United States Department of Agriculture

Food and Nutrition Service

3101 Park Center Drive
Alexandria, VA
22302-1500

DATE: May 1, 2007

MEMO CODE: SP 10-2007, SFSP 06-2007, CACFP 07-2007

SUBJECT: Update on Electronic Transactions in the Child Nutrition Programs

TO: State Agencies
Child Nutrition Programs
All States

Special Nutrition Programs
All Regions

We have received numerous questions regarding the electronic transfer of information in the administration of State-administered Federal programs. This memo updates the October 2, 2001 policy memo regarding electronic transactions in Child Nutrition Programs (CNP).

Two Federal laws which address the electronic transfer of information are the Government Paperwork Elimination Act (GPEA) of 1998 and the Electronic Signatures in Global and National Commerce Act (E-SIGN) of 2000. The provisions in these laws apply to Federal agencies; however, they do not apply to State Agencies (SAs) or local agencies. Local agencies include Local Education Agencies (LEAs) in the National School Lunch Program (NSLP) and School Breakfast Program (SBP), institutions in the Child and Adult Care Food Program (CACFP), and sponsoring organizations (sponsors) in the Sumer Food Service Program (SFSP). Each State and local agency should review their State's statutes and policies regarding the electronic transfer of information in State-administered Federal program.

These Questions and Answers (Q&As) are intended to provide general guidance on the use of electronic transactions for CNP. This guidance can provide a framework for SAs and local agencies to implement their own systems and establish their own policies which must ensure the legal sufficiency of the information and signature provided.

The Q&As cover different types of electronic transactions, those between SAs and local agencies and those between local agencies and households, such as electronic application. State statutes and policies regarding the electronic transfer of information may be different depending on the parties involved.

In accordance with the Child Nutrition and WIC Reauthorization Act of 2004 (Pub. L. 108-265), which amended section 9(b) of the National School Lunch Act, we encourage local agencies to accept electronic household applications. Local agencies must have the capability to provide legally binding electronic signatures as per State and local regulation.

When local agencies do not have the capability to provide legally binding electronic signatures, local agencies must collect a hard copy signature of critical program documents, such as household application. A Level 2 authentication would meet program requirements for most CNP documents as defined in question B5 of this guidance.

At the end of the Q&As, we have also included a definition section and a website list. These documents will assist in understanding some of the more technical terms and concepts used throughout the Q&As.

Please share this information with local agencies. If you have any questions regarding this memorandum, please contact your respective Regional Office.

Original Signed

STANLEY C. GARNETT
Director
Child Nutrition Division

Attachment

Electronic Transactions in the Child Nutrition Programs
Questions and Answers
2007 Revision

A) GENERAL

A1. What is the authority for electronic signatures, or electronic use of information in government programs?

Two Federal laws which address the electronic transfer of information are the Government Paperwork Elimination Act (GPEA) of 1998 and the Electronic Signatures in Global and National Commerce Act (E-SIGN) of 2000. The provisions in these laws apply to Federal agencies; however, they do not apply to State Agencies (SAs) or local agencies. Local agencies include Local Education agencies (LEAs) in the National School Lunch Program (NSLP) and the School Breakfast Program (SBP), institutions in the Child and Adult Care Food Program (CACFP), and sponsoring organizations (sponsors) in the Summer Food Service Program (SFSP). Each State and local agency should review their State's statutes and policies regarding the electronic transfer of information in State-administered Federal programs.

A2. What other guidance should SAs or local agencies review before implementing an electronic system?

These Q&As provide general guidance on the use of electronic signatures and the use of electronic transactions for Child Nutrition Programs (CNP). They provide a framework for SAs and local agencies to implement their own systems and establish their own policies which must ensure the legal sufficiency of the information and signature provided. SAs and local agencies should review their respective State and local laws on electronic transactions with their State and/or local counsel.

Before developing and implementing an electronic based system to manage their school programs, we recommend SAs and local agencies review the following guidance documents used by Federal agencies (See website addresses at the end of this document):

- *Department of Justice (DOJ) legal considerations in designing and implementing electronic processes, November 2000.*
- *Office of Management and Budget (OMB) E-Authentication Guidance, M-04-04, December 16, 2003.*
- *National Institute of Standards and Technology (NIST) Electronic Authentication Guideline,* NIST SP 800-63, April, 2006.

A3. Does FNS approve any specific software product to establish electronic systems?

No. FNS does not review or approve any specific software product dealing with point of service counts, or with the certification or verification processes. If a local agency receives any information to the contrary, the local agency should notify the State agency, which should notify the respective FNS Regional Office.

A4. Are SAs required to accept information online from local agencies and institutions? Are local agencies required to accept online applications from households?

No. However, we encourage SAs and local agencies to make use of the efficiencies that technology can provide.

A5. Several SAs have already implemented online systems. Is there a potential for information sharing?

Yes. Many States already have online systems developed to assist them in administering the CNP. We encourage States to share their experiences and information on their electronic systems with other SAs. If a State system was developed in whole or in part with State Administrative Expense (SAE) funds, some or all of the system may be available to the States without charge.

A6. Can SAs or local agencies use a combination of paper-based and electronic documents or systems?

Yes. Total conversion from a paper-based system to an electronic one may not be appropriate in all cases. Regardless of the systems that SAs or local agencies use, all documents – electronic or paper - must be legally binding.

A7. Do SAs or local agencies need to have a hard copy signature on file, or is the electronic document sufficient?

An electronic document is sufficient when SAs and local agencies have the capability to provide legally binding electronic signatures. When SAs or local agencies do not have the capability to provide legally binding electronic signatures, SAs or local agencies must collect a hard copy signature of critical program documents (e.g., agreements, first claim submission, household applications, etc.).

A8. Which CNP documents can be submitted electronically?

Institution applications, facility applications, site information sheets, claims for reimbursements, agreements, and household applications may all be filed electronically if SAs and local agencies have the capability to provide legally binding electronic signature, as determined in conjunction with their respective State and/or local counsel.

Institution applications and claims may be submitted online from the institution or local agency to the SA using legally binding electronic signatures, such as personal identification numbers (PINs) and passwords.

1. If a system uses digital signatures rather than PINs and passwords, it is possible to obtain all documents electronically, without having the need for an original hard copy.
2. Permanent agreements can be initially filed electronically with the SA provided they are legally binding. Otherwise, permanent agreements must initially be filed in hard copy. It would then be feasible to amend agreements online once a relationship has been established.
3. Household applications may be submitted online from applicants to local agencies, when local agencies have the capability that allows households to provide legally binding electronic signatures.

A9. Can SAs or local agencies require the use of electronic household application submissions exclusively?

No. Local agencies must be able to provide paper household applications even if they have an electronic application process.

B. LEGAL AND SECURITY ISSUES

B1. If a SA or local agency wants to convert its paper-based system to an electronic one, which basic guidelines should it consider?

SAs or local agencies will need to consider several issues such as potential security risks, costs of implementation and training, and any legal risks associated with this change. Some of the risks include deliberate misuse of the data, or accidents and errors which result in a loss of data.

We recommend that SAs and local agencies follow the same general guidelines prescribed to Federal agencies by the Department of Justice (DOJ) for electronic transactions. SAs and local agencies should also review their respective State and local laws on electronic transactions with their State and/or local counsel.

DOJ's general guidelines advise that Federal agencies:

1. Examine the process being considered for conversion to electronic documents, forms or transactions. Identify customer needs and demands as well as the existing risks associated with fraud, error or misuse.

2. Identify and evaluate the risks and benefits of using electronic documents, transfer of information and electronic signatures in terms of cost and increased or decreased security. This evaluation should take into account the relationships of the parties, the value of the transactions or documents, the future need for the documents (i.e., retention of records), and the need for this process.

3. Consult with counsel about the specific legal implications of using electronic documents and signatures for applications and other program documents. Periodically seek counsel's advice for updates on new Federal and State legislation in this area.

4. Develop plans for retaining and disposing of information, ensuring that it can be made continuously available to those who will need it and that the plans can accommodate changes in staffing. They must ensure that the new electronic system(s) meets Program requirements.

5. Develop management strategies to provide appropriate security for access to electronic records. Consider unique legal risks presented when outsourcing management and storage of agency or school data. Any contractual arrangement for outsourcing management or storage functions should comply with the basic requirements of the Federal Programs and State and local laws.

6. Review State agency regulations or policies to make sure they support electronic transactions and recordkeeping. If new regulations, policies or amendments to agreements are necessary, disseminate them to local agencies and institutions, as appropriate.

7. Seek continual input from their computer specialists or technology experts for updates on technology and consider how these updates will affect their system.

8. Perform periodic review and evaluation of electronic documents, processes, and mechanisms, as appropriate.

B2. What steps should SAs and local agencies follow to ensure electronic records are legally binding?

SAs and local agencies should review their respective State and local laws on electronic transactions, consult with their counsel, and consider DOJs's guidelines to determine proper procedures for your State.

In general, to be legally binding documents for the Federal government, DOJ recommends that electronic records contain, at a minimum, the following information:

1. Date and time of the transaction;
2. Identity and location of each person who transmitted the information, such as:
    a. an identifier traceable to a particular individual (e.g. digital or digitized signatures, or other identifiers, depending on which is appropriate), and
    b. a means of identifying the source of the transmission (e.g. mail server identification, e-mail account name, time-stamped Internet Protocol ("IP") address);

    The identity of an individual can be established to varying degrees of certainty by the individual's transmission or use of any of the following:
    - something the individual knows (e.g. a password or secret number, personal information);

- something the individual possesses (e.g. a token or magnetic card);
- something the individual is (e.g. a physical or biometric attribute); or
- any combination of the above.

3. Confirmation from the recipient agency that the transaction was received (e.g. agreements and monthly claims);
4. The intent of the transaction;
5. The complete contents of the transaction, including any attachments or exhibits;
6. A complete listing of the terms of the agreement and instructions and an indication that these were made available to the submitting party;
7. Certification that the submitting party intended to be legally bound by the terms of the transaction (e.g., the person agrees to be held accountable for the information he or she submits);
8. Certification from the individual to the truth and accuracy of the presented information (e.g., the person is not submitting fraudulent information); and
9. A mechanism in place which proves that the transaction was not altered after it was sent.

B3. What are some of the legal issues a SA or local agency should consider in deciding to convert a paper-based system to an electronic one?

DOJ identifies four main issues for Federal agencies, which State and local agencies should consider in deciding whether to convert a paper-based system to an electronic one:

1. Availability and accessibility of the information - (*this issue is expanded in B4).*
2. Legal sufficiency - meet applicable legal requirements and provide adequate evidence of its transactions and actions.
3. Reliability - underlying processes that create or maintain the data must be reliable.
4. Compliance with other Federal and State laws - legal requirements can affect the use of electronic processes in many contexts, some requiring that the government be able to produce or disclose information, others prohibiting the government from releasing specified information.

B4. What are some of the issues relating to information availability and accessibility that SAs and local agencies should consider when developing an electronic based system?

According to DOJ's guidelines for Federal agencies:

1. An electronic process collects all relevant information, such as:
   - Content: content of the transaction, including all records that comprise the substance of the transaction or filing.
   - Processing: records that contain information about how the transaction was processed, including dates received and changes or modifications that were made in records.
   - Identities: a means to authenticate the identity of all people who participated in the transaction both inside and outside the State agency or local agency.
   - Intent of parties: a means for establishing the intent of the participants to enter into the transaction or agreement.

2. The information is retained properly by:
   - Determining which information should be retained and for what period of time.
   - Designing electronic systems to safeguard against data corruption, such as accidental deletion, equipment failures, storage media deterioration over time, or other hardware and software problems.

3. The information is readily accessible:
   - Computer software and formatting standards quickly become obsolete.
   - Qualified staff may not be available with knowledge of the electronic processes necessary to read older data.
   - Passwords and encryption codes are preserved to maintain access to the archived information.

B5. What are some of the security issues a SA or local agency should consider in deciding to convert a paper-based system to an electronic one?

OMB identifies four identity authentication assurance levels for e-government transactions (M-04-04). We recognize that some of the technical guidelines may not be feasible for SAs or local agencies to apply. When SAs do not have the capabilities to provide legally binding electronic signatures, they must require documents to be initially submitted in hard copy. NIST SP-800-63 identifies the technical guidelines for each of the four levels of identity authentication assurance. Levels 1 and 2 are discussed below. Levels 3 and 4 are not included because these levels have more stringent standards and may not be appropriate. SAs and local agencies may review this information on NIST SP 800-63, April, 2006.

• Level 1: Little or no confidence in the asserted identity's validity.

Although there is no identity proofing requirement at this level, the authentication mechanism provides some assurance that the same claimant is accessing the protected transaction or data. It allows a wide range of available authentication technologies to be employed. For example, a verifier might obtain a subscriber password from a Credentials Service Provider (CSP) and authenticate the claimant by use of a challenge-response protocol.

• Level 2: Some confidence in the asserted identity's validity.

At Level 2, identity proofing requirements are introduced, requiring presentation of identifying materials or information. A wide range of available authentication technologies can be employed at Level 2, such as passwords and PINs (*See Definitions).* Eavesdropper, replay, and on-line guessing attacks are prevented.

To determine the appropriate level of assurance in the user's asserted identity; SAs or local agencies must assess the potential risks from an authentication error. The risk from an authentication error is a function of two factors: a) potential harm or impact; and b) the *likelihood* of such harm or impact.

The categories of harm and impact include:

- Inconvenience, distress, or damage to standing or reputation.

• Financial loss or agency liability.

• Harm to agency programs or public interests.

• Unauthorized release of sensitive information.

• Personal safety.

• Civil or criminal violations.

Based on the above categories of harm and impact, a Level 2 authentication would meet program requirements for most CNP documents, including institution applications, facility applications, site information sheets, claims for reimbursements, agreements, and household applications. Therefore, as appropriate, the SA and local agency must establish a process that links the electronic signature to the applicant.

B6. If a State agency would like to use electronic signatures in its transactions with local agencies or institutions, what form of electronic signatures should be used?

SAs or local agencies have discretion on what form of legally binding electronic signatures would be most beneficial to their programs. Digital signatures *(see Definitions)* should be used if the person or entity coming into a contract is unknown. If digital signatures are not possible, a combination of paper-based (hard copy) and PIN or passwords should be used, at a minimum.

B7. What is a Digital Signature and Public Key Infrastructure System? (*See Definitions for these terms.*)

A digital signature ensures the content of a document has not been altered and prevents the sender from denying the fact that he or she signed and sent the document.

Digital signatures are implemented using a Public Key Infrastructure (PKI) system. PKI technology provides the mechanism to ensure electronic transactions are more secure than their paper counterparts. PKI offers the security services of confidentiality, authenticity, integrity, and technical non-repudiation because:

- The sender and recipient both are uniquely identified so the parties know where the information is coming from and where it is going to (identification and authentication);

- There is an assurance the transmitted information was not altered deliberately or inadvertently (data integrity);

- There is a way to establish that the sender's identity is inextricably bound to the information (technical non-repudiation); and

- The information is protected from unauthorized access (confidentiality or privacy). (Please be aware, however, confidentiality and privacy concerns are not covered in that detail in this guidance. Confidentiality requirements are covered in section 9 of the Richard B. Russell National School Lunch Act; for the NSLP at 7 CFR 210.18; for the application process for

the CNP, at 7 CFR 245.1, 245.2(a)(a-3), 245.6(b)(1), 245.6(f), 245.8(b), and in FNS policy memos dated: 12/7/98; 1/26/01; 8/9/04; 9/15/06.

C) ELECTRONIC RECORDKEEPING

C1. How should SAs or local agencies maintain or "file" electronic documents?

For Federal agencies, DOJ states that records need to be complete, uniform, easily understood and easily accessible. In addition, they need to have been kept under a system that ensures a chain of custody (i.e., a system which can identify each person who was responsible for the information during specific times) and insures the integrity of the information gathered from all sources. Records and e-processes will need to comply with other laws such as those governing privacy, confidentiality, State statutes, etc. Some laws may specify which form and format is to be used for certain e-processes. Agencies should also have a method in place to recover data that may have been encrypted or password-protected with forgotten or canceled passwords, and be able to recover data that was received using outdated software.

C2. Can a SA or local agency use an outside entity to help manage its electronic records and information?

Yes. The DOJ guidance permits Federal agencies to contract out with a third party (private or public organization or agency) to help manage collection and storage of electronic data. We believe that the DOJ guidance in this area can be applied to SAs which administer the CNPs as well as to local agencies participating in the Programs. However, it is important to note DOJ emphasizes that not all private industry systems are appropriate for government use. Federal agencies or local agencies must carefully consider the legal and security risks associated with turning over agency files to a third party and ensure that the third party complies with all participant confidentiality rights.

DEFINITIONS

Authenticate - Assuring the identity of the user. With electronic signatures, that would include use of passwords or PINs.

Authentication – Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

Confidentiality - Ensuring limited access to authorized entities (codes).

Credentials Service Provider (CSP) – A trusted entity that issues or registers subscriber tokens and electronic credentials. The CSP may encompass registration authorities and verifiers that it operates. A CSP may be an independent third party, or may issue credentials for its own use.

Digital Signature – A digital signature is created when the owner of a private signing key uses that key to create a unique mark (the signature) on an electronic document or file. A *digital signature* ensures that the content of a document has not been altered and prevents the sender from repudiating the fact that he or she signed and sent the document. It marks a document with one half of a key pair and requires the second half to authenticate the signer. This is commonly known as "Public Key Infrastructure" (PKI, see below). Digital signature, which is implemented by using a PKI system, is the only type of electronic signature to date that completely ensures the information's validity and repudiation. If a digital signature is used, data integrity can be assured.

Digitized Signature – A digitized signature is a graphical image of a handwritten signature. Some applications require an individual to create his or her hand-written signature using a special computer device, such as a digital pen and pad.

Electronic Signature – An electronic signature is a sound, symbol or process attached to or associated with a contract or other record, and executed or adopted by a person with the intent to sign the record. There are different *Electronic Signatures* available, such as digitized signatures, biometrics, passwords, personal URL addresses, personal identification numbers (PINs), smart cards, and "I Agree" buttons.

Integrity/Data Integrity - To ensure that data or information has not been modified or altered in any unauthorized manner.

Password - A secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings.

Personal Identification Number (PIN) – A password consisting only of decimal digits.

Public Key Infrastructure (PKI) - Is the whole system that implements digital signatures and allows them to be used with specific programs to offer secure communications. A PKI enables users of a basically unsecured public network such as the Internet to securely and privately

exchange data through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and a directory service that can store the certificates.

Smart Card - A smart card is a plastic card the size of a credit card containing an embedded integrated circuit or "chip" that can generate, store, and/or process data.

RELEVANT WEBSITES

Please refer to the following websites for more information about electronic transactions.

OMB

Memorandum M04-04, E-Authentication Guidance for Federal Agencies.
http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

Memorandum M00-15, OMB Guidance on Implementing the Electronic Signatures in Global and National Commerce Act.
http://www.whitehouse.gov/omb/memoranda/m00-15.html

Implementation of the Government Paperwork Elimination Act.
http://www.whitehouse.gov/OMB/fedreg/gpea2.html

DOJ

Legal Considerations in Designing and Implementing Electronic Processes: A Guide for Federal Agencies http://www.usdoj.gov/criminal/cybercrime/eprocess.htm

NIST

NIST SP-800-63, Electronic Authentication Guideline
http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf
http://csrc.nist.gov/pki/

Others

Government Paper Elimination Act, National Archives
http://www.archives.gov/records-mgmt/policy/electronic-signature-technology.html