August 1, 1994

Memorandum

To: Denise Ferris, R.D. Dr. P.H

From: Geri Guerin
Senior Assistant Attorney General

Data: August 1, 1994

Subject: Memorandum Opinion Regarding Computerized Progress Notes

---

Issues:

1. Whether electronic signatures meet the requirements of a "signature" under WIC regulations?

2. Whether computerization features of the STORC system, as proposed, meet federal, state and professional standards regarding confidentiality, security, access control and permanency of records stored?

Short Answer: The Comptroller General of the United States has held that electronic signatures fulfill the characteristics of a signature. Computerization of the STORC system appears to meet or exceed the federal standards for computer data authentication, encryption of signatures, access control and password management. The system appears to have adequate safeguards to protect client confidentiality and to insure permanency of a record once filed in the system. Security and access control are at least equal to that afforded paper records available at a Competent Professional Authority's work area.

Discussion: The Storage, Transfer, Organization and Retrieval of Case files {STORC) system includes, but is not limited to, information regarding food voucher issuance and redemption, nutritional risk conditions, certification and any hearing procedures. Individuals making ink and paper entries in STORC records of nutritional risk conditions and prescribing food packages are required, by § 246.7(h)(7) of WIC regulations, to document such entries by signature. Individuals other than those making these notes may need other information kept in the file for other purposes. The computerized progress notes include a nutritional risk assessment, plan and other notations pertinent to the client's nutritional needs.

According to a November 9, 1993, letter to Ms. Denise V. Ferris from Mr. Peter Santos, Regional Director of the Supplemental Foods Program, a literal interpretation of WIC regulations requires a handwritten signature in STORC records. This interpretation is not

borne out by federal statutes. "Writing" as defined at 1 U.S.C. § 1, includes "printing and typewriting and reproductions of visual symbols." The Comptroller General of the United Stated noted in Decision B-104590, dated September 12, 1951, that a signature could be "any symbol adopted as one's signature when affixed with his knowledge and consent". The Comptroller General subsequently approved the use of electronic encryption devices as a signature machine. 33 Comp. Gen. 297 (1954). The use of an electronic encryption device to certify payment vouchers was approved in Decision B-21603S, dated September 20, 1984. In that decision, the Comptroller General of the United States held that the electronic symbol embraced all of the characteristics of a valid, acceptable signature including uniqueness to the individual, verifiability and sole control. The National Institute -of Standards and Technology (NIST) Special Publication 800-4 (March 1992) recognizes that an electronic signature, like its handwritten counterpart, can be used to identify the originator. It has the added feature, however, of verifying "that information has not been altered after it was electronically signed". Id., at 69. This feature improves data integrity.

Mr. Santos advised that the food and Nutrition Service had plans to develop a policy which clarified that the signature may be by electronic means. The following guidelines were suggested:

> 1. Establish a system for the management and issuance of access codes and signature keys including procedures for changing access codes and signature keys on a periodic basis.

The procedures adopted by the West Virginia WIC program for management and issuance of access codes and signature keys alert users to the confidential and exclusive nature of these codes and keys. Verification is determined by performance of an edit to ensure that the user is authorized. This reduces the possibility of fraud and abuse by requiring verification of identification at the time of data entry. The system integrity is, therefore, at least equal to that of written entries with hand-written signatures.

The system proposed and implemented by the agency allows only the system administrator to change a user's password. The administrator should be directed to reinforce the security and confidentiality requirements to be afforded codes and signature keys at the time new passwords are issued and document this action.

It is recommended that guidelines be developed which require that passwords be changed on a periodic basis, with a minimum requirement that passwords be changed at least once per year. To establish the "sole control" characteristic of a signature, access code and signature key assignment must be unique to each certifying CPA.

2. Establish controls which limit access to information which identifies each CPA's access code and signature key.

Guidelines must require that code and key lists not be reproduced once codes and keys are entered and that all lists be kept confidential and secured under lock.

3. Require CPAs to sign an affidavit which states that he/she:

--understands that each time he/she enters his/her access code and signature key, it represents his/her documentation of the nutritional risks identified, WIC food package prescribed, and/or nutrition education provided;

--is aware of the confidential nature of the access code and signature key;

--will not share his/her access code or signature key with any individual, including applicants, participants, and other WIC clinic staff;

--will take all precautions and efforts necessary, to the maximum extent possible, to protect the visual observation of the access code and signature key when entering them into the system,- and,

--understands that appropriate action (as determined by the State or local agency) may be taken against them if such security measures are breached.

Current guidelines meet this requirement. CPA's must sign an affidavit acknowledging awareness of the security required to protect the integrity of access codes and signature keys and agreeing to take all reasonable precautions to maximize the security of the access codes and signature key assigned to them. Local agencies are given the responsibility to establish disciplinary action for failure to comply with security requirements. The affidavit acknowledges receipt of an individualized access code and signature key for the CPA's confidential, exclusive and solitary use and that such use has the same force and effect as a signature for documentation purposes.

The suggestions made by Mr. Santos in the above-referenced letter appear to cover all state and federal requirements for the protection of confidential and sensitive information. The system is not required to meet the NIST digital signature standards because the data is not being sent outside the agency of origination by electronic or other means. The system does utilize an algorithm for password encryption to prevent users from viewing

each others password and/or identification codes. A signature algorithm feature will need to be added if STORC requires electronic transmission of data to any federal agency in the future. No other standards were found which require additional safeguarding of access to the informational data base.

Concerns were also raised regarding state liability and legal ramifications if unauthorized use of a CPA's access and signature codes result in the creation of bogus cases and issuance of WIC food instruments. Additional safety devices built into the West Virginia WIC system minimize the potential for unauthorized use and protect the integrity, authenticity and verifiability of entered information. The West Virginia WIC system utilizes the following computer security features described in NIST Special Publication 800-4:

Identification and Authentication through use of a password.

Discretionary access.

Electronic Signature which provides identification of the originator, nonrepudiation and information integrity.

Key management through use of a secret codes with cryptographic features.

Auditing at the time of saving information to the system.

Data authentication to verify that data has not been modified at some later time.

Only CPAs and local agency directors have authority to enter, retrieve or view progress notes. Other users are limited in the functions which may be performed. The system identifies the user through the sign-in process.

After a note is completed, the user must deliberately "save" the note to the system. Knowledge of the system's operation is needed to accomplish this task. In addition, when the user initiates the "save" function, an edit is performed to ensure that the user identification code of the person desiring to save the note is that of a CPA or local director, if identification is confirmed, the Note is then electronically stamped with the user's identification and saved. In this manner, the information is keyed to a particular user. Keying the data in this way improves the program's ability to investigate fraudulent use of the program by tying the bogus ease or issuance to a particular user code and anyone with potential unauthorized access to that code.

The system has been designed so that no user may modify or delete a progress none that has been saved. After a note has been entered

and saved, it *is* recorded in the system and is not visible on the monitor unless accessed by an authorized CPA or local director. Instead of increasing state liability, these features should reduce the potential for fraud and liability resulting from unauthorized access.

The West Virginia Code does not have any specific provisions governing confidentiality of WIC records or the use of computerized records in the storage of public assistance program records.

This Memorandum Opinion does not analyze the legality of other aspects of record computerization which are not specifically mentioned herein.