Session 2: Technology in Clinical Trials – Digital Health Technology (DHT)

Joint US-FDA | MHRA-UK | Health Canada Good Clinical Practice & Pharmacovigilance Symposium
February 13, 2024 – 10:25 – 11:05 AM

Moderator: **Debbi Fox, BSc**
Compliance Specialist | ROEB | HC

Elena Boley, MD, MBA
Senior Physician | DCCE | OSI | OC | CDER | FDA

Mandy Budwal-Jagait, MSc
Head of GCP and Lead Senior GCP Inspector | MHRA

Technology in Clinical Trials
Digital Health Technology

Elena Boley: Senior Physician | CDER | US FDA
Debbi Fox: Compliance Specialist | Health Canada
Mandy Budwal-Jagait: Head of GCP | MHRA

A Joint US-FDA | MHRA-UK | Health Canada Good Clinical Practice & Pharmacovigilance Compliance Workshop
February 13, 2024

Medicines & Healthcare products Regulatory Agency

Health Canada Santé Canada

Overview

- Definition of Digital Health Technology (DHT)

Case studies:

Access Controls

Compliance Fundamentals and Hybrid Systems

When Data Integrity falls

Digital Health Technology in Clinical Trials

- Any instrument, tool or platform utilized at any point in the data lifecycle of electronic data captured and reported as part of a Clinical Trial.
- Includes any computer system, software application and input sensors/devices used to collect, manage, transmit, store or report electronic data.
- Includes remote data acquisition tools.

Digital Health Technology

Examples

- Data sensors, mobile apps and data / computing platforms
- Electronic patient-reported outcomes (ePRO) devices and software
- Interactive Response Technology (IRT)
- Wearables
- Electronic Case Report Forms (eCRF)

Remote Data Acquisition: Proceed with Caution

Elena Boley, MD, MBA

Senior Physician, Office of Scientific Investigations

Division of Clinical Compliance Evaluation, Office of Compliance

CDER | US FDA

A Joint US-FDA | MHRA-UK | Health Canada Good Clinical Practice & Pharmacovigilance Compliance Workshop

February 13, 2024

Medicines & Healthcare products Regulatory Agency

Health Canada Santé Canada

§ 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…."

21 CFR Part 11 Subpart B Section 11.10

Overview

- The case
- What happened
- The consequences
- How to do better

The Case

- New Molecular Entity
- A single multi-center, randomized, double-blind, placebo-controlled, Phase 3 trial
- Indication: treatment of a disease
- Inspections: 4 Clinical Investigators, sponsor
- Efficacy endpoint data anomalies

Study Design

- Screening
- Baseline assessments including ePRO
- 1:1 Randomization to study drug or placebo
- 12-month treatment phase
- Monthly ePRO assessments
- Change from Baseline to Month 12 in disease severity

Benefits of remote ePRO data acquisition

- Convenient => improved participant recruitment, engagement, and retention
- Real-time data collection yields more meaningful data, avoiding recall bias
- Instantaneous transfer of data while maintaining the blind
- Real-time data monitoring and outlier identification

ALCOA+

Attributable
Legible
Contemporaneous
Original
Accurate
+ Complete, Consistent, Enduring, and Available

Efficacy endpoint data anomalies

- Unusual patterns of ePRO efficacy data for groups of participants
  - Similar patterns of data missingness
  - Similar data collection times
- No simple explanation

What should have happened?

- App installation on a mobile device
- App set up: enter default PIN, select confidential PIN
- Security questions (2) with answers
- Helpdesk phone number

What the inspections found

- Common PINs
- Birthdate-based PINs
- Security question and answer patterns

Subject	Question	Answer
1	A	X
	B	X
2	C	X
	D	X

Subject	Question	Answer
1	A	X
	B	Y
2	A	X
	B	Y

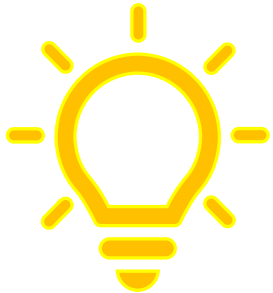
What actually happened?

- Site staff provided instructions/suggestions to participants regarding PIN choice
- No explanation for the unusual patterns found for the security questions and answers
- *ultimately, an analysis by the sponsor revealed the same patterns at a majority of sites for the study

Why would this happen?

Decision support

Inadequate helpdesk assistance



Forgetful participants

Staff access to the participants' ePROs

Consequences for the NDA

- Several FDA Form 483s were issued
- Concerns about data reliability
- Data excluded from the efficacy analysis
- A major protocol amendment and a delay in FDA's review
- Scrutiny by other regulatory agencies

A moment to reflect

- Isolated to this one clinical trial…
- or is this behavior more widespread?

PASSWORD OVERSATURATION

Poll Question

Which of the following is (most) true for you?

A. I have used my birthdate, name, cell phone number, or home address as my password

B. I have written down my passwords or shared them with others

C. I have used the same password more than once

D. I am perfect, and I have never done these things

How to do better

- Identify critical to quality processes
- Ensure data attribution
  - Select or design DHT that is fit-for-purpose
  - Engage stakeholders (participants, site staff, service providers) in the design of DHT
- Use robust data access controls
  - Some examples include biometrics and multifactor authentication
  - Achieve the intended security without greatly impacting user-friendliness

How to do better, continued

- User management processes and procedures
- Education: training and re-training of site staff
- Data monitoring:
  - Efficacy data: centralized monitoring for anomalies
  - ePROs: monitoring of user access information
    - common or birthdate-based PINs
    - unusual patterns of security questions and answers

Summary

- The **sponsor is responsible** for implementing the expectations for computerized systems to ensure that the **ePRO system data is reliable**. That includes effective access controls.
- Technological advances provide a **variety of options** for access control. **Choose wisely**.
- Take **pro-active steps** to **decrease and manage risk** by selecting DHT that is fit-for-purpose, employing risk-proportionate system controls, educating site staff, and monitoring data throughout your trial.

Thank You!

Elena Boley, MD, MBA
Senior Physician, Office of Scientific Investigations
Division of Clinical Compliance Evaluation, Office of Compliance
CDER | US FDA

Acknowledgements: Kassa Ayalew MD, MPH
Jenn Sellers MD, PhD; Cheryl Grandinetti, PharmD
Frederic Moulin, DVM, PhD

Compliance Fundamentals Case Study of a Hybrid System

Debbi Fox: Compliance Specialist | Health Canada

A Joint US-FDA | MHRA-UK | Health Canada Good Clinical Practice & Pharmacovigilance Compliance Workshop
February 13, 2024

Medicines & Healthcare products Regulatory Agency

Health Canada Santé Canada

Overview

A brief refresher of some key compliance considerations for all DHTs

A case study that illustrates some of the risks and negative outcomes of using an electronic system that has not been validated for its intended use.

Compliance Considerations for all DHTs

- The key is to ensure GCP requirements for Data Integrity (DI) are implemented throughout the data lifecycle of all records.
- Requires adequate planning and risk assessment prior to system implementation.
- System design and adequate controls for all record formats are important.
- Collect the right data with appropriate tools.

Compliance Fundamentals

- Define and control data flow.
- Risk identification and management procedures.
- Electronic systems require validation (for intended use).
- Implement adequate procedures/training.
- System controls/ access /oversight.

Case Study: Hybrid System

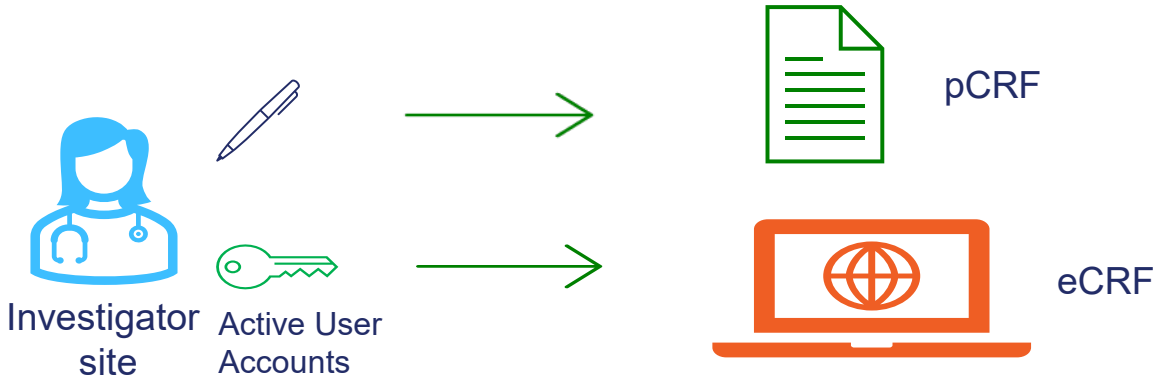
Clinical trial records are created, modified and maintained in both paper and electronic format.

Case Study Overview

- Sponsor did not validate the EDC software sourced for use in the clinical trial.
- Sponsor used a paper CRF (pCRF) for initial data capture.
- An electronic CRF (eCRF) was also used at investigator sites "in parallel" to the pCRF for study data collection.
- Multiple data integrity issues

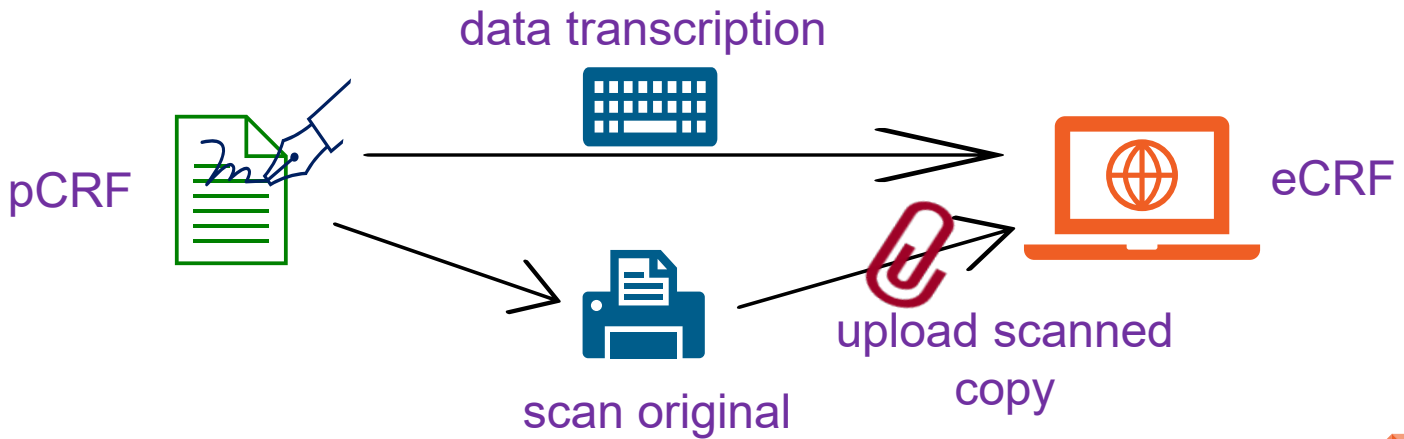
System Implementation

- The investigator sites were provided paper CRFs and access to the eCRF.



System Implementation (cont'd)

- Sites instructed to complete the paper CRFs, enter the corresponding data into the eCRF then scan the paper CRFs and upload the scans to the e-CRF.



Case Study: Hybrid System

Emerging Issues

Duplicate records

Divergent records

Compromised data integrity

Scope of use of electronic system changed over time

Challenging to reconcile all records

Records

- Two systems used to capture study data caused confusion at investigator sites.
- The sites used the tools provided by the sponsor however sites not aware that the e-system was not validated.
- pCRF pages were not always completed with all required information including dates and initials/signatures to attribute entries to authorized study personnel.

Records (cont'd)

- Scans of paper CRFs were uploaded creating duplicate uncontrolled copies of records.
- No control over modification to the records resulting in multiple versions of scanned documents.
- Divergent records were created when scans were printed from the electronic system and additional information was recorded on the printouts.
- Major impact to the data integrity of all records.

Scope Change

- During the study the sponsor began to import lab data directly into the electronic system.
- Data was then exported and used to prepare data listings that were provided to the IDMC for decision making purposes.
- Study decisions were based on the data entered and imported into the electronic system without supporting system validation.

Contributing Factors

- The sponsor did not validate the EDC software prior to use.
- The sponsor failed to identify manage and mitigate the risks associated with the data flow.
- Data Governance procedures did not ensure data capture followed Data Integrity Principles.

Summary

- DHTs should be designed with DI principles in mind
- Remember these compliance fundamentals to maintain integrity of the data
  - Understand and define data flow
  - Identify and manage risks
  - Validate all electronic systems for their intended use in the data lifecycle
  - Implement adequate controls/ procedures /training

Thank You!

Debbi Fox, BSc
Compliance Specialist
Clinical Trial Compliance Program
Regulatory Operations and Enforcement Branch
Health Canada

U.S. FOOD & DRUG ADMINISTRATION

When Data Integrity Falls
MHRA Case Study

Mandy Budwal-Jagait
Head of GCP
Compliance Team 1, Standards & Compliance
HQA | MHRA

A Joint US-FDA | MHRA-UK | Health Canada Good Clinical Practice & Pharmacovigilance Compliance Workshop
February 13, 2024

Medicines & Healthcare products Regulatory Agency

Health Canada Santé Canada

Overview

- This is a case study of a critical data integrity finding from a CRO inspection. It will highlight how one design error led to a cascade of failures and lack of control processes to maintain the integrity of this pivotal trial.
- ***The example has been simplified to highlight the main learning points***

Overview (2)

- Background
- 1st Critical Finding: Data Integrity Control Processes- Impact Assessment
- 2nd Critical Finding: Data Integrity
- Actions and Lessons Learned
- Summary

Background

Routine GCP Systems inspection of a CRO

Trial in a rare disease in paediatric participants

No other treatment options available

Interim analysis undertaken at time of inspection- primary analysis

Primary endpoint: Clinical Outcome Assessment Questionnaire

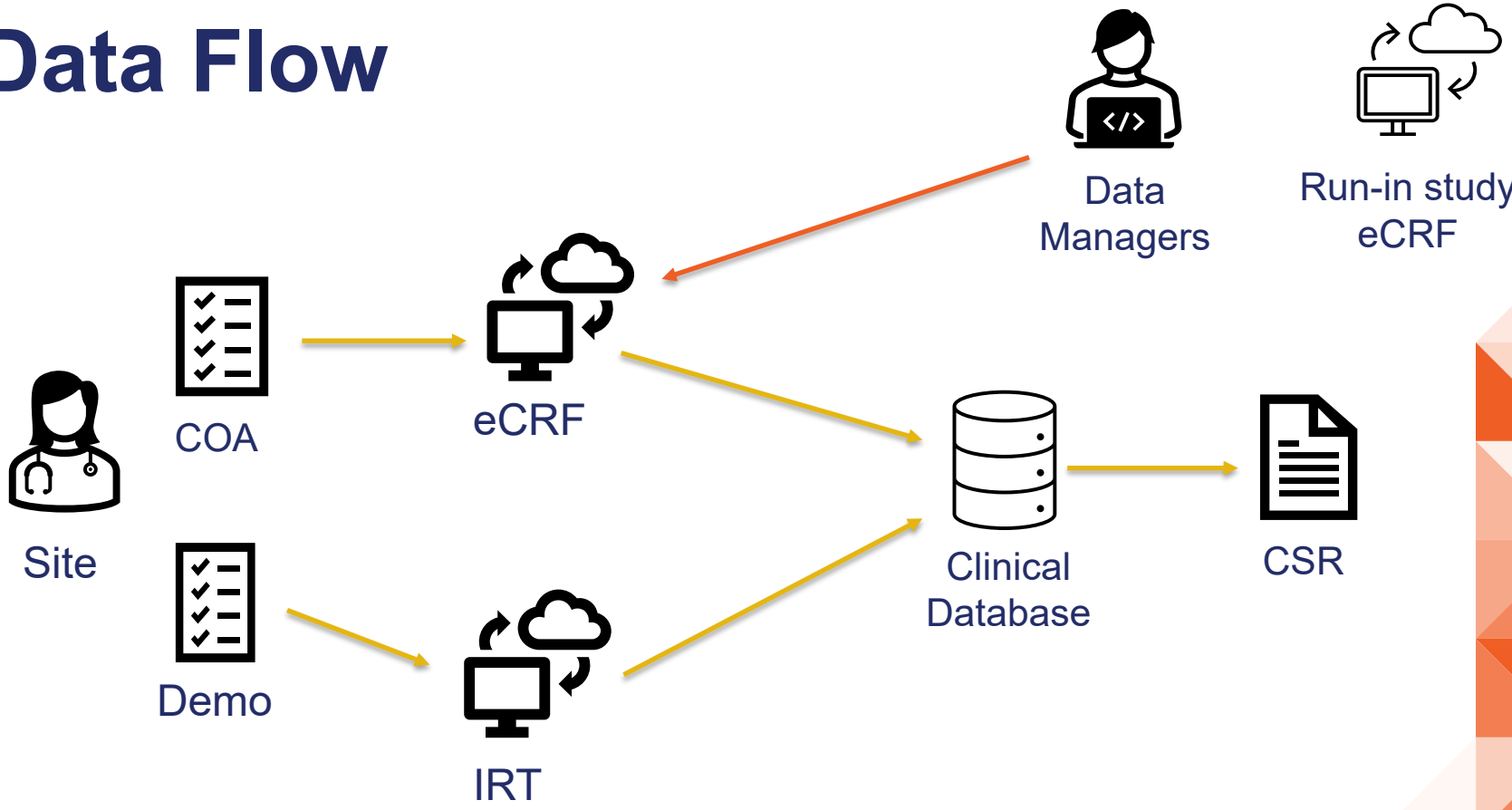
MAA submission planned for the following year

Background (2)

Non interventional run-in study. EOS visit data held in a separate eCRF

Entered as screening visit data for this study (to avoid repeating tests/ data collection)

Data Flow


Data Managers
Run-in study eCRF
COA
eCRF
Site
Clinical Database
CSR
Demo
IRT

Critical Finding for Data Integrity Control Processes (1)

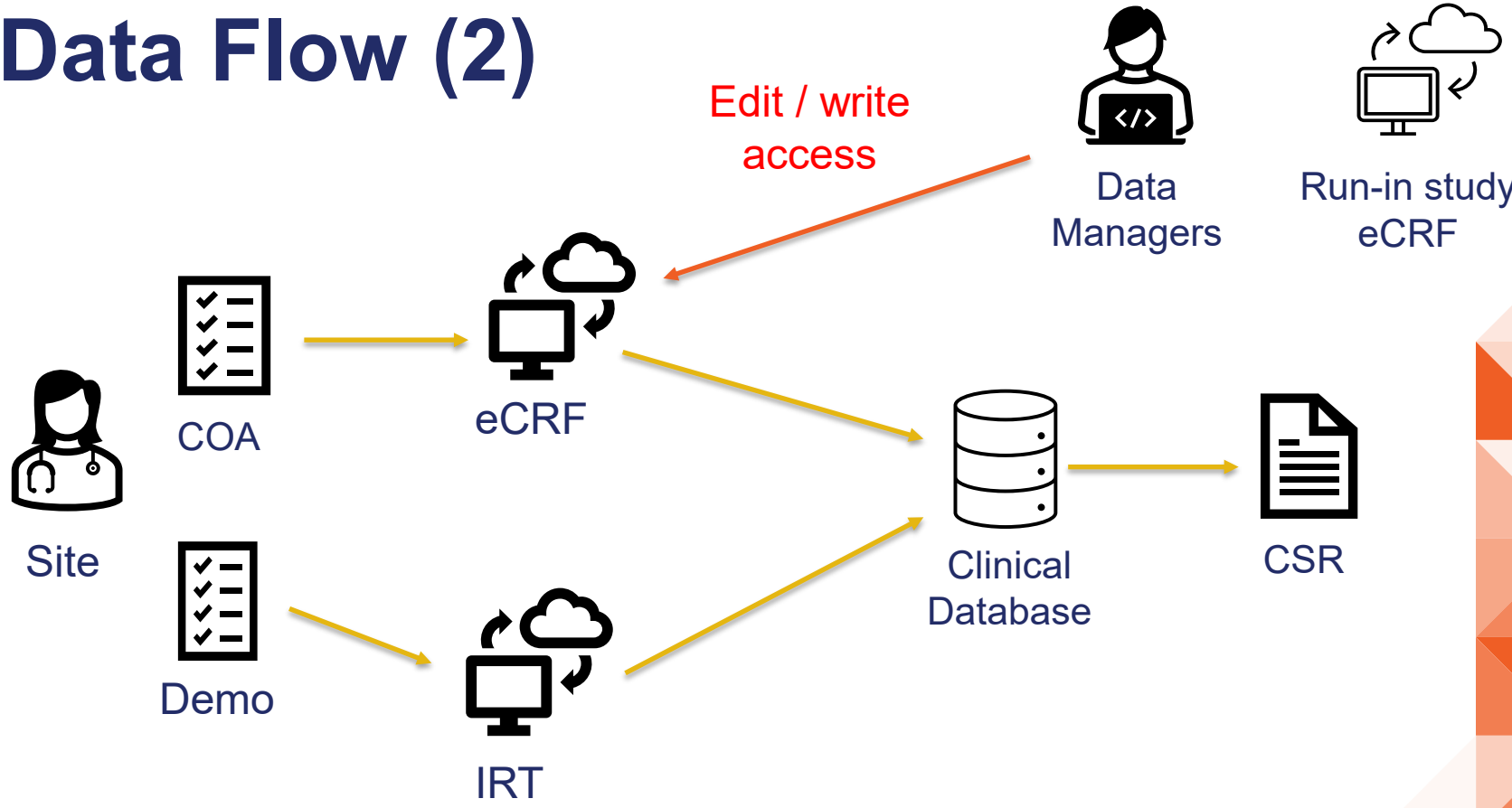
Database lock (DBL) processes

5 DBLs (3 post unblinding)

Analysis of blinded data performed after unblinding

Unable to reconstruct in EDC when pages were locked, unlocked and re-locked to verify what data changed in between.

Data Flow (2)


Edit / write access
Data Managers
Run-in study eCRF
COA
eCRF
Site
Clinical Database
CSR
Demo
IRT

Critical Finding for Data Integrity Control Processes (2)

- CRO staff had edit rights (write access) to the eCRF
- eCRF audit trail format unsuitable
- No review of audit trails for eCRF or IRT
- IRT audit trail unavailable during inspection and system decommissioned (data integrated from IRT to EDC)

Critical Finding for Data Integrity

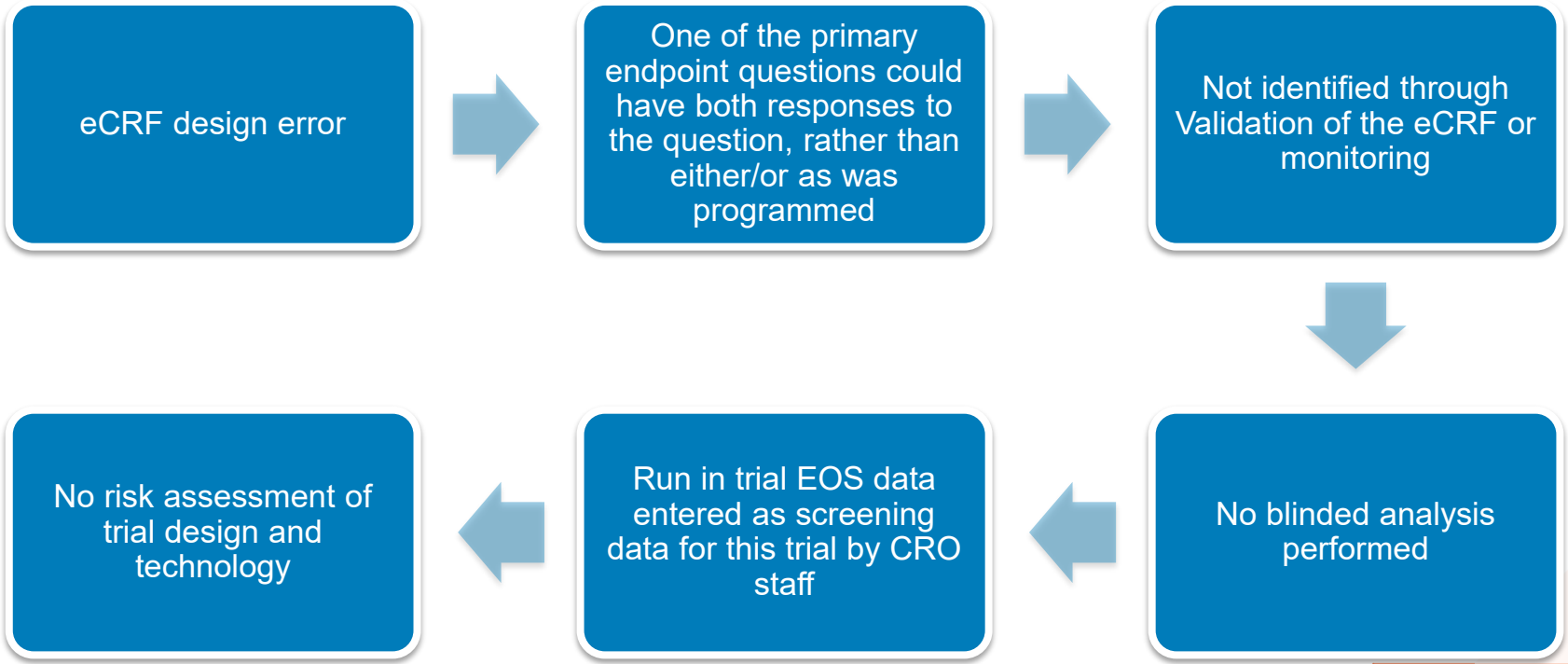
Endpoint data – subjective questionnaire

Evidence of querying endpoint data after unblinding. Missing data point previously SDV'd changed to a value upon querying

Significant potential for bias to be introduced to the trial data

New eCRF audit trail format provided on return inspection unreliable. Manual changes showing as a SYSTEM change

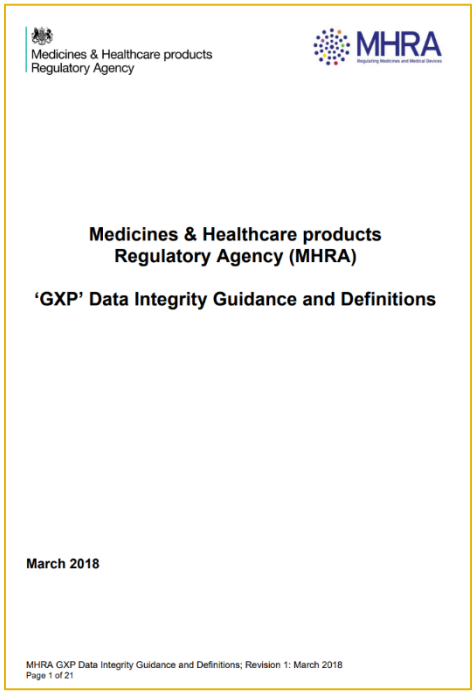
So how did this happen?



Actions

- Critical findings issued to CRO and Sponsor
- Other Regulatory Agencies notified
- Licensing assessor input into CAPA
- Impact assessment and sensitivity analysis to be submitted with MAA
- Issue transparently described in CSR and MAA

Importance of Data Integrity Control Processes


Medicines & Healthcare products Regulatory Agency

MHRA

Medicines & Healthcare products Regulatory Agency (MHRA)

'GXP' Data Integrity Guidance and Definitions

March 2018

MHRA GXP Data Integrity Guidance and Definitions; Revision 1: March 2018
Page 1 of 21

- CRO did not follow own SOPs
- Lack of QC checks to ensure the integrity of data
- No risk assessment performed at trial start or when issue identified.
- Lack of impact assessment and steps taken to minimise potential bias.

https://www.gov.uk/government/publications/guidance-on-gxp-data-integrity

Summary

- Importance of mapping out critical data flow and validating/ QC along the way
- The data in the eCRF is owned by the Investigator.
- Audit trail review as per your risk assessment. Why are you performing a review? What questions do you want answering?
- Identify critical to quality factors and data points in your risk assessment. Consider technology and access rights.
- If something goes wrong, risk assess and undertake an impact assessment. Report as required (PD, Serious Breach or CSR)

Closing Thought

Failure to ensure data integrity could result in patient harm or your data not being accepted for an MAA.

Think about the real impact on patients. Parents were waiting for this product as it may save their child's life.

Thank You!

Mandy Budwal-Jagait, MSc
Head of GCP and Lead Senior GCP Inspector | MHRA

Resources

- MHRA GXP Data Integrity Guidance
- MHRA Inspectorate Blog
  - Is your eSystem an eCRF
  - MHRA and FDA Joint Paper ‘Data Integrity in Global Clinical Trials’
- MHRA GCP Website
- MHRA Customer Experience Centre: info@mhra.gov.uk
- MHRA Clinical Trials Helpline: ctdhelpline@mhra.gov.uk

Copyright information

FDA U.S. FOOD & DRUG ADMINISTRATION

Questions?

Medicines & Healthcare products Regulatory Agency

Health Canada Santé Canada