http://www.colginconsulting.com/3-tips-for-edc-audit-trails/?utm_source=LinkedIn&utm_medium=ISPE_GAMP_R%26D_and_Clinical_Systems_SIG&utm_campaign=EDC_Audit_Trails

NOTE: (EDC=Electronic Data Capture-mn)

3 Tips for EDC Audit Trails

What follows is more or less a transcript of my presentation at the joint annual meeting of the San Diego Regulatory Affairs Network and the Orange County Regulatory Affairs Discussion *Group on 19 Nov 2014. The 3 tips? 1) Use good password reset practices; 2) Don't allow* queries *to fire until data are saved; and 3) Don't use coercive language in queries.*

I recently attended the MAGI West conference in San Francisco. During the conference, many attendees from investigator sites complained that sponsors have stopped providing them worksheets on which they can record the specialized source data required by sponsors' protocols. Some of the sponsors in attendance explained there was a concern that the worksheets were perceived as being too directive and had the possibility of unduly influencing data collection.

What wasn't discussed is that the design and implementation of EDC systems can actually make this situation worse, particularly with respect to queries and data changes.

EDC systems are a bit strange

EDC systems are used to create, modify, maintain, retrieve, and transmit case report forms electronically.

Who's responsible for the adequacy, accuracy, and availability of case report forms? **The investigator** (21 CFR Part 312 and ICH E-6).

Yet…

- The sponsor selects the vendor
- The sponsor negotiates the contract with the vendor
- The sponsor pays the vendor
- The sponsor or vendor designs the eCRFs
- The sponsor or vendor configures the queries and authors the eCRF completion guidelines
- The sponsor and the vendor have access to the case report form data

It’s very important that you be able to verify your eCRF data, whether you’re a sponsor or an investigator.

Audit trails provide confidence

How can you verify eCRF data and establish confidence in their integrity? By checking the audit trail. If the system was designed properly, the audit trail tells you who did what and when.

ICH E-6 requires that any change or correction to a CRF be audit trailed, whether done in writing or electronically. In addition, the investigator is required to “retain records of the changes and corrections.”

Here are 3 tips for working with your EDC providers to improve data integrity and make it easier to verify data. Let’s start with the “Who” part of the audit trail.

Tip 1

Use good password reset practices to ensure you have the right “Who” in the audit trail.

Have you ever forgotten your password for an application and locked yourself out of your account by entering the wrong password too many times? I know I have!

Why are systems designed like this in the first place? It’s not to irritate users. It’s to deter brute force attacks by unauthorized users.

Well-designed systems have good ways of managing users when they lock themselves out.

Good user access management

When a user enters the wrong password and the system locks them out, the system provides a link for the user to reset their password.

- The user clicks the “Reset Password” link.
- The system sends an email to the email address associated with the account. (Sometimes the user even has to enter the correct email address before the system will send the message.)
- The user logs into their email account and uses the link in the email to reset their password.
- The system usually presents a special password reset screen and requires the user to enter the same password twice.

Systems are designed this way to maximize the likelihood they're interacting with the real owner of the account. They're protecting themselves and the user.

Bad user access management

Let's look at the flip side. Some EDC systems make changing passwords far too easy. If all a user has to do is click "Reset" and enter a new password, then you have a security design problem.

Anyone who knows a user id in this situation can reset the password and control the account. It's hard to feel confident that only the correct, authorized person has access to the investigator's records. Can you **ever** be sure in this situation that the "Who" in the audit trail is correct?

Side note: This "feature" is really a design flaw. It isn't something sponsors can control. And it illustrates the importance of selecting your providers carefully and performing a thorough qualification audit.

Scenario

Here's a scenario to help us through the next two tips for queries.

The study goal is to reduce blood pressure in hypertensive adults to a "normal" range of 130/80. The subject has been on study for 2 months, comes in for Visit 5, and has a blood pressure of 145/80. The study nurse records 145/80 in the medical chart or source data worksheet during the visit. Later in the week, the data entry coordinator enters the data into the CRF.

Tip 2

Don't allow queries to fire until data are saved.

EDC queries prompt users to verify or make changes to case report form data. Automated queries are designed by sponsors to fire when users enter unexpected data. They are a perfectly legitimate way to get cleaner data ready for analysis faster.

In general, a good automated query fires in such a way that the fact that it fired, who made the changes (if any), when the changes were made, and what the previous values were are all recorded in the audit trail.

Good queries are audit trailed

The data entry coordinator

- Enters 154 for systolic blood pressure
- Tabs to the diastolic blood pressure field
- Enters diastolic blood pressure
- Saves the CRF

The system fires an automated query: “Please verify systolic blood pressure.”

The data entry coordinator

- Checks the medical record or source data worksheet and sees they made an error
- Changes 154 to 145 on the CRF
- Saves the CRF

The system fires an automated query: “Please verify systolic blood pressure.”

The data entry coordinator closes the query because they know the data were entered correctly.

The system records the following in the audit trail

- 154 for systolic blood pressure and the associated date, time and user id
- Record of the query firing
- 145 and the associated date, time and user id

The key takeaway? **All changes prompted by the sponsor through queries are captured in the audit trail.**

Bad queries (and data changes) are written in invisible ink

The data entry coordinator

- Enters 154 for systolic blood pressure
- Tabs to the diastolic blood pressure field

The system fires an automated query: “Please verify systolic blood pressure.”

The data entry coordinator

- Checks the medical record or source data worksheet and sees they made an error
- Changes 154 to 145 on the CRF
- Tabs to the diastolic blood pressure field

The system fires an automated query: “Please verify systolic blood pressure.”

The data entry coordinator

- Closes the query because they know the data were entered correctly
- Enters the diastolic blood pressure
- Saves the CRF

The system records the following in the audit trail

- 145 and the associated date, time and user id

Problem? There is no record the query fired, nor is there any record of what the site originally entered. The system was designed to use what I call invisible ink. Except in this case, there’s no trick to reveal what’s invisible. In fact, the change wasn’t recorded at all. **The audit trail is incomplete.**

Why does this happen? In my experience, the reason most IT professionals give for this practice is that “It’s not data until the site saves it.” However, there is no provision in the regulations for draft CRF data.

As the investigator fulfills their responsibility for oversight and reviews the eCRF, they’ll never know if data entry personnel are making these types of errors. And the sponsor has no insight into what a site or sites might be struggling with.

Tip 3

Don’t use coercive language in queries.

Good, non-coercive queries

When users enter impossible data (e.g., 41 Oct 2014 for a visit date), it is not coercive to query: “Please correct visit date.”

When users enter improbable data (e.g., 280 for systolic blood pressure), it is not coercive to query: “Please verify systolic blood pressure.”

Bad, coercive queries

When the user enters biologically likely data, (like 145 for systolic blood pressure), what do they do when presented with the following queries?

- “Systolic blood pressure is too high. Please verify.” What does the sponsor mean by “too high?”
- “Systolic blood pressure is too high. Please correct.” The sponsor has decided this is a mistake ahead of time?
- “Systolic blood pressure is too high. Please change.” It doesn’t get much more coercive than that , does it?

None of these queries are well-written. All of them could be viewed as coercive.

Combine coercive language with invisible ink, and you have a recipe for making it appear that the sponsor is too directive and has undue influence on the CRF data.

Tips

Follow these 3 tips, and you’ll go a long way to being able to verify the quality and integrity of your eCRF data by being able to rely on the audit trail.

1. Use good password reset practices to ensure you have the right “Who” in the audit trail.
2. Don’t allow queries to fire until data are saved.
3. Don’t use coercive language in queries.