The eCCF in Federally Regulated Workplace Drug Testing Programs: Security, Confidentiality, and Integrity of Drug Test Information

In accordance with the Government Paperwork Elimination Act (GPEA) and in an effort to reduce burden, the Department of Health and Human Services (HHS) has authorized the use of an electronic Federal Custody and Control Form (eCCF) for federal workplace drug testing programs. As with the current paper Federal CCF, HHS has established standards and oversight procedures to ensure the authenticity, integrity, and confidentiality of drug test information when a Federal eCCF is used. This paper describes Federal CCF requirements, the procedures that HHS will use to verify compliance with those requirements through the National Laboratory Certification Program (NLCP), and HHS guidance for agencies and service providers choosing to use a Federal eCCF for regulated workplace drug testing. An overview of Federal eCCF use is included at the end of the paper.

Federal CCF Requirements

Both the HHS Guidelines and the DOT Regulations allow transmission of the Federal CCF by various electronic means and both specify that service providers must ensure the security of the data transmission and limit access to any data transmission, storage, and retrieval system.

The Mandatory Guidelines for Federal Workplace Drug Testing Programs (Guidelines; effective October 1, 2010; 73 FR 71858) includes records security, CCF distribution, and result reporting requirements applicable to the use of a Federal eCCF. Some relevant sections are:

- Section 11.7:   *What security measures must an HHS-certified laboratory maintain?*
- Section 11.19(n) and (o): *What are the requirements for an HHS-certified laboratory to report a test result?*
- Section 12.7:   *What security measures must an HHS-certified IITF maintain?*
- Section 12.15(e) and (f): *What are the requirements for an HHS-certified IITF to report a test result?*
- Section 14.5: *Who receives the split specimen result?*

The Department of Transportation (DOT) also includes requirements in the Procedures for Transportation Workplace Drug and Alcohol Testing Programs (49 CFR Part 40, updated May 4, 2012) that are applicable to the use of a Federal eCCF. Some relevant sections are:

- Section 40.97: *What do laboratories report and how do they report it?*
- Section 40.185: *Through what methods and to whom must a laboratory report split specimen results?*
- Section 40.345: *In what circumstances may a C/TPA act as an intermediary in the transmission of drug and alcohol testing information to employers?*
- Section 40.351 *What confidentiality requirements apply to service agents?*
- Appendix F: *Drug and Alcohol Testing Information that C/TPAs May Transmit to Employers*

Procedures to Verify Compliance with Federal CCF Requirements

Initial Review

Before a Federal eCCF can be used for regulated specimens, an HHS-certified test facility must submit a detailed plan and proposed standard operating procedures (SOPs) for the eCCF system for HHS review and approval (through the NLCP).

Ongoing Review

The review of validation records, specimen records, SOPs, staff training records, and practices associated with the eCCF will be part of the NLCP inspection process.

The current NLCP Checklist and Manual include requirements that are applicable to the use of a Federal eCCF such as requirements for CCF annotation, computer system validation, security, electronic records, electronic reports, electronic signatures, audit trails and logs, system monitoring, incident response, and disaster recovery. The program requires:

- The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying upon request of authorized parties (e.g., the MRO, federal agency, or SAMHSA)

- Protection of records to enable accurate and ready retrieval through the records retention period

- Limiting system access to authorized individuals

- Secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete records (changes should be evident when reviewing the original record, and any electronic or paper copy of the original record)

- Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand

- Measures to ensure the accuracy and security of electronically transmitted results

- Verification that confidentiality is maintained at the receiving end of electronically transmitted reports. Laboratories must have on file copies of letters from the MRO attesting to the security of off-site receiving devices and must verify the MRO information concerning the security of receiving devices on an annual basis. The RP of each HHS-certified laboratory must ensure the security and confidentiality of reports sent from their laboratory to MROs. They must ensure that records documenting the confidentiality and security of any electronically transmitted result (e.g., letters attesting

to MRO compliance with security requirements), are properly maintained, whether they be stored on- or off-site.

Relevant Checklist questions and Manual pages include, but are not limited to:

- **Checklist Question D-2:** *Does the custody and control form (CCF) provided by the laboratory to its federally regulated clients satisfy all the requirements of the OMB-approved CCF?* **NLCP Manual Page: D-2**

- **Checklist Question D-4:** *Does the individual opening the leak-resistant plastic bag containing the specimen bottles and CCF (i.e., breaking the secondary seal) properly document receipt of the specimen on the CCF in accordance with Federal requirements?* **NLCP Manual Pages: D-2 - D-3**

- **Checklist Question D-6b:** *When sending a specimen or aliquot to another HHS-certified laboratory for retesting, does the laboratory send a copy of the original CCF to the receiving laboratory?* **NLCP Manual Pages: D-4 – D-5**

- **NLCP Manual Section F:** General Comments
  NLCP Manual Page: F-1

- **Checklist Question F-1:** *Does the laboratory use acceptable security procedures to control and document who has access to the HHS-certified drug testing laboratory and to each drug testing area?* **NLCP Manual Page: F-1**

- **Checklist Question F-4:** *Does the laboratory store records in an off-site location?* **Checklist Question F-4b:** *Is access to the records at the off-site storage facility limited to appropriate laboratory personnel?* **NLCP Manual Page: F-3**

- **Checklist Question I13a.** (This question addresses the laboratory's contingency plan for cessation of regulated testing and lists required elements, some of which are applicable to records) *Does the contingency plan include: Disaster preparation plan (e.g., personnel safety procedures, procedures for securing and protecting specimens and records, procedures for backing up data on analytical instruments and laboratory computers, procedures for shutting down instruments); Plan for maintaining existing specimens and records?* **NLCP Manual Pages: I-5 – I-7**

- **NLCP Manual Section M:** General Comments
  NLCP Manual Page: M-1

- **Checklist Question M-1e.** *Prior to reporting results to the MRO for negative and rejected specimens, does **one** certifying technician or certifying scientist certify his/her review on the Federal CCF as required by the regulated program?* **NLCP Manual Pages: M-1 – M-2**

- **Question M-6:** *Does the laboratory forward a copy of a properly completed Federal CCF to the MRO for a primary specimen reported as positive, adulterated, substituted, invalid, or rejected?* **NLCP Manual Page: M-7**

- **Question M-7:** *Does the laboratory forward a copy of a properly completed Federal CCF and Laboratory Split Specimen Report to the MRO for a split specimen?* **NLCP Manual Pages: M-7 – M-8**

- **Checklist Question M-10.** *Are specimen results transmitted electronically?*
    *If **YES,***
    a.   *Are security measures acceptable to ensure the confidentiality of electronically transmitted results?*
    b.   *Does the laboratory obtain a letter attesting to the security of receiving devices from each MRO receiving computer-generated electronic reports?*
    c.   *If the letters are maintained off-site (e.g., another corporate facility), has the RP verified that the laboratory has a letter from each MRO receiving computer-generated electronic reports?*
    d.   *Does the laboratory verify and update MRO information concerning the security of receiving devices on an annual basis?*
    e.   *If the verification documents are maintained off-site, has the RP verified the annual updating of MRO information concerning security of receiving devices?*
    NLCP Manual Pages: M-10 – M-11

- **Checklist Question O-5a.** (This question concerns client services personnel who are not under the supervisory authority of the RP and have access to specimen information and laboratory results.) *Is there documentation of training by an RP concerning the handling of forensic records and NLCP issues associated with confidentiality?* **NLCP Manual Page: O-3**

- **NLCP Manual Section P:** General Comments
  NLCP Manual Page: P-1

- **Checklist Question P-2:** *Have significant changes been implemented since the previous inspection, or are significant changes planned before the next inspection?*
    *If **YES**,*
    a.   *Did the laboratory develop a plan for implementing the changes?*
    b.   *Are the changes properly validated?*
    c.   *Are security measures properly implemented?*
    d.   *Are personnel properly trained?*
    NLCP Manual Page: P-2

- **Question P-3:** *Does the laboratory or IT department have policies and procedures for laboratory computer systems and information systems?* **NLCP Manual Pages: P-2 – P-4**

- **NLCP Manual Section P:** General Comments on Computer and Software Validation
  NLCP Manual Page: P-4

- **Checklist Question P-4:** *Are the computer and software systems validated?*
  NLCP Manual Pages: P-4 – P-5

- **Checklist Question P-4a:** *Are the validation experiments properly documented and available for review?* **NLCP Manual Page: P-6**

- **Checklist Question P-5:** *Does the laboratory have software and configuration version control procedures?* **NLCP Manual Pages: P-6 – P-7**

- **Checklist Question P-6:** *Does the laboratory have policies and procedures that address the useful life of software and hardware?* **NLCP Manual Page: P-7**

- **Checklist Question P-7:** *Are all required software patches and upgrades implemented, validated, and documented?* **NLCP Manual Page: P-6**

- **Checklist Question P-9:** *Does the laboratory review and document its computer and information systems security at least annually?* **NLCP Manual Page: P-8**

- **Checklist Question P-10:** *Is physical access to computer system hardware limited to appropriate personnel?* **NLCP Manual Pages: P-8 – P-9**

- **Checklist Question P-11:** *Are procedures in place to change or revoke physical access when personnel are reassigned or are no longer employed by the organization?* **NLCP Manual Page: P-9**

- **Checklist Question P-14:** *Does the laboratory use an appropriate user identification and authentication system for network operating systems, LIMS, and/or database systems that connect to or provide access to the LIMS?*
  *If **YES**,*
  a. *Does the computer system deny access to users after multiple failed attempts to access the system?*
  b. *Does the system automatically prevent unauthorized access if a user session is left unattended?*
  c. *Does the system allow user identification and passwords to be inactivated without losing the historical record?*
  d. *Are procedures in place for expeditiously changing or revoking access when personnel are reassigned or are no longer employed by the organization?*
  e. *Do user passwords expire at least every six months?*
  f. *Does the system require complex passwords (e.g., minimum length, and combinations of letters, numbers, and symbols)?*
  NLCP Manual Pages: P-10 – P-11

- **Checklist Question P-15:** *Does the laboratory limit computer access to specimen records to appropriate personnel?* **NLCP Manual Page: P-11**

- **Checklist Question P-16:** *Does the laboratory limit access to critical system functions to appropriate personnel?* **NLCP Manual Page: P-11**

- **Checklist Question P-17:** *If remote access is used to allow access to the LIMS from an external network connection, is it limited to appropriate personnel?* **NLCP Manual Page: P-12**

- **Checklist Question P-18:** *Does the laboratory use wireless network(s)? If YES,*
    a. *Is each wireless network secured?*
    b. *Has the laboratory verified and documented the security of each wireless network?*
  NLCP Manual Page: P-12

- **Checklist Question P-19:** *Do specimen records or other records related to specimen processing exist only in an electronic form? If YES,*
    a. *Does the laboratory have procedures to prevent undetected modification of the electronic records?*
    b. *Can electronic records be retrieved and assembled into a full documentation package to support a drug test result?*
    c. *Can electronic data be retrieved through the entire record retention period regardless of any changes to the laboratory computer and information system?*
  NLCP Manual Pages: P-13 – P-14

- **Checklist Question P-20** *Are archived electronic records stored in a proprietary format? If YES, a. Does the laboratory maintain retired software versions?* **NLCP Manual Page: P-14**

- **Checklist Question P-21:** *Does the laboratory send electronic reports to the MRO?*

  If YES,
    a. *Are electronic reports transmitted in a format that prevents interception and alteration?*
    b. *Has the laboratory verified and documented the accuracy of electronic reports?*
  NLCP Manual Page: P-15

- **Checklist Question P-22:** *Does the laboratory use an Internet-based reporting method? If YES,*
    a. *Has the laboratory evaluated the security of the Internet applications used for reporting?*
    NLCP Manual Pages: P-15 – P-16

- **Checklist Question P-23:** *Does the laboratory use a third party report provider to report test results to an MRO? If YES, a. Is the report data secured in a manner that allows only the MRO to have access to the specimen results?*

NLCP Manual Page: P-16

- **Checklist Question P-24:** *Does the laboratory use electronic signatures?*
  *If **YES**,*
  - a. *Does the laboratory verify the identity of the individual and obtain a certification statement from the individual?*
  - b. *Is the electronic signature properly secured?*
  - c. *Are the printed name and date, and the meaning associated with an electronic signature included when it is executed?*
  - d. *Is the electronic signature bound to the associated electronic record?*

  NLCP Manual Pages: P-16 – P-17

- **Checklist Question P-25:** *Is the ability to amend computer-resident data that changes the results or identification of reported specimens limited to appropriate personnel?* **NLCP Manual Page: P-18**

- **Checklist Question P-26:** *Do audit trails include the following? If **NO**, check the deficient area(s):*
  - ___ a. *The user identification, date, and original and revised data*
  - ___ b. *A link between individual user identities and various tasks documented on the computer system*
  - ___ c. *A human readable format*
  - ___ d. *Mechanism for searching by specimen ID, user, date range, and transaction type*
  - ___ e. *Audit trail protection from edit*

  NLCP Manual Pages: P-18 – P-19

- **Checklist Question P-27:** *Does the laboratory have procedures for monitoring system performance and for responding to problems?*
  NLCP Manual Page: P-19

- **Checklist Question P-28:** *The laboratory must have procedures to protect its systems from computer viruses. Do the procedures include the following? If **NO**, check the deficient area(s):*
  - ___ a. *Up-to-date anti-virus software and virus definition files*
  - ___ b. *Periodic virus scans (at least weekly)*
  - ___ c. *Documentation of anti-virus measures*

  NLCP Manual Pages: P-19 – P-20

- **Checklist Question P-29a** *Does the laboratory have procedures to address potential sources of disaster? If **NO**, check the deficient area(s):*
  - ___ a. *Regularly perform backups of specimen records and other critical system functions.*
  - ___ b. *Secure backups and limit access to appropriate personnel.*
  - ___ c. *Store backups in an area that is environmentally satisfactory for the media.*
  - ___ d. *Document backups.*
  - ___ e. *Have emergency power equipment or an acceptable alternate plan for dealing*

with prolonged power failure.
NLCP Manual Pages: P-20 – P-21

- **Checklist Question P-30:** *Does the laboratory have procedures for recovering the laboratory computer systems in the event of disaster?*
  *If **YES**, does the laboratory*
  - a.   *Periodically test and evaluate its disaster recovery procedures?*
  - b.   *Document the results of the test?*
  - c.   *Verify the accuracy of recovered data?*
  - d.   *Document when disaster recovery procedures are utilized?*
  NLCP Manual Page: P-21

- **Checklist Question P-32:** *Does the laboratory have hardware and software documentation?* **NLCP Manual Page: P-22**

- **Checklist Question R-1:** *Have laboratory staff properly completed external chain of custody documents for a) Routine specimens? b) Split specimens?*
  NLCP Manual Pages: R-1 - R-3

- **Checklist Question R-9d:** *Is there evidence that the certifying scientist who reported results to the MRO for positive, adulterated, substituted, and invalid specimens certified his/her review by signing the Federal CCF?***NLCP Manual Pages: R-5 – R-7**

- **Checklist Question R-11** *Are all laboratory records that support specimen test results retained by the laboratory for at least two years?* **NLCP Manual Page: R-7**

- **NLCP Manual Section U:** General Comments
  NLCP Manual Page: U-1

- **Checklist Question U-4** *Are laboratory reports for split specimens in accordance with NLCP guidance (see the example Split Specimen Report form and Tables U-2 and U-3)? Do the laboratory's Split Specimen Reports contain all required elements?* **NLCP Manual Pages: U-5 – U-6**

- **Checklist Question U-5:** *When specimen identification or results were changed for a reported specimen, did the laboratory send a **corrected** report to the MRO? If **YES**,*
  - a.   *Do specimen records clearly specify when a corrected report was sent to the MRO?*
  - b.   *Were the corrected reports acceptable?*
  NLCP Manual Pages: U-6 - U-7

Additional questions will be added to the Checklist, with explanatory comments included in the NLCP Manual describing specific program requirements for a Federal eCCF system and addressing a test facility's procedures and practices for use of an eCCF.

HHS Guidance

1. Guidance for using the Federal Custody and Control Form

HHS has updated the Guidance for using the 2010 Federal Custody and Control Form to address the use of a Federal eCCF. This will be posted on the SAMHSA Drug Testing website.

2. HHS Urine Specimen Collection Handbook for Federal Agency Workplace Drug Testing Programs

3. HHS Medical Review Officer (MRO) Manual for Federal Agency Workplace Drug Testing Programs

HHS has added wording addressing the roles of the collector and MRO using eCCFs, to emphasize maintenance of donor confidentiality and protection of personal identifying information (PII) obtained on the Federal CCF. The Collector Handbook and MRO Manual are focused on collection procedures and on MRO interpretation and reporting duties, respectively, and not on requirements of computerized systems which may be used during collections and review/reporting.

4. NLCP Checklist and Manual: NLCP Manual for Urine Laboratories, Section P (Laboratory Computer Systems)

As noted above, additional questions will be added to Section P of the Checklist, with explanatory comments included in the NLCP Manual describing specific program requirements for a Federal eCCF system. The NLCP will provide Section P of the Manual describing specific program requirements to entities interested in developing and implementing a Federal eCCF system. Note: the NLCP has separate checklists and manuals for laboratories and IITFs.

5. The NLCP will offer an online training course on requirements for a Federal eCCF.

Overview of Federal eCCF Use

At a minimum, the eCCF system must be set up with the collection site and the test facility. If an eCCF is provided to the MRO, the eCCF system must be coordinated with the MRO also.

Electronic CCF systems are currently used in non-regulated testing. HHS foresees similar processes will be used for regulated testing. The attached slides give an overview of a process using the current paper Federal CCF and two options using a Federal eCCF. Other systems may be acceptable: proposed systems must be reviewed by HHS prior to implementation. One eCCF option shown is a paperless system in which the CCF is sent to the test facility solely as an electronic document (i.e., CCF information and data in digital form). The other is a combination electronic/paper system. In the combination system, the collector initiates the eCCF and maintains the signed eCCF as an electronic document, but sends a printout of Copy 1 with the specimen to the test facility, which is used by the laboratory to document receipt and report the

specimen. The collector also provides the CCF to the other parties (e.g., printout of Copy 2 given to the donor or legible image emailed to the donor; eCCF Copy 2 provided to the employer and MRO). Note: A third party may maintain files for secure access by the laboratory/MRO/employer.

The collector will follow the same required procedures for specimen collection currently used with a paper CCF. The collector and donor will sign the Federal eCCF using electronic signatures. As with a paper CCF, the donor's refusal to sign the eCCF is not a reason for rejection. The collector documents the refusal and continues. The collector will distribute the Federal CCF to the other parties (test facility, MRO, employer, and donor).

Paperless eCCF system: When the Federal eCCF is sent to the test facility only as an electronic document, additional steps are needed to facilitate linkage of the specimen package to the Federal eCCF. The collector must either 1) include a printed copy of the Test Facility copy (i.e., Copy 1) of the Federal CCF with the specimen; or 2) apply a label to the outside of the specimen package, with the specimen identification number, test facility name and contact information, and collection site name and contact information. The accessioner at the test facility that receives the specimen package from the collection site continues the specimen chain of custody on the Federal eCCF. In addition to documenting receipt of the specimen using an electronic signature, the accessioner documents the condition of the primary specimen seal and releases custody of the specimen (e.g., to a storage area). Note: If a printed copy of Copy 1 is also included in the specimen package, the accessioner may, but is not required to, annotate this form. This is only a replica of the Federal CCF which contains the collector's electronic signature and is not the chain of custody for the specimen.

Combination Electronic/Paper eCCF system: In a combination electronic/paper system, the collector uses the Federal eCCF to document the collection process and start the specimen chain of custody, and maintains the signed Federal eCCF as an electronic document. A printout of the eCCF (Copy 1) is sent to the test facility with the specimen. The collector also provides the CCF to the other parties. For example, the donor may choose to receive a printout of the eCCF (Copy 2) at the end of the collection or provide an email address to receive a legible image of the eCCF. The collector provides Copy 2 of the eCCF to the employer and MRO. Various methods may be used. For example, parties may access the Federal eCCF via a secure, password-protected website, receive an eCCF printout (e.g., by fax, mail, transporter), or receive an electronic file (i.e., legible image of the CCF).