United States Department of Agriculture

Food and Nutrition Service

3101 Park Center Drive
Alexandria, VA 22302-1500

October 2, 2001

SUBJECT: Electronic Transactions in the Child Nutrition Programs

TO: Regional Directors
All Regions
Special Nutrition Programs

We have received numerous questions regarding electronic submission of information in the Child Nutrition Programs (CNPs). The purpose of the attached Question and Answer (Q&A) document is to provide guidance on electronic transfer of information in CNPs. It establishes a framework for States to follow when determining if conversion from paper-based systems to electronic ones is appropriate. This memo does not discuss electronic transfers from States to the Federal level.

There is no Federal requirement for State agencies or school food authorities (SFAs) to establish a method for collecting Program information electronically or via the Internet. Rather, the intent of this memorandum is to provide information regarding the use of technology in CNPs and assist in determining if electronic transactions are appropriate for a State or SFA. For those States which choose to pursue electronic transactions with their schools and institutions, we remind you that electronic documents are legal documents and are intended to be as legally binding as the paper documents they replace.

At the end of the Q&As, we have 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 your State agencies. If you have any questions regarding this memorandum, please contact Mandy Briggs (CACFP/SFSP Section) or Karen Smith (Schools Section) at (703) 305-2590.

STANLEY C. GARNETT
Director
Child Nutrition Division

Attachment

cc: Lenore Siwiec, ITD Headquarters
Regina Ryder, ITD Headquarters

A) GENERAL

A1. Why should a State agency consider accepting online submission of information in the CNPs?

Some of the benefits to converting paper-based systems to electronic ones include:

- Customer satisfaction
- Improved recordkeeping efficiency and data analysis opportunities
- Increased employee productivity
- Improved security, especially for highly sensitive information
- Long-term cost savings

A2. Are State agencies required to accept information online from schools and institutions?

No. However, we encourage State agencies to make increased use of the efficiencies this technology can provide.

A3. We have heard other States have already implemented an online system. Is there a potential for information sharing?

We know many States already have online systems developed, or are in the process of developing systems, to assist them in administering the Child Nutrition Programs (CNPs). To the maximum extent possible, we encourage States to share their experiences and information on their electronic systems with other State agencies. If these other State systems were developed in whole, or in part with, State Administrative Expense (SAE) funds, some or all of the system may be available without charge. However, if no SAE funds were used, contracts with independent computer consultants or companies may prohibit or limit a State agency from sharing this information with other States.

A4. Currently, all of our transactions with schools and institutions are paper-based. However, we would like to have some, or all, of the transactions conducted over the Internet. Where do we begin?

State agencies interested in converting one or all of their paper-based systems to electronic ones should first evaluate the appropriateness and consequences of such a conversion. When making this decision, States will need to consider several issues such as potential security risks, costs of implementation 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.

To avoid any legal pitfalls, we recommend State agencies follow the same guidelines prescribed to Federal agencies by the Department of Justice (DOJ) for electronic transactions. These guidelines advise that agencies:

- 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.
- 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.
- 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.
- Develop plans for retaining and disposing of information, ensuring it can be made continuously available to those who will need it and that the plan can accommodate changes in staffing. You must ensure that the new electronic system(s) meets Program requirements.
- Develop management strategies to provide appropriate security for access to electronic records.
- 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 schools and institutions, as appropriate.
- Seek continual input from your computer specialists or technology experts for updates on technology and consider how these updates will affect the State's system.
- Perform periodic review and evaluation of electronic documents, processes, and mechanisms, as appropriate.

A5. Can State 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. In certain circumstances, a phased implementation may be more viable than a total conversion.

A6. We have received a document online from a school or institution which requires a signature. Do we also need to have a hard copy signature on file, or is the electronic document adequate?

We recommend State agencies first collect a hard copy signature of critical Program documents (e.g., agreement, first claim submission, etc.), if the State has no prior relationship with the institution or school (unless the State is using digital signatures - *see definitions*). This minimizes the security risks associated with transactions with new applicants.

B. CNP DOCUMENTS

B1. Which CNP documents can be submitted electronically?

Institution applications, facility applications, site information sheets, claims for reimbursements and agreements can all be electronically filed. Applications and claims may be submitted online from the institution or school to the State agency using personal identification numbers (PINs) and passwords if a prior relationship has been established. Permanent agreements should initially be filed with State agency in hard copy. It is feasible to amend agreements online once a relationship has been established. On the other hand, 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.

Electronic submission of information is permissible for documents between the State agency and the school food authority, centers and organizations if PINs and passwords are used.

B2. Can free and reduced-price applications be submitted via the Internet?

While technology is available for schools and institutions to accept free and reduced-price applications over the Internet, this option seems unlikely for most States. The cost of implementing such a system for which the general public can transmit information is expensive. It requires the use of more robust security measures than in situations where there is already an established relationship between the parties (i.e. schools/institutions and States using PINS/passwords). In most cases this means involving a third party to ensure data security. In the future, it is possible that this option will become more practical.

In addition to security issues, several operational issues must be considered. A paper-based application system must always be available to families who do not have access to computers and the Internet. Also, electronic systems must be able to accommodate future changes that may occur in the Programs, including the free and reduced-price application process.

If you would like to share your ideas on collecting free and reduced-price applications online, please contact your regional office. Regional office staff can then share this information with Headquarters.

C. LEGAL ISSUES

C1. What steps should State agencies follow to ensure electronic records are legally binding?

According to the DOJ, electronic records should contain the following information, at a minimum:

- Date and time of the transaction
- Identity and location of each person who transmitted the information (i.e., the information needs to be traceable to a particular individual)
- Confirmation from the recipient agency that the transaction (e.g. agreements and monthly claims) was received
- The intent of the transaction
- The complete contents of the transaction, including any attachments or exhibits
- A complete listing of the terms of the agreement and instructions and an indication that these were made available to the submitting party
- Certification that the submitting party intended to be legally bound by the terms of the transaction (i.e., the person agrees to be held accountable for the information he or she submits)
- Certification from the individual to the truth and accuracy of the presented information (i.e., the person is not submitting fraudulent information)
- A mechanism in place which proves that the transaction was not altered since it was sent
- A means of distinguishing final documents from drafts

C2. What are some of the security issues a State agency should consider in deciding to convert a paper-based system to an electronic one?

There are four main issues States should consider in deciding whether to convert a paper-based system to an electronic one:

1. Availability and accessibility of the information—(e.g., the collection and retention of the information in light of changing technology and computer upgrades)
2. Legal sufficiency—does the system under consideration meet applicable legal requirements and provide adequate evidence of its transactions and actions?
3. Reliability—will the system ensure that if the documents are needed for legal reasons, the context will be preserved in a useable format?
4. Compliance with other laws, including State laws (e.g., the statutes of fraud)

As part of the assessment process, States should factor in the relationship between the parties, the value of the transaction and the perceived risk of intrusion, or unauthorized access to the information. Other preventative security measures include having trained staff, or contractors, available who are familiar with the system and know how to operate the programs. You should also have a contingency plan in the event that these program operators leave their position, as well as a way to remove operators from the system.

We support DOJ's recommendation to Federal agencies that agencies convert their systems in phases, or incrementally from low-risk to high-risk, and follow the recommended steps *[see A4 in the General section]* when implementing a new electronic system.

D) ELECTRONIC RECORDKEEPING

D1. How should we maintain, or "file," electronic documents?

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. The State agency 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.

D2. Can we use an outside agency to help manage our 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 its collection and storage of electronic data. We believe that the DOJ guidance can be applied to State agencies which administer the CNPs. However, it is important to note DOJ emphasizes not all private industry systems are appropriate for government use. Agencies must carefully consider the legal risks associated with turning over agency files to a third party and ensure that they are complying with participant confidentiality rights.

E) TECHNOLOGY

E1. We would like to use electronic signatures in our transactions with our schools/institutions. What form of electronic signatures should we use?

State agencies have discretion on what form of electronic signatures would be most beneficial to their programs. However, we believe PIN or password systems are

sufficient in cases where a relationship has already been established with the school or institution. 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.

E2. 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 will be identified uniquely so the parties know where the information is coming from and where it is going (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 detail in this guidance.

F) LEGISLATION

F1. What is the authority for electronic signatures, or electronic use of information in government programs?

Two Acts 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, however, apply to Federal agencies and do not apply to State agencies. Therefore, each State should review its own statutes and policies regarding the use of electronic information in the administration of State-administered Federal programs.

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).

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. Some types of *Electronic Signatures* are digitized signatures, biometrics, passwords, personal URL addresses, personal identification numbers (PINs), smart cards, "I Agree" buttons, and digital signatures are all types of electronic signatures.

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

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

http://www.whitehouse.gov/omb/memoranda/m00-15.html

http://www.whitehouse.gov/OMB/fedreg/gpea2.html

DOJ

http://www.usdoj.gov/criminal/cybercrime/eprocess.html

Others

http://csrc.nist.gov/pki/

http://www.nara.gov/records/policy/gpea.html

http://www.etsi.org/sec/el-sign.html

http://www.fda.gov/ora/compliance_ref/part11/FRs/background/pt11finr.txt

http://www.dss.state.ct.us/pubs/BIOMET_BREAKING_%20NEWS.html

http://www.fafsa.ed.gov/ or http://www.ed.gov/

https://vabenefits.vba.va.gov/vonapp/default.asp