

CNP DOCUMENTS

A1. Which CNP documents may be submitted electronically?

Institutions applications, facility applications, site information sheets, claims for reimbursement and agreements may 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 be initially filed 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.

A2. May 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 may transmit information is expensive. It requires the use of more robust security measures than in situations where there is already an established relationship between parties. 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 also be considered:

1. A paper-based application system must always be available to families who do not have access to computers and the Internet.
2. The electronic systems that you select 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 you ideas on collecting free and reduced-price applications on line, please e-mail them to Irene Wimbush. She will forward your responses to the USDA Regional Office.

B. LEGAL ISSUES **Note: This item is shared for your information only.**

B1. What steps should State agencies follow to ensure electronic records are legally binding?

According to the Department of Justice (DOJ), electronic records should at a minimum, contain the following information:

- 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/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 is in place which proves that the transaction was not altered since it was sent
- A mechanism is in place to distinguishing final documents from drafts

As part of the assessment process, States are asked to 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 preventive security measures include having trained staff or contractors, available who are familiar with the system and know how to operate the programs. In addition we are asked to 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.

C. ELECTRONIC RECORDKEEPING

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.

D) TECHNOLOGY

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/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 that 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).

E) LEGISLATION

E1. 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 (EIGN) 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 and PINs.

Authentication - Security measure designed to establish the validity of a transmission, message, or originator, or 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/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) 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/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, and personal identification numbers (PINs).

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.