Supplement to the Guidance for Electronic Data Capture in Clinical Trials

January 10, 2012

Drug Evaluation Committee,
Japan Pharmaceutical Manufacturers Association

Note: The original language of this document is Japanese, and in the event that a discrepancy arises between interpretations of this English version and the original version, the original Japanese version shall govern.

Table of Contents

Introduction

In November 2007, the Drug Evaluation Committee of the Japan Pharmaceutical Manufacturers Association issued the "Guidance for Electronic Data Capture in Clinical Trials," as a voluntary guidance on requirements to be met in the electronic capture of clinical trial data[1] ("Guidance 2007").

The scope of Guidance 2007 was limited to the data entered at the sites by EDC systems (eCRF), related audit trails, and electronic data obtained from central laboratories etc. Recently, the implementation of the Electronic Patient Reported Outcomes (ePRO) systems, which were not included in the scope of Guidance 2007, has gradually started. Since ePRO systems are effective for identifying subjects' compliance status with the protocol and obtaining high-quality subject-reported data, the use of this system is expected to expand further.

With ePRO systems, data may be managed by the Contract Research Organization, or may be stored in devices and subsequently sent to vendor servers. Therefore, Guidance 2007, provided mainly for eCRF, cannot be applied to ePRO systems *as is*. It is needless to say that records must be formulated and appropriately abided by laws and regulations, in order to fulfill requirements for a new drug application dossier.

This document has been prepared as a supplement to Guidance 2007 to have important points be common view when using ePRO systems.

At the same time, some of the contents of Guidance 2007 have been revised, with the focus on the issue that had already been recognized by the authors and the regulatory authority at the time of the issuance of Guidance 2007 - concepts concerning the accountability of the sponsor regarding the identicalness between electronic data directly obtained from central laboratories and source documents at the sites.

Requirements for electronic signatures used in eCRFs have also been reconsidered from the viewpoint of regulatory requirements and operational conditions.

This document includes the following supplements to Guidance 2007; Chapter 1 "Requirements for Using Electronically Collected PRO for Drug Applications" for regulatory requirements and related operation for using ePRO systems, Chapter 2 "Important Points concerning the Electronic Data Directly obtained from Central Laboratories" for revised parts of Guidance 2007 concerning electronic data directly obtained from central laboratories, and Chapter 3 "Requirements for Electronic Signatures Used in the eCRF."

[1] http://www.jpma.or.jp/about/basis/guide/pdf/20071101guidance.pdf

1 Requirements for Using Electronically Collected PRO for Drug Applications

1.1 ePRO and ePRO systems

Assessment data directly provided by subjects, pertaining to all aspects of their health conditions, to which no interpretation is added by physicians or other persons, are called "Patient-Reported Outcomes (PRO)" (reference: FDA's Guidance for Industry - Patient-Reported Outcome Measures: Use in Medical Product Development to Support Labeling Claims; translated into Japanese by ISPOR Japan Charter's Working Group). In recent years, PRO has increasingly been collected electronically in clinical trials. In this guidance, electronically collected PRO are hereinafter referred to as "ePRO," and systems to obtain PRO as source documents and upload PRO to the trial database are referred to as "ePRO systems".

Please note that this guidance provides requirements for the electronic collection of PRO, and does not refer to the methods of collection, use etc. of the PRO itself.

1.2 Typical business model for ePRO systems

Before switching from receiving a paper PRO to collecting electronic PRO (ePRO), it is required to prepare necessary equipment (e.g. devices) and environment (e.g. internet line, telephone line) for data entry by subjects, make operational procedures for transmitting subject data to the operational database, operational procedures for providing the collected subject data to investigators. and sponsors, and also procedures for data retention after completion of the clinical trial and location of storage. As is defined in "PRO," a system must be established to avoid any interruption or change of data reported by subjects.

Figure 1 shows a typical business model of ePRO systems. A subject enters PRO using a device, IVRS (Interactive Voice Response System), or IWRS (Interactive Web Response System). The entered data are stored in the vendor's server as source documents. During this process, the vendor ensures reliability of the source documents as a "trusted third party."

During the trial, both the site and sponsor representatives can view the ePRO data in the vendor's server via web as necessary. The sponsor incorporates the ePRO data in its own trial database. After the completion of the trial, the source documents on the vendor's server are transferred to a CD-R or other general media, such as a PDF file or other format that can address the requirements of readability and retainability, through a process required for ensuring authenticity[2], and are stored at the site.

Definition of the respective data shown in Figure 1 is explained below.

First, in case of an ePRO system using an IVRS or IWRS, data in the server is regarded as source data, as it is directly recorded PRO (original). Therefore, the data must include an input trail and, in case of correction, an edit trail.

[2] As describing in section 1.5.1, "authenticity" in this document includes the meaning of "integrity".

In case of an ePRO system using an entry device, data saved in the device is the original record created by the subject, and is thus regarded as the source data. Therefore, the "Usage of Electromagnetic Records and Electronic Signatures in the Application for Drug Approval or Licensing" must be complied for the device itself. In other words, requirements for authenticity, readability and retainability must be fulfilled under precondition that the device has been validated. These requirements include recording of an audit trail in case the data saved in the device are changeable. Encryption or other security methods must be implemented in data transmission to the server via an open system. Since the data stored in the device lacks durability, it is necessary to transfer the data to a durable ePRO server at an early stage, by a verified procedure.

Next, data that has been transferred from the server to a CD-R or other recording media with intention of source data transfer after the completion of the trial, are regarded as a new source document as long as a copy of the data including the audit trail has been certified after verifications as being certified copies (note: The GCP definition of "source documents" includes copies and transcriptions certified after verification as being certified copies). Since the data is copied with the intention to transfer source documents, the relevant CD-R or other recording media is considered as the source documents, and the data in the server is no longer considered as the source documents, once transfer is completed.

On the other hand, data that the sponsor obtains from the vendor and stores into its database is merely considered as a dataset. This dataset is being used for analysis activities, but does not usually contain input and edit trails, etc. In other words, the vendor provides the relevant data, but the source documents of ePRO have not been transferred to the sponsor.

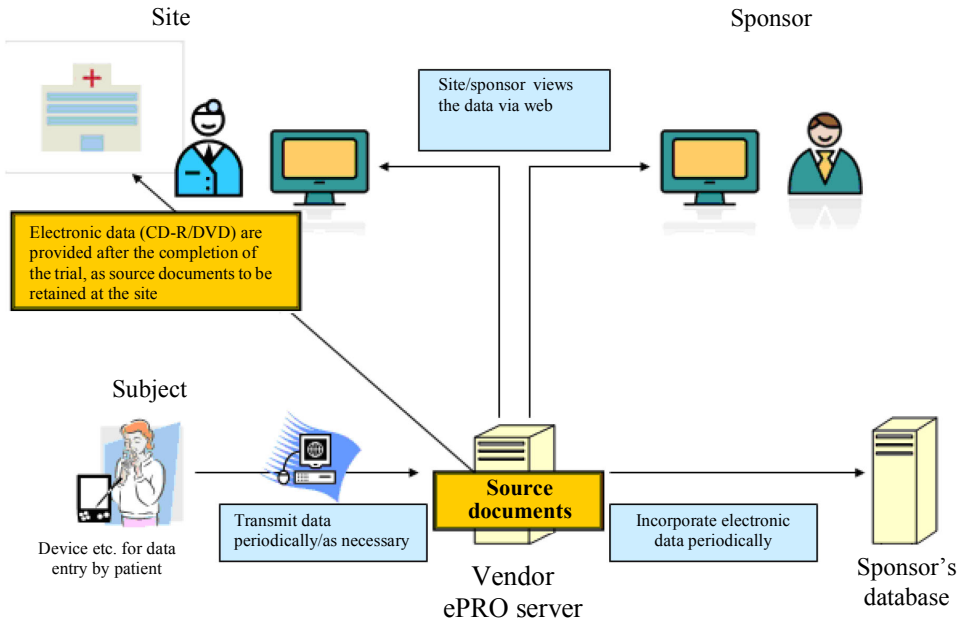

Figure 1. Typical business model of ePRO systems

1.3 Regulatory requirements

Based on the following regulations, the application and retention by electromagnetic records are admitted for a new drug application dossier. Important points are also specified in the regulations.

- Laws on the Usage of Information Technology for Saving Documentations by Private Businesses (Law No. 149 of 2004, hereinafter referred to as "e-Document Law")

- Ministerial Ordinance on the Usage of Information Technology for Saving Documentation by Private Businesses, pursuant to the Provisions of Laws and Regulations under the Jurisdiction of the Ministry of Health, Labor and Welfare (MHLW Ordinance No. 44 of 2005, hereinafter referred to as "Ordinance of the Governing Ministry")

- "Usage of Electromagnetic Records and Electronic Signatures in the Application for Drug Approval or Licensing" (PFSB Notification, dated April 1, 2005, hereinafter referred to as "ER/ES Guidelines")

When considering specifications and operation of ePRO systems that handle electronic PRO, the regulatory requirements listed above must be complied. In addition to the above, the following regulatory requirements must also be complied.

- Ministerial Ordinance on Good Clinical Practice for Drugs (MHW Ordinance No. 28 of 1997, hereinafter referred to as "GCP Ordinance")

- "Enforcement of Standards on the Conduct of Clinical Trials for Drugs" (PFSB/ELD Notification No. 1001001, dated October 1, 2008; superseded by the PFSB/ELD Notification No.1024-1, dated October 24, 2011 from April 1, 2012 onward; hereinafter referred to as "GCP Enforcement Notification").

Sections 1.4 and 1.5 focus on provisions of the GCP and requirements of the ER/ES Guidelines that must particularly be complied when using ePRO systems.

1.4 Requirements of the GCP

GCP stipulates retention of trial records, including both paper documents and electronic data. The sponsor must fulfill the requirements provided in Article 26 (Record Keeping), and the site must meet the requirements provided in Article 41 (Record Keeping).

Article 26, Paragraph 1-3 of the GCP Enforcement Notification specifies requirements for data handling using an electronic data processing systems (including remote electronic data systems), as follows.

When an electronic data processing system (including remote electronic data systems) is used to handle clinical trial data, the sponsor shall conduct the following:

1) Ensure and document that the electronic data processing systems fulfill the sponsor's established requirements for completeness, accuracy, reliability and consistent intended performance (i.e. validation);

2) Maintain the operating procedures for using these system;

3) Ensure that the systems are so designed as to permit data correction in such a way that the data correction are documented and that all records of correction of entered data remain undeleted as logs distinguishable to the inputter as well as to the corrector (i.e. to maintain audit trail, input trail, and edit trail);

4) Maintain a security system for the data;

5) Maintain the adequate backup of the data;

6) Prepare and maintain a list of the individuals who are authorized to make data correction; and

7) Keep the blinding in case of a blinded clinical trial.

Since ePRO systems are included in "electronic data processing systems," the sponsor must note the above requirements when selecting an ePRO system to be used.

When conducting data-converting operations on data in an ePRO system, the following requirements, provided in Article 26, Paragraph 1-4 of the GCP Enforcement Notification, must be fulfilled.

If data are converted during the processing, the sponsor should ensure that it is always possible to compare the original data with the processed data.

Article 41 of the GCP lays down the requirements for record keeping at the site, including the source documents.

As for ePRO system, which records assessment by subjects directly in electronic data, the data stored in the system server is expected to be used as source documents. Unlike data collected in the CRF, such ePRO source documents are not managed by the site. Therefore, the sponsor must always document which data must be used as the source documents.

For example, an ePRO system using a data entry device saves data within the device temporarily, and transfers the data to the ePRO server by a pre-defined timing and procedure. During this process, the data saved in the device are temporarily regarded as source documents. After the data is transferred to the ePRO server, the data in the ePRO server are considered as source documents. It is necessary to identify the "source documents" in the protocol etc., and document the timing and locations of source document storage.

It must also be noted that, the ePRO must be durable enough to be kept for their retention period specified in Article 26 of the GCP, "The sponsor shall appropriately retain the records," since ePRO refers to "data generated in conducting the clinical trial".

1.5 Requirements of the ER/ES Guidelines

An ePRO system that handles PRO electronically, must comply "3. Requirements for the Usage of Electromagnetic Records" of the ER/ES Guidelines. In other words, 1) authenticity, 2) readability and 3) retainability of electromagnetic records must be ensured. As a precondition for this process, the reliability of an ePRO system must be ensured through Computerized System Validation (CSV).

4) When Open Systems such as internet are used, additional measures must also be taken to ensure the authenticity and confidentiality of the electromagnetic records from their creation to receipt.

The requirements and operational procedures of the four points indicated above are described in the subsequent sub-paragraphs.

1.5.1 Requirements and operational procedures for authenticity

The ePRO system must be complete, accurate and reliable, and the responsibilities for the creation, change and deletion of data are clarified. To ensure authenticity, the following requirements must be fulfilled. "Entry" refers to the creation of new data, and "correction" refers to change or deletion of the existing data.

1) The ePRO system is designed to enable assignment of authorities in accordance with the responsibility of the users, as well as correct entry of the intended data under the assigned authorities.

   - User management and authority setting must be appropriately undertaken, as per the pre-set rules.

   - Authentication of users who access the system must be established. A combination of at least two elements must be used for user authentication before access. For example, in case of an ePRO system using a mobile information terminal or similar device, a user must be authenticated using his/her subject ID (case number), which is pre-registered by the site's administrator, and the access code (PIN number or password) entered by the subject. In case of an ePRO system using an IWRS, an ID and password entered by the subject must be used for his/her authentication.

   - Appropriate training must be provided to ensure appropriate usage and compliance. Since the users of an ePRO system are subjects, it is essential to provide them with understandable manuals and pre-trial trainings using equipment related to the ePRO system in order to collect intended data and improve quality of the trial data. It must be noted that, basic handling procedures of equipment and management of passwords and IDs must be included in the training program. It is also desirable to establish a help desk in advance to minimize loss of data reliability due to missing data that may be caused by device failure, forgotten access codes etc., and subsequent transcription from paper media.

   - The following points must be confirmed in advance, through User Acceptance Test of the ePRO system;

The entered data are accurately recorded as intended, can be confirmed on the display screen etc., and are accurately transferred to the server. The system is also designed to ensure that the intended data are entered accurately under the assigned authorities.

- An audit trail can be retained automatically.
  Together with the entered data, the date and time of entry and the person who enters the data can be recorded. If the system is also designed to permit data correction, then the data corrections are documented and that all records of correction of entered data remain undeleted as unchangeable logs distinguishable to the inputter as well as to the corrector, automatically.

- Accurate time stamps of data entry can be recorded.
  One of the significant advantages of using an ePRO system is the recording of time stamps of data entry. The date and time should be set accurately.

2) Security is maintained in the ePRO system and its operational procedures.

   - An audit trail shall enable identification of the persons who entered the data, the entered data and the time of entry. In case of correction, the persons who corrected, the correction details and the time of correction must be identifiable.

   - The system must be designed to prevent and/or detect unauthorized access.
     For examples, the system has a function that demands an access code in case of loss of a device, or a specific equipment or program to download data from the device, etc.

3) The operation and management of the process should ensure the same data quality as that of the clinical data collected in a paper PRO (e.g. subject diary).

   - The time and location of storage of data collected by an ePRO system must be identified and documented in advance.

   - After the completion of the trial, the electronic data including the audit trail managed in the vendor's ePRO server must be transferred to a CD-R or other alteration-proof recording media, through a pre-verified procedure, and must be provided to the site as "source documents."

4) Backup of the ePRO data including user lists and authority information etc., should be maintained appropriately.

   - Based on a documented procedure, the latest data should be backed up on a regular schedule. In case of an unexpected situation, the data should be restored through a predetermined procedure.

   - In case of hardware or software failure, the operating environment should be restored through a predetermined procedure.

5) In case of revision to an ePRO system is needed during trial, tasks related to the revision should be undertaken appropriately.

- Revision of an ePRO system includes upgrading of the system version, modification of the data entry screen, and addition, correction, deletion of programmed automatic queries, etc. In any case, reliability of the system must be ensured through CSV.

- If data migration is needed after the revision of an ePRO system, validation documents must prove that the data conversion or export has been performed through a verified procedure, and the updated data are identical to the source data before the conversion or export.

- Procedures for the revision and change control of validation documents and other documents must also be established in advance, thus enabling a chronological and traceable history of the creation and revision of validation documents and other documents to be retained.

1.5.2 Requirements and operational procedures for readability

All the data entered into an ePRO system and audit trail should be able to output in a human-readable format (e.g. showing on a display device, printing on paper, copying to electromagnetic recording media). The output should be easy to read and handle.

If it is necessary to evaluate safety and efficacy and/or to conduct monitoring with the data collected by an ePRO system, such data should be viewable at any time throughout the trial period.

During the transfer of data with the relevant audit trail to recording media for archiving after the completion of the trial, the readability should be maintained at the same level as in the ePRO system, so that such data is easily accessible throughout the specified period of record keeping.

1.5.3 Requirements and operational procedures for retainability

Throughout the specified period of record keeping, the authenticity and readability of the electromagnetic records must be ensured. In order to ensure retainability, the following requirements must be met.

1) Requirements concerning the retainability of electromagnetic records (data and the relevant audit trail) in the ePRO system

- Procedures for retaining electromagnetic records with appropriate risk assessment should be documented in advance. (Establish operating procedures)

- Electromagnetic records should be placed under the same level of control as that of the retention of paper source documents (e.g. assignment of a retention manager, assurance of security)

- Electromagnetic records in the ePRO server should be readily retrievable at any time throughout the specified period of record keeping, in case of inspection by the regulatory authority etc.

2) Requirements concerning the retainability of electromagnetic records that are transferred from the ePRO device to the ePRO server

- The authenticity, readability and retainability of electromagnetic records after the transfer must be ensured.

- When data is transferred from the ePRO device to the ePRO server, the content and meaning of the records must be retained by a pre-verified automatic conversion or export procedures.

3) Requirements concerning the retainability of electromagnetic records that are transferred from the ePRO server to other recording media

- The authenticity, readability and retainability of electromagnetic records after the transfer must be ensured.

- In case of data transfer from the ePRO server to other recording media for archiving, the content and meaning of the records must be retained by a pre-verified automatic conversion or export procedures.

- Appropriate recording media should be used for archiving. In other words, the recording media should be capable of long-term retention of data, and be alteration-proof.

4) Requirements concerning the retention of ePRO systems

- Even though the ePRO system is revoked after data transfer, validation documents and other record documentation must be stored to allow later reference to the requirement specifications, design, validation process etc. of the system.

- In case ePRO system software is retained after data transfer, readability must be ensured in the new computer environment. In other words, in case of fulfilling the retainability requirements by retaining the ePRO software after data transfer, and by re-install in the server as needed, the readability in the new computer environment must be ensured.

1.5.4 Requirements and operational procedures when an open system is used

When an open system is used for the creation, change, maintenance, storage, retrieval and/or transmission of electromagnetic records in an ePRO system, appropriate measures must be taken and added in addition to the requirements indicated from 1.5.1 through 1.5.3, in order to ensure the authenticity and confidentiality of electromagnetic records from their creation to receipt.

- Before transferring the data in the device to the vendor's ePRO system via the web, the data must be encrypted.

2. Important Points concerning the Electronic Data directly obtained from Central Laboratories

Concerning the requirements for electronic data obtained from central laboratories, Guidance 2007 describes the relevant concepts from the viewpoints of authenticity, readability and retainability, and states that the sponsor has the primary responsibility to ensure the identicalness of the electronic data obtained from central laboratories and the test results (i.e. source documents) reported to the sites from central laboratories. However, specific procedures to prove the identicalness of such data was not described when Guidance 2007 was issued.

As a supplement to this point, this section describes the procedures to be taken by the sponsor to prove the identicalness of source documents at the sites and electronic data obtained directly from central laboratories.

2.1 Qualification of central laboratories

The sponsor must conduct the system audit and/or assessment for the central laboratories in order to ensure that there are no problems with their data reliability and quality management systems.

- The central laboratories must establish Standard Operating Procedures for all processes related to the collection and processing of measured data.

- CSV must be conducted in a planned manner.

2.2 Verification of transfer and conversion processes of electronic data

The sponsor must test its transfer and conversion processes of electronic data, and ensure that there are no problems with the operating procedures and data identicalness before and after the transfer or conversion of data.

- Specifications for electronic data capture should be established.

- Specifications on compatible software and hardware used for electronic data capture should be defined.

- For testing purpose, the sponsor should receive and check the electronic data of test results from the central laboratories.

- The sponsor should confirm the procedures to correct the test results at the central laboratories, and check the process for obtaining revised data.

2.3 Verification of data by direct access

Although it is a given fact that the accuracy of electronic data provided to the sponsor is assured by the central laboratories, the implementation of 2.1 and 2.2 above enables the sponsor to secure identicalness of the electronic data obtained from the central laboratories and the test results (i.e. source documents) reported to the sites by the central laboratories. Note that it is also required to verify the consistency of patient IDs, dates, and other information between test

reports and other source documents by direct access, in order to ensure authenticity of the data of each subject.

2.4 Confirmation of received data

The sponsor should implement the processes to confirm that electronic measurement data obtained from the central laboratories do not contain missing or redundant data. The scope of confirmation should include the data transmission logs from the central laboratories to the sponsor.

3. Requirements for Electronic Signatures Used in eCRFs

Article 47 of the GCP Ordinance requires Case Report Forms to be sealed or signed by the investigator. The following sections describe the requirements for electronic signatures used in eCRFs.

3.1 Regulatory requirements

Article 4 of the e-Document Law states that electromagnetic records may be created in place of paper documents for items specified by the Ordinance of the Governing Ministry, and electronic signatures as specified by the Ordinance of the Governing Ministry may replace conventional signatures.

The Ordinance of the Governing Ministry on eCRF refers to MHLW Ordinance No. 44 (see section 1.3). In Appendix 2 of this ordinance, it is indicated that CRFs may be created as electromagnetic records. Article 7 of this ordinance states that conventional signatures may be replaced by electronic signatures.

According to the provision in Article 7 of this ordinance, "electronic signatures" refers to "electronic signatures under Article 2, Paragraph 1 of the Law on Electronic Signatures and Certification Services (Law No. 102 of 2000, called 'Electronic Signature Law')." Therefore, electronic signatures that fulfill the following two requirements specified in the Paragraph 1, are considered acceptable.

(1) A measure to indicate that such information was created by the person who has taken such measure (hereinafter referred to as "identity"); and
(2) A measure to confirm whether such information has been altered (hereinafter referred to as "non-falsification").

Function for electronic signature implemented in commonly-used EDC systems secures the identity by combining a user ID with password, while confirming non-falsification by the audit trail function. Thus such EDC systems are considered to comply with the requirements for electronic signatures as specified in Article 7 of the MHLW Ordinance No. 44.

Nonetheless, ER/ES Guidelines have been issued from the standpoint of ensuring the reliability of a new drug application dossier and source documents that are submitted and/or retained as electromagnetic records, and it provide specific requirements for using electronic signatures.

Therefore, the requirements for using electronic signatures, as specified in the ER/ES Guidelines, must be complied when electronic signatures are used in eCRFs.

3.2 Operational procedures

Based on the above section, operational procedures on electronic signatures used in the eCRF are described below.

1) Procedures regarding management and using electronic signatures shall be documented, and implemented appropriately.

   Management rules for accounts with the authority of electronic signature must be established and implemented. For example,

   - To establish the approval process for account application by an appropriate approver.
   - To establish authentication process for the applying person.
   - To establish procedure to confirm that correct authority is granted to appropriate accounts.
   - To establish rules for users to be granted with the authority of electronic signatures, and the timing of authorization and other relevant rules (e.g. after education, training) must be established in advance.

   In addition to authorization, the procedures must include the revoke of authority after a change in the investigators.

   Procedures must also be established to disable authority provided by a card or token, in case they are lost, stolen or deteriorated.

   The appropriate implementation of the above rules and procedures must be confirmed by audit for the sponsor itself and sites, and monitoring.

2) Each electronic signature shall be uniquely assigned to one authorized individual, and shall not be reused by or reassigned to other individuals.

   In case biometrics is not used for user authentication, a combination of at least two elements (e.g. user ID and password) must be used.

   Rules should also include the interval of password change, length of the password, types of letters to be included in the password, etc.

   If the combination of user ID and password is used for electronic signatures, the same user ID must not be assigned to other persons.

3) An electromagnetic record with an electronic signature shall contain explicit information on all of the following items:

   - First and last name of the signer,
   - Date and time of when the signature was executed, and
   - Roles of the signature (e.g. creation, confirmation, approval)

   The same information must be included in each copy of the eCRF.

4) To prevent falsification, electronic signatures shall be linked to respective electromagnetic records to ensure that the signature can not be deleted, copied etc. by ordinary means.

5) Miscellaneous (issues concerning education, training required for the users of electromagnetic records and electronic signatures)

Relevant education and/or training should be provided to all related persons, and recorded.

Responsibility for electronic signatures must be clearly understood by the investigators and their sites. Article 3 of the Electronic Signature Law states that information provided in an electromagnetic record is supposed to be authentic as long as an electronic signature is executed to the record by the authenticated person. The person who executes electronic signature has the same responsibilities as those accompanying a handwritten signature in a paper document. Therefore, training should be provided to enable each signer to understand the responsibilities properly, and the training records need to be retained.

Terms and Definitions

Terms	Definitions
PRO (Patient Reported Outcomes)	Assessment data that are directly provided by subjects pertaining to all the aspects of their health conditions, and to which no interpretation is added by physicians or other persons
ePRO (Electronic Patient Reported Outcomes) system	System for obtaining PRO as source documents and incorporating it into the trial database
ePRO (Electronic Patient Reported Outcomes) server	Server for storing data in an ePRO system
ePRO (Electronic Patient Reported Outcomes) device	Device designed to store data temporarily and used for data transfer to the server in a pre-defined timing and procedure
IVRS (Interactive Voice Response System)	Computerized system that automatically answers with recorded voice messages on phone calls; as the caller dials a specific number, the corresponding pre-set voice message is played automatically, and the caller registers his/her answers using the dial operation; also used as a system for collecting ePRO
IWRS (Interactive Web Response System)	System for collecting data as the user enters his/her answers to the questions indicated on the Internet website ; also used as a system for collecting ePRO
Source Data	All information in original records and certified copies of original records of clinical findings, observations and other activities in a clinical trial, necessary for the reconstruction and evaluation of the trial. Source data is included in the source documents (i.e. original records or certified copies)
Source Documents	Original documents, data and records that were initially created (e.g. hospital records, clinical and office charts, laboratory notes, memorandum, subjects' diaries and evaluation checklists, pharmacy dispensing records, recorded data from automated instruments, microfiches, photographic negatives, microfilms and other magnetic media, X-rays, subjects' films and other records kept at the pharmacy, laboratory, medico-technical departments etc. involved in the clinical trial), and copies or transcriptions certified after verification as being accurate copies