(1) USDA Memorandum CACFP 07-2007: Update on Electronic Transactions in the CNP

USDA Policy Memo Hyperlink

The following screenshots list some important Q & As and definitions within this policy memo:

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.

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.

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.

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.

WI State Statutes: Chapter 19 - General Duties of Public Official

Subchapter IV - Personal Information Practices

19.62 (5) Definition of Personally Identifiable Information (PII) Webpage Hyperlink

"Personally identifiable information" means information that can be associated with a particular individual through one or more identifiers or other information or circumstances.

19.68 Collection of personally identifiable information from Internet users Webpage Hyperlink

No state authority that maintains an Internet site may use that site to obtain personally identifiable information from any person who visits that site without the consent of the person from whom the information is obtained. This section does not apply to acquisition of Internet protocol addresses.