

## **2.19 Electronic Signatures for the Competent Professional Authority (CPA)**

---

### **POLICY:**

The CPA may use an electronic signature in lieu of a hand-written one for documenting an individual's nutritional risk condition(s), food package prescription and clinical assessment/plan.

### **PROCEDURE:**

#### **A. Accountability and Security**

The State Agency must ensure adequate accountability and security measures.

1. The State Agency will 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.
2. The State Agency will establish controls which limit access to information which identifies each CPA's access code and signature key.
3. The State Agency will require that CPAs sign an **Affidavit** before a notary public (see **Policy 2.03, Competent Professional Authority**).

#### **B. Electronic Signatures Meet Signature Requirements**

As outlined in the **Memorandum Opinion Regarding Computerized Progress Notes**, dated August 1, 1994 by Geri Guerin, Senior Assistant Attorney General (WV) (see **Attachment #1 2.19**):

1. The Comptroller General of the United States has held that electronic signatures fulfill the characteristics of a signature.
2. 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.
  - a) The system appears to have adequate safeguards to protect client confidentiality and to ensure permanency of a record once filed in the system.
  - b) Security and access control are at least equal to that afforded paper records available at a CPA's work area.
  - c) The STORC system requires a user to change his/her password every thirty (30) days.

## **2.19 Electronic Signatures for the Competent Professional Authority (CPA)**

---

### **C. Responsibilities of the System Administrator**

The System Administrator will be responsible for the security and confidentiality regarding codes and signature keys.

1. The STORC system allows only the System Administrator to change a user's password.
2. The System Administrator will ensure that once codes and keys are entered, that this information is not reproduced and that the original hard copy of these lists be kept confidential and secured under lock.
3. The System Administrator will be responsible for reinforcement of the security and confidentiality requirements afforded codes and signature keys at the time new passwords are issued and document this action.

### **D. Affidavit**

The CPA must sign an Affidavit before a notary public acknowledging 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 (see **Policy 2.03, Competent Professional Authority**).

### **E. Security Against Unauthorized Use of Access and Signature Codes**

To ensure against unauthorized use of a CPA's access and signature codes which could result in the creation of bogus cases and unauthorized issuance of food instruments, the STORC system uses computer security features described in NIST Special Publication 800-4 (see **Attachment #1 2.19, Memorandum Opinion Regarding Computerized Progress Notes**).

### **REFERENCES:**

1. WIC Regulations 246.7, Certification of Participants

### **ATTACHMENTS:**

1. Memorandum Opinion Regarding Computerized Progress Notes