PharmaSUG 2013 - Paper MS06

# Managing 21 CFR Part 11 Compliance:

# Using Checksums on Opens Systems

Carey Smoak, Roche Molecular Systems, Inc., Pleasanton, CA
Mario Widel, Roche Molecular Systems, Inc., Pleasanton, CA

## ABSTRACT

Generally, closed systems are encouraged in order to ensure compliance with 21 CFR Part 11 regulations. Databases with audit trails are typically considered to be examples of closed systems, which are designed to ensure the authenticity, integrity, electronic records confidentiality while the signer cannot repudiate the signed record as not genuine. Open systems do not have these capabilities.

In this paper the authors will show how to address record authenticity and integrity using checksums. They will describe the managing of electronic lab instrument data in an open system. Checksums can be used to ensure that data has not been accidentally modified during the process of acquisition from the lab instrument to its final destination as a SAS® dataset on a secure server. While the lab instrument data is not maintained in a database with an audit trail, it is shown how the spirit of 21 CFR Part 11 compliance is kept with respect to data integrity and record authenticity.

## INTRODUCTION

21 CFR Part 11 compliance (see Appendix A) is an important issue for pharmaceutical, biotech and medical device companies. Section 11.3 defines closed and open systems as follows:

> *Closed system* means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.
>
> *Open system* means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

Section 11.30 (see Appendix A) further defines the controls for open systems:

> Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances**, record authenticity, integrity, and confidentiality**.

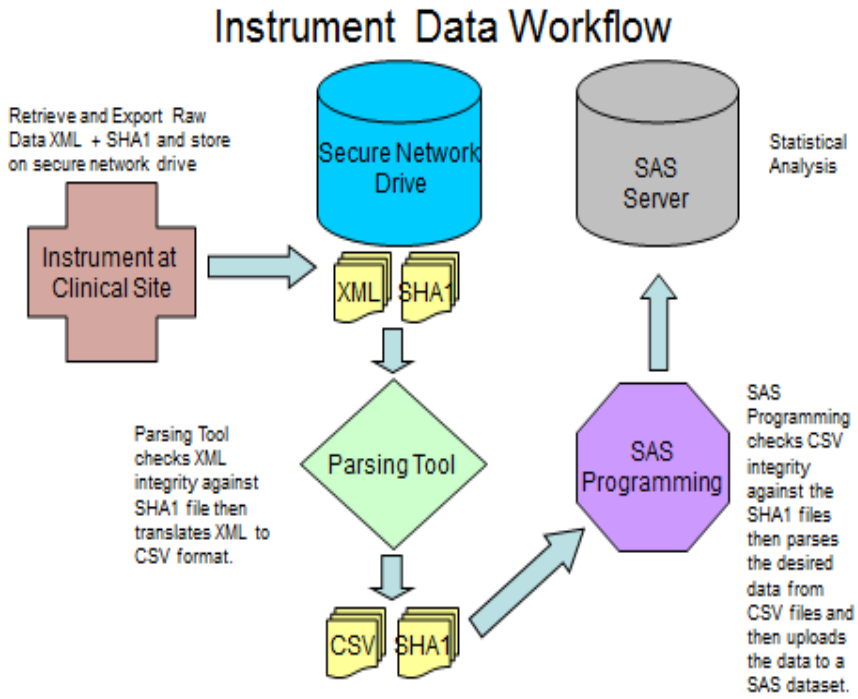
This paper will show when and when not to use checksums address compliance issues on record authenticity, integrity and confidentiality in an open system.

## EXAMPLE 1: CHECKSUMS IN AN OPEN SYSTEM

### DESCRIPTION

Figure 1 below shows the use of checksums in an open system to verify data integrity. For further information on the use of checksums in the healthcare industry please see the paper by Smoak, Widel and Truong (2012A, 2012B). In this open system, a user connects remotely (at the sponsor site) to a lab instrument (the clinical study site) and exports the lab data as an .xml file. The system is designed so that when the .xml file is exported a checksum is run on the .xml file. In this example, the checksum is a .sha1 file. The user then places the .xml and .sha1 files on a secure network drive at the sponsor site. A parsing tool then checks the .sha1 file to ensure that the .xml file has not been modified during the transmission. The parsing tool then converts data from the .xml file into a .csv file. When the .csv file is outputted from the parsing tool, it generates a checksum for the .csv file (a new .sha1 file). A SAS program then checks the .sha1 file for the .csv file to ensure that the .csv file has not been modified. The SAS program then imports the .csv into a SAS dataset on a secure server with limited access.

**Figure 1. Use of Checksums in an Open System**




### COMPLIANCE

Does the open system described meet the spirit of 21 CFR Part 11 compliance? From the time that the raw data is exported until it resides on the SAS server it is in a secure environment with limited access. The use of checksums ensures correct transmission of data. Moreover, this process of exporting data from the lab instrument to import of the data into SAS datasets has been validated with appropriate test cases. Therefore, adequate procedures are in place in this open system to ensure that from the point of creation of the electronic records (the lab data) to its receipt on the secure server (as SAS datasets) that the data is being handled in a manner that is in the spirit of 21 CFR Part 11 compliance.

What would be the alternative to this open system? The .csv files could be uploaded into a clinical database. But the initial steps of exporting the data and running the parsing tool would still apply. Thus 21 CFR Part 11 compliance applies to these initial steps of exporting the lab data and the parsing tool using checksums in either case (importing the .csv file into SAS datasets on a secure versus uploading the .csv files into a clinical database). The main advantage of the clinical database is that the data would be in a closed system with an audit trail. While this is compelling, in the absence of a data upload tool (into a clinical database), this open system is an alternative which is still in the spirit of 21 CFR Part 11 compliance.

Thus checksums ensures data integrity in an open system, but only for unintended changes. For the detection of malicious changes and authenticity checksums can be used, but they need to be transmitted in a secure manner. For example, in the figure above if the parsing tool placed the checksum in a secure location (separate from the .csv file) then malicious changes could be detected.

In the example in the above figure confidentiality was not a consideration.

## EXAMPLE 2: NO CHECKSUMS IN AN OPEN SYSTEM

### DESCRIPTION

Sporon-Fielder, Lassen and Lundbeck (2002) have pointed out that ”the standard consolidated SAS environment is non compliant with FDA 21 CFR part 11.” These authors do point out that some people will debate whether or not SAS is an open or closed system, but based on their definition of an open system, SAS can maintain 21 CFR Part 11 compliance in an open system based on the following criteria:

- Security
- Auditing
- Data Management
- Generation of Human Readable Electronic Records
- System Management Documentation

## COMPLIANCE

Thus this is another example of a commonly used open system in pharmaceutical, biotech and medical device companies. If sponsor companies and regulatory authorities can accept SAS as being 21 CFR Part 11 compliant in an open system then the acceptance of other open systems can be valid as long as the spirit of compliance is maintained.

## REGULATORY COMPLIANCE

A key question is can an open system pass a Regulatory audit? Generally, closed systems are thought of being 21 CFR Part 11 compliant. Braun (2010) mentions three keys that an auditor would use to assess compliance with regulatory requirements:

1. CVs, job descriptions, and training records to provide assurances that staff are qualified to perform the proposed activity.
2. Applicable SOPs and plans to provide assurances that the activity is conducted in a consistent manner and in line with regulatory requirements.
3. Documents and records generated during the activity to provide assurances and/or evidence to clarify and to support the auditor's assessment.

In the spirit of 21 CFR Part 11 compliance, an open system can meet these requirements and pass an auditor's inspection. Assurances can be provided that people are properly trained on the open system; SOPs and plans can provide assurances that data in the open system is handled in a consistent manner and in line with regulatory requirements and documentation and records can be made available to provide assurances that to support an auditor's assessment of the open system.

## CONCLUSION

Open systems can be perfectly compliant, but sponsors are responsible for ensuring that they satisfy all of the criteria, namely integrity, record authenticity and confidentiality. Vendors can offer required technical elements of a compliant system, but it is not compliant out of the box. It is the responsibility of the sponsor or user to implement the procedural and administrative controls to ensure compliance (see reference for Frequently Asked Questions for 21 CFR Part 11 Compliance). For example, SAS provides tools for Installation and Operational Qualification, but the sponsor must use the validation tools to achieve compliance (Smoak, Truong 2011).

## REFERENCES

21cfrpart11.com. Frequently Asked Questions. Available at: http://www.21cfrpart11.com/pages/faq/index.htm

Ryan, Barry. 2010. "Database/biostatistics audits: from the auditor's perspective." Pharmaceutical Programming 3:5-7.

Smoak Carey; Truong, Sy. 2011. "Managing the Validation and Migration from SAS 9.13 to 9.2 on a New Server." *Proceedings of the Pharmaceutical Industry SAS Users Group*, Nashville, TN. Available at: http://www.lexjansen.com/pharmasug/2011/ma/pharmasug-2011-ma02.pdf

Smoak Carey; Widel Mario; Truong Sy. 2012A. "Checksum Please: A Way to Ensure Data Integrity." *Proceedings of the Pharmaceutical Industry SAS Users Group,* San Francisco, CA. Available at: http://www.lexjansen.com/pharmasug/2012/TA/PharmaSUG-2012-TA01.pdf

Smoak Carey; Widel Mario; Truong Sy. 2012B. "The use of checksums to ensure data integrity in the healthcare industry." Pharmaceutical Programming 5:38-41.

Sporon-Fielder Gustav; Lassen Marie; Lundbeck H. 2002. "SAS Coexistence with FDA 21 CFR Part 11, How Far Can We Get?" *Proceedings of the Pharmaceutical Industry SAS Users Group*, Salt Lake City, UT. Available at: http://www.lexjansen.com/pharmasug/2002/proceed/fdacomp/fda05.pdf

Wilson, Steven A. 2004. "Why SAS is the Best Place to Put Your Clinical Data." *Proceeding of the 29th SAS Users Group International*, Montreal, Canada. Available at: http://www2.sas.com/proceedings/sugi29/112-29.pdf

## CONTACT INFORMATION

Your comments and questions are valued and encouraged. Contact the author at:

Carey Smoak
Senior Manager, SAS Programming
Roche Molecular Systems, Inc.
4300 Hacienda Drive
Pleasanton, CA 94588
E-mail: carey.smoak@roche.com

Mario Widel
Manager, SAS Programming
Roche Molecular Systems, Inc.
4300 Hacienda Drive
Pleasanton, CA 94588
E-mail: mario.widel@roche.com

SAS and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration.

Other brand and product names are trademarks of their respective companies.

# APPENDIX A

**[Code of Federal Regulations] [Title 21, Volume 1]**
**[Revised as of April 1, 2012] [CITE: 21CFR11**]

TITLE 21--FOOD AND DRUGS CHAPTER I--FOOD AND DRUG ADMINISTRATION

DEPARTMENT OF HEALTH AND HUMAN SERVICES SUBCHAPTER A--GENERAL

PART 11ELECTRONIC RECORDS; ELECTRONIC SIGNATURES

**Subpart A--General Provisions**

Sec. 11.1 Scope.

(a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

(b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.

(c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically except by regulation(s) effective on or after August 20, 1997.

(d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with 11.2, unless paper records are specifically required.

(e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.

(f) This part does not apply to records required to be established or maintained by 1.326 through 1.368 of this chapter. Records that satisfy the requirements of part 1, subpart J of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

[62 FR 13464, Mar. 20, 1997, as amended at 69 FR 71655, Dec. 9, 2004]

Sec. 11.2 Implementation.

(a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.

(b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:

(1) The requirements of this part are met; and

(2) The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are
acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.

Sec. 11.3 Definitions.

(a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in

this part.

(b) The following definitions of terms also apply to this part:

(1)*Act* means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)).

(2)*Agency* means the Food and Drug Administration.

(3)*Biometrics* means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.

(4)*Closed system* means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

(5)*Digital signature* means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

(6)*Electronic record* means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

(7)*Electronic signature* means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

(8)*Handwritten signature* means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.

(9)*Open system* means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

Sec. 11.10 Controls for closed systems.

Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.

(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.

(d) Limiting system access to authorized individuals.

(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.

(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

(g) 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.

(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.

(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.

(k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.

(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development

and modification of systems documentation.

Sec. 11.30 Controls for open systems.

Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

Sec. 11.50 Signature manifestations.

(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

(1) The printed name of the signer;

(2) The date and time when the signature was executed; and

(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).

Sec. 11.70 Signature/record linking.

Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.

**Subpart C--Electronic Signatures**

Sec. 11.100 General requirements.

(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual`s electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.

(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 12420 Parklawn Drive, RM 3007 Rockville, MD 20857.

(2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer`s handwritten signature.

Sec. 11.200 Electronic signature components and controls.

(a) Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an
identification code and password.

(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.

(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.

(2) Be used only by their genuine owners; and

(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone

other than their genuine owners.

Sec. 11.300 Controls for identification codes/passwords.

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.

(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

(c) Following loss management procedures to electronically de-authorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.

(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.

(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.

**Authority:** 21 U.S.C. 321-393; 42 U.S.C. 262.
**Source:** 62 FR 13464, Mar. 20, 1997, unless otherwise noted.
http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfCFR/CFRSearch.cfm?CFRPart=11&showFR=1 – revised April 1, 2012.