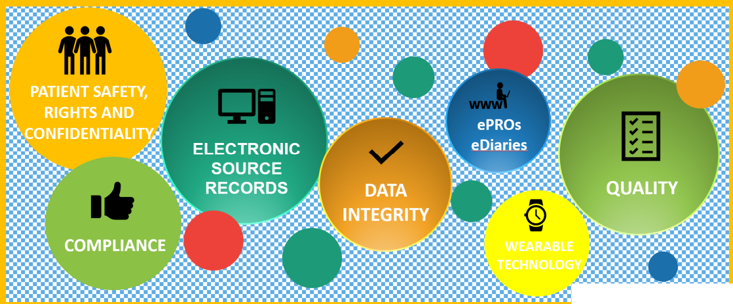
ELECTRONIC SOURCE RECORDS – FRIEND OR FOE?

Authors: Katarina Eghan, Maxim Bunimovich and Marina Freiberga, TMQA and Matt Jones, Digital Quality Associates


PATIENT SAFETY, RIGHTS AND CONFIDENTIALITY
ELECTRONIC SOURCE RECORDS
DATA INTEGRITY
ePROs eDiaries
QUALITY
COMPLIANCE
WEARABLE TECHNOLOGY

INTRODUCTION

The use of electronic source records and electronic source data collection tools can be considered to be the norm in today's clinical trials. However, regulators as well as quality and other clinical research professionals are struggling with assuring the integrity of e-records supporting the data submitted to regulatory agencies, including providing governance and provenance solutions.

Many electronic medical record (EMR) systems used by healthcare providers have been developed or sourced with limited consideration for the requirements of clinical research. The Principal Investigator (PI) and other site staff do not always have the necessary understanding of the system characteristics and how these relate to the principles of data integrity (the EMR system is usually managed by a dedicated IT department within the institution). Moreover, monitors and other clinical research professionals, including Quality Assurance (QA), do not always fully comprehend the data integrity principles and how these apply in practice, or, there are insufficient tools available to help them assure data integrity when reviewing such systems and performing source data verification. Workarounds are often put in place for the management of medical records used in clinical trials (e.g. printing of EMRs) and for the monitoring and other data and quality verification activities such as audits and inspections (e.g. in the form of signed certified copies, for which it is difficult to determine if they are current).

Additionally, various electronic solutions are being used to collect trial data such as patient reported outcomes (PROs), wearables (e.g. Smart watches) and sensors (e.g. cardiac monitors). However, are these always designed and developed with the relevant data integrity principles in mind and can data integrity be demonstrated appropriately and evidence of this retained for as long as necessary?

Insufficient knowledge of data integrity principles often leads to inappropriate workarounds and solutions being put in place, which are frequently onerous and do not necessarily assure data integrity. Quality management and assurance activities regularly assess some but not all critical elements of e-source management. This poster contains some common issues and questions as well as some considerations and possible solutions.

Digital Quality Associates

www.digitalqualityassociates.com

TMQA

Excellence in Research Quality Assurance

www.tmqa.co.uk

Site EMR Systems
Common Issues and Questions
Considerations and Possible Solutions

The system meets all applicable data integrity principles (audit trails, validation, e-signatures, individual access, back-up, etc.) - what should we watch out for?

- Can audit trails be viewed by monitors, auditors or inspectors to determine when the record was first made and by whom and subsequently changed (when, who, why, how)?
- Does the audit trail capture if records were deleted?
- Is it possible to switch off the audit trail functionality?
- Is the e-signature compliant with the relevant principles? For instance, can it be determined what the meaning of the e-signature is and are there appropriate timestamps that reflect the signatory's current location and not the location of the server?
- What evidence of validation of the system is there, and does it meet all requirements?
- What security measures are in place? Adequate security patching, regular planned review of firewall settings and users.
- What are the back-up procedures and are they adequate (frequency, location – different for critical data)? Is regular restore testing performed and documented?
- Are there adequate measures in place against loss or accidental destruction of data?
- Do staff know that accounts cannot be shared? How do staff remember their log-in details (are these documented in an insecure manner, e.g. in notebooks)?
- Are there appropriate governance procedures in place and are site staff appropriately trained on these as well as the use of the EMR system?

The system has no audit trail/e-signature functionality/validation i.e. the site uses it as a 'typewriter' and the official medical documentation is paper

- The e-records cannot be used to make medical decisions and paper records containing appropriate sign-off must be referred to.
- Even if the official medical documentation is paper, the monitor/auditor should perform appropriate due diligence activities to ensure that all available medical records are on file (e.g. 'over the shoulder' review of e-records with site staff).

The monitor/auditor cannot be granted unaided direct read-only access to EMRs or the access cannot be restricted to trial subjects only

- Certified copies of the EMRs are provided for monitor/auditor review. The copying process should be 'validated' and the copies should contain all attributes of the original (e.g. colour, metadata, etc.).
- Certified copies are available for any changes to EMRs.
- Periodic spot checks of the available EMRs versus print-outs (i.e. 'over the shoulder' review with site staff) is performed and documented (the extent and frequency should be based on a risk assessment).

The system is assessed during monitoring and audit activities, but the assessor is not conversant with all applicable requirements and principles

- Upskilling and training the assessor in electronic technologies, related requirements and guidelines, as well as company rules and expectations.
- User-friendly tools to aid the assessment process, pointing out the potential problems and possible solutions.
- Simplification of technology and terms.
- Mindset change.
- Allocation of key experts in departments.

The monitor does not know what is the source for each data point and/or who performs the related procedure and/or collects the data

- Document what is source for each data point in a source data agreement/ location document (e.g. paper worksheet, EMR progress note, etc.).
- Documented review of site's data collection methodology, including continuous review for any changes.
- Ensure that it is clear from the records which staff member has performed each procedure and/or collected the data. For example, if vital signs are measured by nurses they should record the relevant values or if this is typed by the investigator directly in the EMR notes, the nurse should also validate the data by appropriate sign off. Any paper records containing first entry of data is source and must be retained.
- Reduce record duplication (e.g. transcription of source data documented on a vital signs worksheet into EMR).
- If the system allows for storage of scans, how are the original paper records maintained and are the scans accurate copies of the original, containing all attributes (e.g. colour)?

Log-in sharing by site staff

- Review audit trails for data entry at appropriate intervals and verify if staff were present at site at the time of data collection.
- Question spurious data collection patterns (e.g. all data collected using the same log-in).

Long-term data storage and retrieval

- Discuss and document long-term data storage and retrieval, including the archival of metadata.
- Document the requirements in the contract.

References and Further Reading

- ICH E6 (R2)
- Medicines and Healthcare products Regulatory Agency (MHRA) 'GXP' Data Integrity Guidance and Definitions (Mar 2018)
- MHRA Position Statement and Guidance Electronic Health Records (Sep 2015)
- European Medicines Agency (EMA) Reflection Paper on Expectations for Electronic Source Data and Data Transcribed to Electronic Data Collection Tools in Clinical Trials (Jun 2010)
- Food and Drug Administration (FDA) Code of Federal Regulations Title 21 Part 11
- Use of Electronic Health Record Data in Clinical Investigations, FDA Guidance for Industry (Jul 2018)
- Good Automated Manufacturing Practice (GAMP) 5 Guide: Compliant GxP Computerized Systems (Feb 2008)
- GAMP Guide: Records & Data Integrity (Mar 2017)
- ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements
- Clinical Data Interchange Standards Consortium (CDISC) Standards & Electronic Source Data within Clinical Trials (Nov 2006)
- MHRA GCP Symposium 2018
- MHRA Blogs

For further discussion, please contact Katarina Eghan (katarina.eghan@tmqa.co.uk) or Matt Jones (matt.jones@digital-quality.co.uk).

Are there any changes made to e-source (e.g. ePRO data) during sponsor data management activities that are not endorsed by the subject and/or the PI (ownership of source data)?

- No changes to source data can be made by the sponsor or Contract Research Organisation (CRO) personnel and this principle also applies to e-data collected using sponsor or CRO-provided tools.
- Verify data changes during audits, including appropriate documented endorsement by the subject/PI.
- The sponsor should not have exclusive control of the source data, including those collected electronically on tools provided to sites.

How reliable is the data entered by subjects?

- Routinely check audit trails to verify if the data have been entered at credible times. For example, does the time of e-data collection by subjects coincide with other trial procedures such as ECG collection and their validity is therefore questionable?
- Review audit trails to determine how long it takes the subjects to enter the data. Are relatively long questionnaires completed within seconds as subjects get used to the questions?
- Review data for reasonable variability.
- Change the questions around, if possible, at appropriate intervals.
- Verify with the subjects the validity of the provided answers and document.

How can you determine that the data have been entered by the subject (e.g. eDiaries for home use or ePROs)?

- The simple step of adding a PIN/password security level for the entry of data by trial subjects may not be sufficient as this alone does not provide assurance that the data have been entered by the subjects themselves. Anyone who can set-up a new subject in the system can then also create the necessary PIN/ password.
- Check IP addresses, if possible and allowed by local data sharing laws. There have been reports that eDiary data supposedly entered by subjects at home had been entered for multiple subjects at the investigator site.

Safety alerts (e.g. via eDiary)

- The set-up of any safety alerts should be appropriate for the studied population and any over-notification (e.g. via phone or e-mail) should be corrected following an appropriate risk assessment.
- Data privacy should be considered when setting up alerts (e.g. the use of subjects' e-mail addresses or phone numbers and their sharing with the CRO maintaining the system).

Are e-tools appropriate for the target subject population (e.g. age or mental capability) and does the technology support seamless data collection?

- Ensure the design and functionality is appropriate for the target population.
- Ensure that subjects have appropriate technology (e.g. internet access at home to allow data transfers).
- Ensure appropriate back-up procedures (e.g. paper questionnaires).
- Ensure appropriate issue resolution and escalation.

(Long-term) data storage and retrieval

- Are there adequate measures in place against loss or accidental destruction?
- Provide the site with a copy of the source data in a format that will allow data retrieval for the required time, including the metadata.

Retrospective data entry

- Unrestricted retrospective data collection is not acceptable, unless supported by an appropriate risk assessment. For example, ePRO data collected with delays of a few months.

Is the patient the wearer? Potential for removable wearables to be 'swapped' with other users. Similar results.

- Is it the true patient that is using the device, or could one person be wearing multiple devices?
- Check consistency of vital signs if recorded, this could give an indication that the correct person is using the device.
- Could the results be fabricated and not being produced by a device?
- Is the device functioning correctly – are the results between patients 'too similar' – lack of accuracy.
- Biometrics (e.g. fingerprint reader).

Data transmissions

- Examine data for gaps and drops in connection, especially if transmitted through the patient's smart phone.
- Check the status of the data transmission; is it consistent, are there any gaps – this could signify that there are interruptions in the connection between device and internet/smart phone.
- Check how those data are received by the site and the review cycle by the investigator, look for indications that they have been reviewed and acted upon e.g. out of range results.