Detecting Data Integrity Issues

Mark E Newton
Consultant-QA, Global Lab Informatics
newton_mark_e@lilly.com

Agenda

- Expectation of Oversight
- Detection by Inspection
- Data Review
- Analytics for Data Integrity
- Some “Quick Wins”

Expectation: Oversight

Regulators expect firms to routinely look for improper activities as part of review

- “There was a lack of **basic oversight** by operations, quality unit, and site managers, as rewriting and destruction of original CGMP records was allowed to persist over a significant period without *implementation of systems and controls to prevent data manipulation*”. – Sun Pharmaceuticals 2014-May
- “Failure of your quality unit to properly *review production records* and *detect instances* where testing was not performed to support your company’s certifications on your COAs.” – Canton Labs 2014-Feb
- “Your firm’s failure to *prevent, detect, and rectify* the falsification of your GMP documentation is concerning.” – Posh Chemicals 2013-Aug

Detection by Inspection

- Change the approach
- Detecting good design
- Detecting good execution
- Warning signs

Detection by Inspection

Change the approach

- Spend time on the floor
- Practice vs. promise
- Look at live data
- Identify queries that indicate overall health- use them!

Detection by Inspection

Detecting good design

- Requirements include critical audit trails
- Process/data flow diagram, with risks to data integrity identified and prioritized
- Mitigations planned for gaps, and included in performance testing
- Justification of configuration choices and their contribution to data integrity

Detection by Inspection

Detecting good execution

- Where are GMP records in work area? Near people, on desks…
- Are procedures near activities, or do people go on memory?
- If electronic, are entry terminals near work?
- Sticky notes in use?
- Users leave open sessions during work?

Warning Signs

- Shared passwords
- Enhanced roles for everyone
- Admin sits with users
- Use reports for data review

Data Review

Review procedures include:

- Review of original data at the source-not a report
- Give reviewers, QA access and training to review electronic data
- Identify critical audit trails and complete record set for review

Consider use of custom queries for reviews

Analytics: Limitations

- 1 report record = 1 real integrity issue is not reality
  - Most "issues" on reports have a logical explanation
- Some real issues never make it to a report
  - Data in memory is deleted before a save (it is gone!)
  - e.g. Balance data is viewed, deleted and re-weighed
- Manually prepared data analytics do not last
  - Heavy time resources, hard to use….seldom effective
- Manually-entered data is problematic
  - Transcription errors, manipulated before entry
  - Need real-time verification instead
- "Manipulators" can become more clever
  - E.g. change sample naming schemes to avoid detection

Analytics: Limitations

Analytics should be thoughtfully used because….

- Each has a different optimum frequency of use
- Each "signal" requires investigation (e.g. resources)
- Can get buried in mounds of useful data (e.g. noise)—and real signals are missed
- Time to develop an analytic might be better used in other activities (e.g. improved technical controls, training, validation/configuration)

Start small and assess the value of each by trial

Sample Analytics

Many of these are based on enforcement actions--

- See: enforcement observation
- Ask: "could that be detected/prevented with a query?"

- *These do not include a backup verification report, which is a common data integrity-related enforcement citation and should probably be the first analytic created*

Sample Analytics

Right First Time

Source	LIMS/ELN, Batch Release
Description	List of tests that required rework prior to release. May include analyst ID, date/time, batch, material name, method ID. Might also include a summary percentage: rework % for a given material or method ID.
Note	This is typically done using an audit trail that lists status changes of the tests/samples, looking for those with 2+ audit records of "ready for review" and/or "released to QA" Indicates a test/sample requiring re-processing due to errors that were not detected prior to review and/or release, depending on status. Can illuminate trends in methods, materials or analysts with rework rates above the rest of the population.

Sample Analytics

Manual Peak Integrations

Source	Chromatography
Description	By Method ID, provides a count of manual integration peaks vs. auto-integrated peaks
Note	Provides a view of methods where efforts can be expended to reduce manual peak integration, resulting in efficiency increases and reducing enhanced reviews due to manual processes
Enforcement	"There was no Standard Operation Procedures (SOP) to describe the policy, standard practice, and circumstances under which manual integration would be allowed" *Micro Labs Warning Letter 2014-May*

Sample Analytics

Manual Integration Detail

Source	Chromatography
Description	In each run, lists peaks with manual integration and **Count of audit trail entries**
Note	The Count of entries can illuminate injections where more manual intervention is happening, thereby deserving of closer review. This can happen when analysts engage in "integration until passing" types of behavior. With methods that require manual integration, there could be large numbers of peaks for each run. One variation: set a threshold count to be met before peaks appear, so routine activity is removed, to focus on exceptional manual actions
Enforcement	"your firm reintegrated multiple chromatograms to determine (b)(4) levels; however, the parameters for the reintegration were not retained." *Cadila Pharma Ltd 2014-Oct*

Sample Analytics

Duplicate File

Source	LIMS/ELN, Lab Execution System, Standalone systems, Data Storage Areas
Description	List of files in a library (or set of libraries) with identical checksum, or with identical File Creation Dates.
Note	Data in the file will be the same (checksum might be the same as well), but sample ID will change. Usually a copy will retain the same File Creation Date, but Last Modified Date will differ. Checksum will likely fail if Sample ID or other metadata is embedded in file.
Enforcement	"Your firm used the IR spectra for one lot to approve and release two subsequent incoming lots." *Xian Libang Pharmaceutical Co., Ltd. 2010-Jan* "HPLC Chromatograms had been copied from previous batches and renamed with different batch and file names." *Zhejiang Apeloa Kangyu Bio-Pharmaceutical Co. Ltd. 2014-Nov*

Sample Analytics

Short Run

Source	Chromatography
Description	List of sample runs with a small number of injections (e.g. 1-2)
Note	List Run #, Method ID, Sample ID(s), # Injections, Analyst ID Users engaging in "testing into compliance" behaviors will inject sample solution multiple times, often in short runs. Could allow report to have an adjustable minimum injection value, for added flexibility
Enforcement	"Your firm acknowledged that the analysts involved in performing single injections failed to follow good laboratory practices described in the SOP "General Laboratory Working," and that the analysts conducting the injections in question made decisions to perform unauthorized, unapproved injections." *Apotex Research Private Ltd 2015-Jan*

Sample Analytics

Date of Last Access

Source	LIMS/ELN, Lab Execution System, Standalone systems, Data Storage Areas, Chromatography, Electronic Batch Records
Description	Last time target system was accessed by each active user.
Note	Lists User ID, User Name, Role, Last Access Date Can identify people not using the system who can be removed without impact. In some circumstances, can point to account hijacking (e.g." I did not use the system last week") Useless if shared accounts are used

Sample Analytics

Convert to Manual

Source	LIMS/ELN, Lab Execution System, Chromatography, Electronic Batch Record System
Description	List of Sample/Test IDs where a manual override was performed for an automated step/calculation This is only valid for systems that permit manual override AND have an audit trail that captures change
Note	Include Analyst ID, Method ID, Material ID, Batch ID, (step), (reason for override) Can be valid reasons for override, but merits enhanced review due to risk of inaccuracy/falsification

Sample Analytics

Employee Performance

Source	LIMS/ELN, Lab Execution System, Chromatography, EBRS
Description	List of performance times by the various employees in a group
Note	List by Method ID and User ID: mean time to execute method/process step, # sample/test records released in a given time period Looking for employees whose performance deviates from normal (good or bad), in both time to perform method and # sample/tests released. This has both efficiency and data integrity uses. Could indicate performance levels “too good to be true”

Sample Analytics

Data Review

Source	LIMS/ELN, Lab Execution System, Chromatography, EBRS
Description	List of review activities, with mean time to perform activity by each person
Note	List by Activity, Analyst ID: mean time, # records in a given time period. This requires status changes or some other means to capture start/stop times. Differences could reveal shortcuts taken in review, such as failure to look at source data.

Sample Analytics

Access Changes

Source	Any system
Description	List of access changes (historical) for all people using a system
Note	List of security-related changes, including User ID, (site) date/time of change, new Role, Person making change Could indicate improper role changes for people, including conflicts of interest. For global systems, this could be performed for all sites, giving the added perspective of comparing sites for levels of security activity (e.g. Site Y makes twice the security changes as Site Z even though they are similar in size.) Pair this with the Access Roster, which lists current users
Enforcement	"Your quality control analysts used administrator privileges to change the controls for the time and date settings and manipulate file names to overwrite injections and delete original HPLC test data. Analysts also routinely turned HPLC audit trails on and off." *Sri Krishna Pharmaceuticals Ltd. - Unit II 2016-Apr*

Sample Analytics

Aborted Runs

Source	Chromatography, Standalone Systems
Description	List of people, by access role, using a system (point in time)
Note	List of aborted runs over a date range, including Method ID, Run #, position in run when aborted, reason to abort, date/time, User ID performing action. Systems that put a status on aborted runs to differentiate them from other runs can create this report. Some systems allow users to end a run with no audit trail record.
Enforcement	"Your response regarding the failure to maintain complete laboratory records of KF raw data states, in part, we were not able to find the four printouts of the Karl Fischer instrument.... and, the missing printouts were probably aborted instrument runs that were not filed with the complete sequence of analysis." *Cambrex Profarmaco Milano Srl 2009-Aug*

Sample Analytics

"Demo/Test/Trial"

Source	Chromatography, Standalone Systems
Description	List of samples with suspicious names
Note	Look for files named "demo%, "test%", or "trial%" and samples with the same name(s) in systems Should always question why users are doing this in a GxP environment; even if proper activity
Enforcement	"the inspection found multiple raw data chromatograms in digital files labeled 'test' and 'demo' that were injected prior to the sample injections that were used to conclude that batches were in conformance with the specification" Fresenius Kabi 2013-Jul "employees in both of your Quality Control (QC) laboratories had frequently conducted unauthorized 'trial' High Performance Liquid Chromatography (HPLC) injections prior to additional injections that were used in the reported test results.... The data from 'trial' injections was not reviewed or considered in determining batch quality" Micro Labs Ltd 2015-Jan

"Quick Wins"

- Chromatography SOP
- Standalone Instrument Review
- Training
- Interface Review
- Elevated Access Review

"Quick Wins"

Chromatography SOP

- **Every** injection has a purpose! Must be justified by method, protocol or procedure
- When is manual integration acceptable? Process to review?
- Are drift, system stability or other injections acceptable? How reviewed?

Failure to present and review the complete record of testing - 21CFR211.194(a) - is one of the most common Warning Letter citations!

"Quick Wins"

Standalone Instrument Review

- Review each for integrity gaps
- Review access roles
- Check Recycle Bins for records!
- Consider disabling Recycle Bin
- Adequate archive/recovery ?
- Consider use of Alternate Windows Shell to address integrity gaps

"Quick Wins"

Training

- ALCOA+ Principles
- Good documentation behaviors
- Detecting unexpected data
- Review of Raw Data
- Managing for Integrity (leaders)

Everything we do requires people!
Data Integrity is >50% Human Factors

"Quick Wins"

Interface Review

- How many failures/restarts last 12 mos?
- Who owns the interface?
- Is the interface validated?
- What "bad" decisions result, if fails?
- Who/how is interface failure notified?
- Is failure easily detected-or not?

"Quick Wins"

Elevated Access Review

- Start with roster of administrators
- Review for # of admins-challenge each!
- Verify: no conflicts of interest
- Any default admin accounts in system?
  - Many printed in user guide w/password!
- Look for improper service provider access (e.g. former employees)

- END -

Mark E Newton
Eli Lilly and Company
Indianapolis, IN 46285
newton_mark_e@lilly.com