedule approved by the State Archives.**

Most federal funding requires a minimum 3-year record retention, but there is no standard timeframe for retention because the start date usually is based on the final grant expenditure report. State rules [09 NCAC 03M .0703 (4)] require a retention period of 5 years or until all audit exceptions have been resolved, whichever is longer. Agencies subject to these policies should be aware that the DHHS Controller's Office tracks both federal and state retention periods and issues specific guidance in a schedule. See the DHHS retention and disposition schedule for "Aging Grants." It lists specific guidance regarding first allowable purge date for specific federal funds (e.g., Title III C1 congregate meals) and specific grant fiscal years (e.g., SFY 09 – records may be purged July 1, 2015; SFY 10 – do not purge/retain files). In addition, the State Archives approves agency-specific schedules (e.g., county departments of social services and public health departments) that provide disposition instructions for other categories of records (e.g., agendas and meeting packets, correspondence, minutes of public bodies, budgets, payroll records, bank statements, receipts, personnel records, etc.). Often the State Archives schedule will reference the DHHS schedule if records are clearly related to federal funding. For example, the schedule for Regional Councils lists a disposition schedule for the AAA's Home and Community Care Block Grant files that references the DHHS retention schedule.

In the event that a federal or state law or legal requirement dictates that a record be kept longer than a purge date in the applicable schedule, the records in all such cases must be kept for the longest applicable period. Amended federal expenditure reports, pending/open audits, litigation, or other types of official or legal actions may extend the period of required retention.

5. Substitution of Surrogates for Paper Originals

Often agencies adopt document management procedures to streamline storage requirements and reduce administrative costs. In these cases, a "digital surrogate" may take the place of a paper record during scanning. **Any records reproduced by electronic means that are still within the retention period must not be destroyed unless the agency has a digital imaging policy that has been approved by the NC Department of Natural and Cultural Resources, Division of State Archives and Records, the Division of Aging and Adult Services, or the Area Agency on Aging.** With an approved policy, copies made by microfilming, scanning, or similar methods may be substituted for the original records. Original records may not be destroyed unless an analog copy exists prior to destruction if the record is still within the specified retention period.

6. Destruction of Records

Confidential information stored in any format should be destroyed when no longer needed and when allowed by record retention schedules, funding requirements, and/or other official or legal actions. The

retention of records beyond their purge dates obligates agencies to continue protecting confidential information from unauthorized disclosure as required in III.B below.

All agencies must comply with 07 NCAC 04M .0510 when deciding on a method of record destruction. Confidential records, including electronic records, must be destroyed in such a manner that the data, metadata, and/or physical media cannot be read or reconstructed. The NIST Special Publication 800-88 R1 Guidelines for Media Sanitization is the recommended guidance used by NC DHHS.

7. Access to Records

7.1. Federal and State Funds – DHHS, the Comptroller General of the United States, the Division of Aging and Adult Services, or any of their authorized representatives, shall have the right of access to any books, documents, papers, or other records of grantees/contractors which are pertinent to a grant/contract of Federal funds made by the Division in order to make audit examinations, excerpts, and transcripts. Similarly, the Division of Aging and Adult Services, or its authorized representatives, shall have access to records pertaining to grants or contracts involving State funds. These provisions extend to subgrantees/subcontractors. In such cases, the right of access shall include the grantee/contractor making the subgrant/subcontract.

7.2. Expiration of Right of Access – The right of access in this section shall not be limited to the required retention period, but shall last as long as the records are retained.

7.3. This section does not require grantees/contractors to permit public access to other records that are not pertinent to the grant/contract under review.

8. Confidentiality of Personal Information

All information which is identifiable with any specific individual must be kept confidential unless the person concerned gives informed consent for the information to be released. This applies to both client information and personnel records. Requirements for protecting client confidentiality are provided in Sec. III.B.

B. Confidentiality and Security of Information

[Table of Contents]

1. Definitions

Unless the context clearly specifies otherwise, the following terms are defined as follows:

1.1 "Agency" means Division of Aging and Adult Services, Area Agencies on Aging, or community service provider.

1.2 "Client" means any applicant for, or recipient of, services administered under the auspices of the Division of Aging and Adult Services.

1.3 "Client information" or "client record" means any information, whether recorded or not, including information stored in computer data banks or files, relating to a client which was received in connection with the performance of any function of the agency.

1.4 “Personal identifying information” means for purposes of this policy any client information that can be used to distinguish a person’s identity alone or when combined with other identifying information, such as date of birth, gender, or race.

1.5 "Court order" means any written order from a judge that directs explicitly the release of client information.

1.6 "Community service provider" means any public or private agency from which Division of Aging and Adult Services funded services are purchased or authorized.

The DHHS Security Manual notes that data classified as confidential:

- Is limited to authorized users with a demonstrated and documented need-to-know
- Has regulatory restrictions or safeguards related to access, storage or usage
- Must not be posted on any public website
- May not be disclosed without explicit authorization
- Is stored with appropriate physical and logical access controls
- Requires protection during transmission
- Must be destroyed when no longer needed
- Requires sanitization prior to equipment disposal, reuse, or being serviced by an external party
- Is of such a nature that the loss, damage, or unavailability causes an increased impact, such as loss of opportunity, loss of organization/program confidence on behalf of the citizens, or financial or regulatory sanctions.

For purposes of this policy, all client information in any form is confidential information that must be protected. Certain confidential client information has the potential for increased impact if it is not protected because it can be used to distinguish or trace a person's identity either alone or because it is linked or linkable to a specific individual. Confidential and/or personal identifying information might include, but is not limited to, a person's name, Social Security Number (including only the last 4 digits), date of birth, digital signature, address, and phone number. This information must be protected from unauthorized disclosure per the policies and procedures below.

Certain agencies have funding sources other than the funding to which these policies apply, and those funding sources may have more stringent requirements for protecting the privacy and security of information even if similar services are provided. This includes agencies subject to the privacy and security rules of the Health Insurance Portability and Accountability Act (HIPAA) because they are in business associate relationships with covered entities (health care plans, health care providers, or health care clearinghouses). Licensed home care agencies, for example, are likely to be certified for Medicare and Medicaid reimbursements. Since Medicare and Medicaid are health care plans, these home care agencies are business associates of covered entities and subject to the HIPAA privacy and security rules. If they are also funded for HCCBG in-home aide services, it is highly likely that their policies and practices meet and exceed the confidentiality and security requirements detailed here. HIPAA rules have very specific definitions of protected client information that apply to "Protected Health Information" maintained in or transmitted by electronic media and "Individually Identifiable Health Information" about a person's health condition or treatment information that is created or received by a health care plan, health care provider, or health care clearinghouse.

Although the policies and procedures in this manual do not require HIPAA protections, the following requirements and guidance convey responsibilities on funded agencies to establish policies and procedures to protect client information and to train those authorized to access this information in order to minimize the risk of unauthorized disclosures.

2. Confidentiality of Client Data

2.1 As specified in 45 C.F.R. 1321.51, client information obtained by the Division of Aging and Adult Services, Area Agencies on Aging, or community service providers from an older person or their designated representative shall not be disclosed in a form that identifies the person without the informed consent of the person or legal representative, unless the disclosure is required by court order or for program monitoring by authorized federal, state, or other designated monitoring agencies.

2.2 If the agency receives information from another community service organization or individual, then such information shall be treated as any other information generated by the Division of Aging and Adult Services, Area Agency on Aging, or community service provider and disclosure thereof will be governed by any condition imposed by the furnishing community service organization or individual.

3. Disclosure Pursuant to Other Laws

Whenever federal or state statutes or regulations specifically address confidentiality issues, the agency shall disclose or keep confidential client information in accordance with those federal or state statutes or regulations.

4. Ownership of Records

All client information contained in any records of the agency is the property of the agency. Employees of the agency shall protect and preserve such information from dissemination except as indicated by the policies established.

5. Security of Records

5.1. The agency shall provide a secure place with controlled access for the storage of client records or reports, or both, which contain client specific information.

Appropriate steps must be taken to assure confidentiality, but certain steps are common sense and require little or no technology. Conversations and paperwork involving client information should be handled in a private location behind closed doors if possible to assure privacy. Agencies with an open floor plan should designate at least one office with a door to be the location where staff can go to conduct sensitive business with a client.

Locked files, locked doors, and restricted access can provide basic protection against unauthorized access to confidential information in paper or electronic form. However, the security and long-term maintenance of electronic records requires special commitment and active management by agencies. For example, computerized records should be backed up routinely, and there should be plans for protecting computer systems in case of emergencies. Agencies can install anti-virus/anti-spyware software and check for regular updates. All information should be password protected with strong passwords. Screens should be locked when staff are away from their computers. Sensitive information must be protected during electronic transmission, including email and faxes. Identifying information should never be sent in the body of an email. It should only be sent as an attachment to an encrypted email or as an encrypted attachment to an email.

5.2. Only employees, students, volunteers or other individuals who must access client information in order to carry out duties assigned or approved by the agency shall be authorized to have access to such information.

Agencies should identify which individuals or positions have a documented need to know confidential client information in order to carry out their duties. These are the only people who should be authorized to have access. In addition to the consideration of who is allowed to access confidential information, agencies should evaluate how these individuals access information in carrying out their assigned duties. For example, it is recommended that agencies consider whether or not to allow staff to create, update, or store confidential information on personal electronic devices (e.g., computers and flash drives) or personal online accounts.

5.3. Only authorized individuals may remove a record or report, or both, from the storage area and that individual shall be responsible for the security of the record until it is returned to the storage area.

In current practice, this policy should apply in principle not only to the protection of paper records containing client information, but also to the transmission of client information electronically or the creation/storage of confidential client information on a mobile device with official business outside the agency's secure environment. Agencies should strictly control (or even prohibit, depending on the agency's capabilities) the transport of and/or access to client information from mobile devices such as laptops, tablets, and cellphones, whether they are agency-issued or personal devices, because they are generally higher risk than non-portable desk top computers located in an organization's controlled access areas. If agencies allow the storage or transmission of client information via portable devices that leave the facility, they should be aware that protecting the confidentiality of this information is most often accomplished by encryption software on the mobile device – either encrypting the communication or encrypting the information before it is transmitted.

5.4. The agency shall assure that all authorized individuals are informed of the confidential nature of client information and shall disseminate written policy to and provide annual training for all persons with access to client information.

Agencies may not be able to protect information from all imaginable threats, but they must use protections that provide reasonable safeguards within the context of their business environment. This is usually done after carefully analyzing the sensitivity of client information collected and stored in any format, assessing potential risks, controlling access points, and taking into account the nature of the agency's overall business. The most secure facilities and equipment can still be undermined unintentionally by authorized individuals who are unaware of their obligations to protect confidentiality or are unaware of the agency's plan for protecting client information. Training at orientation before an individual is granted access and then annual training thereafter are good opportunities to reduce the possibility that confidential information, especially data that alone or in combination could be used to identify an individual, will be accessed, used, or disclosed inappropriately.

5.5. The agency shall be allowed to destroy records in accordance with Record Retention Schedules promulgated by the Division of Archives and History, and state and federal statutes and regulations.

In addition to the authorized methods of record destruction outlined for various data formats on the website of the State Archives, agencies undertaking record destruction should consider some of the places where electronic document images may be stored that are not as obvious as others. For example, most offices now have digital printers, copiers, faxes, and scanners with hard drives that require the same attention as computer hard drives when they are taken out of service. With the use of electronic equipment such as these, agencies should remember to

securely delete confidential information stored in the document images on these hard drives as well. NC DHHS recommends the use of NIST Guidelines for Media Sanitization, Special Publication 800-88 Revision 1 (or subsequent revisions), for determining appropriate methods of destroying, sanitizing, clearing, or purging confidential electronic information.

5.6. Area Agencies on Aging and community service providers shall establish written procedures to prevent accidental disclosure of client information from automated data processing systems.

Determining appropriate safeguards requires an agency to consider carefully what policies and procedures will support the security of information collected for specific programs. Many agencies have funding sources other than the funding to which these policies apply, and those funding sources may have more stringent requirements for protecting the privacy and security of information even if similar services are provided.

Within the funding sources covered by these policies, confidential information and client identifying information will be collected on all clients receiving services. However, certain services, such as adult day services and in-home aide services, also will include limited medical information stored at the local level that will require careful consideration of appropriate safeguards. Agencies need to evaluate the sensitivity of all information collected and minimize the collection to what is absolutely necessary to accomplish a program's purpose. Certain information (e.g., last 4 digits of the SSN or medical condition) is more sensitive than other information (e.g., address and phone number). Once obtained, all confidential and/or identifying information must be protected from accidental disclosure throughout its life cycle in various formats, up to and including its authorized destruction. For this reason, for example, AAAs should never take copies of confidential client information used to demonstrate compliance with service standards during monitoring, but should simply note on monitoring tools the documentation that was viewed. Likewise, community service providers should weigh what information they document when clients offer medical information that is not requested or needed for eligibility or service delivery.

One potential source of guidance is the Special Publication series of reports by the National Institute of Standards and Technology (NIST). For example, one publication issued by NIST is a Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), Special Publication 800-122. This guide outlines various ways agencies can evaluate their legal obligations to protect information, including the assessment of impact if a person's identifying information is not protected and there are any negative or unwanted effects from disclosure. Typical examples in the case of services supported by funding subject to these policies might include identity theft or emotional distress if information is not safeguarded.

In the final analysis, agencies should seek the advice of an attorney or security consultant to determine the actual policies and procedures needed by the agency to protect the client information associated with the agency's services and programs.

6. Release of Client Information

6.1. No client identifying information, except as referenced in Sec. III.B.5, which is maintained by the Division of Aging and Adult Services, Area Agency on Aging, or community service provider shall be released to other individuals or community service organizations without obtaining a signed consent for release of information from the client or legal guardian.

6.2. The consent for release of information shall include, at a minimum, the following items:

- **Name of the provider and recipient of the information;**
- **The extent of the information to be released;**
- **The name and dated signature of the client or client representative;**
- **A statement that the consent is subject to revocation at any time except to the extent that action has been taken in reliance on the consent;**
- **Length of time the consent is valid.**

The client may alter the form to contain other information, including but not limited to a statement specifying the date, event, or condition upon which the consent may expire even if the client does not expressly revoke the consent and the specific purpose for the release.

6.3. A copy of the signed consent for release of information shall be maintained in the client record.

7. Informed Consent

Prior to obtaining a consent for release of information, the delegated representative shall explain the meaning of informed consent. The client shall be told the following:

- **Contents to be released;**
- **That there is a definite need for the information;**
- **That the client can give or withhold the consent and the consent is voluntary;**
- **That there are statutes and regulations protecting the confidentiality of the information.**

8. Client Access to Records

8.1. Access to information about herself/himself is the right of the client. Upon written or verbal request, the client shall have access to review or obtain without charge a copy of the information in her/his records with the following exceptions:

- **Information that the agency is required to keep confidential by state or federal statues or regulations;**
- **Confidential information originating from another community service organization;**
- **Information that would breach another individual's right to confidentiality.**

8.2. Response to a client's request for access to information contained in his record must be provided as promptly as feasible but no more than five working days after receipt of the request.

8.3. The Director or delegated representative shall be present when the client reviews the record. The Director or delegated representative must document in the client record the review of the record by the client.

9. Contested Information

A client may contest the accuracy, completeness or relevancy of the information in his record. A correction of the contested information, but not the deletion of the original information if it is required to support receipt of state or federal financial participation, shall be inserted in the record when the Director or designee concurs that such correction is justified.

When the Director or delegated representative does not concur, the client shall be allowed to enter a statement in the record. Such corrections and statements shall be made a permanent part of the record and shall be disclosed to any recipient of the disputed information. If a delegated

representative decides not to correct contested information, the decision not to correct shall be reviewed by the supervisor of the person making the initial decision.

10. Withholding of Information from the Client

When the Director or delegated representative determines on the basis of the exceptions outlined in Sec. III.B.8 to withhold information from the client record, this reason shall be documented in the client record.

The Director or delegated representative must inform the client that information is being withheld, and upon which of the exceptions specified in Sec. III.B.8 the decision to withhold the information is based.

If confidential information originating from another community service organization is being withheld, the client shall be referred to that community service organization for access to the information.

11. Disclosure of Client Information Without Client Consent

Client information included in the client record may be disclosed without the consent of the client under the following circumstances:

11.1 To other employees of the agency for the purpose of making referrals, supervision, consultation or determination of eligibility.

11.2 Between the community service provider, Area Agency on Aging, and Division of Aging and Adult Services for the purposes of reporting and monitoring.

12. Information Needs of Community Service Providers

Client information may be disseminated to community service providers in accordance with the release of information statement included on the client registration form. Any further disclosure will require a signed release of information form from the client.

13. Security Incidents and Data Breaches

Community service providers, including subcontractors and vendors, must develop a process by which the Division of Aging and Adult Services is notified within 24 hours of suspected or confirmed security incidents and data breaches. DAAS is responsible for notifying DHHS privacy and security staff. Once that occurs, both the Division and the provider will await further guidance and instruction.

C. Electronic Records and Electronic Signatures

[Table of Contents]

1. Definitions

Unless the context clearly specifies otherwise, the following terms are defined as follows:

1.1 "Agency" means Division of Aging and Adult Services, Area Agencies on Aging, or community service provider.

1.2 "Client" means any applicant for, or recipient of, services administered under the auspices of the Division of Aging and Adult Services.

1.3 "Client information" or "client record" means any information, whether recorded or not, including information stored in computer data banks or files, relating to a client which was received in connection with the performance of any function of the agency.

1.4 "Court order" means any written order from a judge that directs explicitly the release of client information.

1.5 “Electronic records” include electronic databases, electronic mail, and all other records created and maintained in an electronic format by all state and local offices in NC, per DHHS records retention policy.

1.6 “Electronic signature” is a technology-neutral term for various ways that an electronic record can be signed, e.g., a digital signature, a digitized image of a signature obtained by using an electronic tablet or signature pad, a biometric identifier, a scanned handwritten signature, or an image captured with digital photography. For purposes of this policy, an electronic signature does not include a name typed as a signature on a form by the person who completed the form unless a software application for an electronic record also applies a digital signature that serves as a unique identifier for the individual and a time/date stamp.

2. General Requirements

2.1 Agencies may create and maintain records in an electronic format without the necessity of creating and maintaining paper copies, so long as all requirements for the completion of forms (including client, staff, or other professional signatures) and other necessary documentation can be met.

2.2 Per the requirements related to informed consent in Sec. III.B, client information in any format, whether recorded or not and including information in computer data banks or files, must be kept confidential by all agencies, including their subcontractors and vendors, and not disclosed in a form that identifies the person without the informed consent of the person or legal representative. The only exceptions are when disclosures are required by court order or for program monitoring by authorized federal, state, or other designated monitoring agencies.

2.3 Agencies shall maintain electronic records in a legible and retrievable form and provide for adequate data backup. Agencies must assure that electronic records can be retrieved and printed for such purposes as monitoring, record reviews, hearings, and audits if requested.

2.4 Per the record retention requirements in Sec. III.A, agencies must maintain required documentation on file when it chooses to store documents electronically until they have met their required retention period. Record retention schedules and purge dates are maintained by the DHHS Controllers’ Office for records related to federal funding grants and by the NC Department of Natural and Cultural Resources, Division of Archives and Records, for other types of records that are common to most agencies (e.g., personnel records, program records, financial records, etc.). This policy is intended to complement the use of approved record retention and disposition schedules, not replace or supersede them.

2.5 Any records reproduced by electronic means that are still within the retention period must not be destroyed unless the agency has a digital imaging policy that has been approved by the Division of Archives and Records, the Division of Aging and Adult Services, or the Area Agency on Aging.

3. Required Policies and Procedures

3.1 In terms of normal business operations and grant management, agencies should adopt and apply data security standards and procedures that comply with all applicable federal, state, and local laws, regulations, and rules.

3.2 Agencies must adopt written policies and procedures to govern the creation and maintenance of documents electronically and the authorization and use of electronic signatures, if

applicable. At a minimum, policies related to electronic records and, if applicable, electronic signatures must include:

3.2.1 The designated persons or positions authorized to use electronic signatures (e.g., specific staff positions, clients, dietitians, authorizing professionals for special nutrition products, qualified healthcare professionals, etc.).

3.2.2 The intended scope of circumstances under which electronic signatures can be used by the agency (e.g., specific programs and forms).

3.2.3 Written policies and procedures to prevent accidental disclosures of client information from data processing information systems. Information created or maintained in electronic formats must be maintained in a secure environment with controlled access.

3.2.4 Any related efforts that must be undertaken by staff to assure compliance with requirements for privacy, confidentiality, and security of electronic records. When documenting compliance with policy requirements, agencies may reference broader policies on data security, i.e., policies not specific to electronic records only, to demonstrate that requirements apply across formats. However, agencies should carefully consider whether general policies adequately detail the procedures needed for the security of information created and stored in an electronic format.

4. Security Awareness Training

4.1 Agencies must have an annual security awareness training plan for employees to reduce the risk of improper access, uses, and disclosures of confidential information created, maintained, and transmitted in an electronic format.

4.2 Agencies must maintain documentation that each individual with access to confidential information has been made aware of security measures (e.g., signed/dated training plan or agenda for existing employees and/or new employees at orientation).

5. Electronic Signatures

5.1 As specified in Sec. III.C.3.2, agencies must specify in policy any persons or positions that are authorized to use electronic signatures.

5.2 An electronic signature has the same validity and effect as the use of a signature affixed by hand. Agencies may permit individuals to attest to entries on forms or in records either by written signature or by electronic or digitized signature in lieu of a signature in ink. For purposes of this policy, "attestation" means that, if requested, the author of an entry can authenticate authorship, verify that the contents of the entry are what the author intended, and assume responsibility for the information.

5.3 Requirements related to electronic signatures are technology-neutral with respect to the electronic process or electronic format used. Agencies adopting policies for the use of electronic signatures are not required to obtain any certain technology (e.g., digital signatures that are cryptographically tied to digital IDs or certificates, although this technology is certainly acceptable and represents the highest level of security and accountability for documenting electronic signatures).

5.4 Any technology for electronic signatures chosen by an agency must protect documents from unauthorized modifications. Agencies must be able to demonstrate if requested that electronic signatures are protected by system safeguards (e.g., application software) or other security procedures for assuring the integrity of records. A typical electronic record has a

time/date stamp indicating the document's creation and any subsequent modification. Once an individual signs a form or document by any means, it is expected that the signature will become a permanent, unaltered part of the form or document. The following are two examples of acceptable formats that stop short of the most expensive tamper-proof technology:

- A hand-written signature on an electronic signature pad or tablet that also contains the document being signed and time/date stamps.
- A scanned or faxed paper copy with a hand-written signature and date.

5.5 Electronic Signatures – Applicants/Clients/Designated Representatives

5.5.1 The digitized signatures of applicants/clients/designated representatives may not be saved on file for later use by an agency and imported into a form to "sign" the document. **Each form must be reviewed with applicants/clients/designated representatives before signing, as required by applicable policy. If information is viewed electronically before signing, all information on a form must be viewable to support the person's understanding of what they are signing.**

5.5.2 **Each form that requires a signature must be offered for review and signed individually, whether the signature is handwritten or collected electronically.** In other words, it is not allowable for an agency that uses digitized electronic signatures to populate an entire set of forms with one electronic signature. **If a client requests a copy of a signed form, the copy must contain all information on all sides of the printed form as well as the image of the signature(s) and date signed.**

5.5.3 Examples of forms that may be signed electronically by applicants/clients/designated representatives include consent forms for the release of client information, plans of care, aide timesheets, and client registration forms. Previous requirements for new registrations in ARMS to include an original copy of a client signature on file when updating the DAAS-101 may be met with either a signed paper form or an electronic signature.

5.6 Electronic Signatures – Agency Staff or Other Professionals

5.6.1 **Staff members who are authorized by written agency policies to have electronic signatures on file shall not delegate the use of their electronic signatures to any other staff member except in the case of routine business correspondence.**

5.6.2 Agency staff signatures may be obtained in real time as the author applies the signature or may be a saved image captured during normal business operations. Examples of forms that may be signed electronically by authorized staff include the consumer contributions provider assurance form and program monitoring tools.

5.6.3 **If monitoring tools are completed electronically and/or signed electronically by AAA staff, all handwritten, printed, or electronic monitoring notes, working papers, correspondence, etc., must be available for review (and printing, if requested) with the completed monitoring tool.** Relevant paper documents may be scanned into an electronic monitoring record, but either the paper original or a digital copy must be retained and available for retrieval per Sec. III.A above and instructions on the DHHS record retention website at http://www.ncdhhs.gov/control/retention/retention.htm. As with other records subject to retention requirements, scanned monitoring documentation may not be destroyed unless the agency has a digital imaging policy that

has been approved by the Department of Cultural Resources Division of State Archives and Records, the Division of Aging and Adult Services, or the Area Agency on Aging.

5.6.4 Other professionals – As noted in Sec. III.C. 3.2, persons or positions authorized to use electronic signatures must be specified in the agency's policies and procedures. This includes other professionals such as dietitians, authorizing professionals for special nutrition products, and qualified healthcare professionals who interact with the agency and its clients to authorize or deliver services.