Forensic Science Regulator
Overseeing Quality

Lessons Learnt

Issue 8/ 2019

Data Audit Findings

Key Words: Data integrity, audit, hazard analysis and critical control point (HACCP).

Following a serious data handling issue identified at one forensic science provider (FSP), the Regulator wrote to other FSPs that provide a significant toxicology service to ensure that they incorporated a data integrity audit into their schedule of internal audits. Internal audits are carried out in greater depth than inspections or assessment visits for accreditation.

Although this was a specific request for an extra audit in response to an issue, in general all procedures/methods should already have been subject to an audit that should include sampling data at any critical stages to ensure that the safeguards are effective. The aim of this audit was to detect whether there is any evidence of the questionable practices in handling and reporting of results that had been seen in one company. Although, no evidence was found in audits that the targeted issues had occurred, potential vulnerabilities or risks were spotted that others could learn from in designing their future audits. It should be borne in mind, the presence of a risk is not evidence that the risk has occurred (i.e. become an issue) or will occur, and ought not to be used as the basis for a 'fishing exercise'. Lord Bingham made clear in R. v. H. & C. [2004] 2AC134, [2004] UKHL 3 at [35]:

"The trial process is not well served if the defence are permitted to make general and unspecified allegations and then seek far-reaching disclosure in the hope that material may turn up to make them good".

Of course, if inappropriate data handling has actually been identified that affects casework, there is a clear disclosure requirement.

In conducting the audit, various overall approaches were taken. Almost all used an element of vertical audit, drilling down from records in the case file, to cross reference with the raw data, checking batch validation data, competence records of staff as well as method validation data, etc. The planning of the audit typically included setting out the sampling technique as well as the composition of the audit team and its collective competence.

Investigation items to consider based on the findings of the audit

A full audit plan based upon the organisation's activities is required. However, the following questions arose during the data integrity audits, which may assist this process.

Responses to these questions should be risk assessed and any unacceptable vulnerabilities need to be managed.

1. Is it possible to change the data after entry or transfer to a spreadsheet, and what risk does this pose?
2. Is it possible to demonstrate who has completed or changed a spreadsheet entry?
3. Is it possible to change the time and date on an instrument's computer?
4. Are instrument's computers part of your organisation's IT back-up service?
5. Are the back-ups adequate and do they comply with the storage periods in the FSR's Codes of Practice and Conduct (the Codes)?
6. Is the risk of cyber threats considered and mitigated against if an instrument's computer is connected to a network?
7. Do records capture what changes are made to key data, and by whom; for instance, peak integration adjustments or updating a database?
8. Is the legitimate deletion of data (e.g. internal standard failure) traceable on the screen and/or printouts?
9. Is it appropriate for the same individuals to be routinely checking and/or witnessing each other's work?
10. Are individual staff log-ons used for each of the analytical instruments, e.g. use of administrator and user log-ons?

11. Are checks of data integrity in the validation procedures adequate, e.g. does the validation need to include a specific section on data integrity checks?

12. Are transfers of key data assured?

13. Are all paper record corrections traceable through initialling and dating?

14. If macros are used, are they validated, and if the macro is reliant on the user selection of a template, does the critical findings check procedure include a specific check that the correct template is selected?

Critical Control Point

The Regulator specifies process mapping to help to identify critical control points for the potential hazard of contamination. This is loosely based upon the hazard analysis and critical control point (HACCP) methodology used in the food and pharmaceutical industry. In these fields, several hazard types are looked at the same time and the next version of the FSR's Codes will include this approach for data vulnerabilities.

Assessing how to protect critical control points ought to be conducted during method development and validation. However, the continuing effectiveness of the control measures should be part of internal audits. This allows for an assessment of what are critical data and allows proper focus on what is relevant.

Codes of practice and conduct

The next version of the FSR's Codes (Version 5) will incorporate the key learning from the audits. The main relevant changes from the previous version are in grey below.

21.3 Electronic information security

21.3.1 The forensic unit shall establish and document a policy and procedure for the management of electronic information based on business and security requirements and include this in the schedule of regular audit and review.

21.3.2 The policy and procedure should include a formal method of granting and removing access rights, privileges and password control.

21.3.3 The policy and procedure should include:

a) the selection and use of passwords;

b) that unattended equipment has appropriate protection;

c) a clear desk and screen policy;

d) management of removable storage media;

e) segregation of developmental and operational IT environments;

f) network security;

g) identification of critical control points (i.e. places where data are entered, transferred, stored or processed in a manner where they may be vulnerable to corruption, errors, unauthorised manipulation, etc.).

h) protection steps to prevent loss, corruption (deliberate, degraded, actual or suspected) and unauthorised access to and/or amendment of all electronic records identified by assessment as key data,[1] and for maintaining an audit trail; and

i) the method of sampling of key data to check that protection steps have been effective, and the results are reliable and analytically sound.

Further reading

Lessons Learnt: Manipulation of data (Issue 5/2019).

www.gov.uk/government/publications/forensic-science-lessons-learnt-issue-5

Forensic Science Regulator's (FSR's) Codes of Practice and Conduct.

www.gov.uk/government/collections/forensic-science-providers-codes-of-practice-and-conduct