Data Integrity and APIs
The Regulatory Perspective

PDA-PIC/S
ICH Q7 Training
Hyderabad/Ahmedabad, India
September 2015

Carmelo Rosa, MS, Psy.D.
Director, Division Drug Quality-I
CDER/OC/OMQ
US FDA

Topics

- Definitions
- Why is data integrity important
- Common data integrity problems
- Red flags for FDA
- Data integrity case study
- Current trends
- How to resolve data integrity problems

General Objectives

Apply Q7 Principals to Data Integrity Practices

Explain Regulators Expectation

Distinction between a GMP deficiency versus a data integrity practice

Recent Examples of Data Integrity

Definitions

- Data integrity may mean:
  - accurate and reliable data and information
  - ensuring data trustworthiness and reliability, as related to the security of the information/data
    - See FDA's Guidance to Industry: Part 11, Electronic Records; Electronic Signatures — Scope and Application, available at http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM070295.pdf
  - the degree to which a collection of data is complete, consistent, and accurate. Syn: data quality
    - IEEE definition
    - See Glossary of Computer Systems Software Development Terminology (8/95), available at http://www.fda.gov/ICECI/Inspections/InspectionGuides/ucm074875.htm
  - ALCOA: Attributable, Legible, Contemporaneous, Original, and Accurate
    - Under Good Clinical Principles, FDA may look to see that the process of data creation at the site can be reconstructed and that it matches the information submitted to the agency. If problems are discovered, the integrity of the data are questionable.

What is Data Integrity?

- Refers to requirements for complete, consistent, and accurate data

- Data should be attributable, legible, contemporaneously recorded, original or a true copy, and accurate (ALCOA)

- The concept of data integrity underpins CGMPs and is a requirement for electronic record keeping and the use of electronic signatures

Why is Data Integrity Important?

- Undermines the safety and efficacy and/or assurance of quality of the drugs that consumers will take
- Data integrity problems break trust/confidence
- We rely largely on trusting the firm to do the right thing when we are not there
- Lets us rely on the information used to ensure the quality of the drugs our patients will take

Why Data Integrity Matters

Data integrity breaches casts doubt on all results and records.

- Can we trust what we see during an inspection?
- Are drugs within specification?
- Is data submitted in applications to FDA reliable and truthful?
- Can we be confident in providing these drugs to patients?

Why Data Integrity Matters

Data integrity breach: often leads to adulterated drug under U.S. law

Drug is adulterated because data integrity breach is a violation of CGMP.

- Under U.S. law, adulterated drug is subject to detention.
- Generally, significant CGMP issues require re-inspection.
- Firms must fix problems and be re-inspected.

Why Data Integrity Matters

"…the term 'current good manufacturing practice' includes the implementation of **oversight** and controls **over the manufacture of drugs to ensure quality**, including **managing** the risk of and establishing the safety of raw materials, materials used in the manufacturing of drugs, and finished drug products."

Food and Drug Administration Safety and Innovation Act, Sec. 711 Enhancing the Safety and Quality of the Drug Supply

Why Data Integrity Matters

If data integrity has failed, what needs fixing?

- Data integrity – illuminates state of the quality system
- Serious data integrity problems – deficient quality systems
- Quality systems require sustained effort and resources to fix.
- Changing culture; much harder than changing equipment.

Data Integrity and Quality System

- GMP requirements' central objective: a system (policies and processes) that prevents errors and defects – Pharmaceutical Quality System
- PQS success assures an ongoing state of control.
- PQS culture means vigilance, timely action, early warning of emerging quality issues.

Data Integrity and Quality System

Managers should establish a **vigilant quality culture** in which:

- Timely action prevents risks to quality
- Lifecycle adaptations address manufacturing weaknesses and continually improve systems
- Effective process performance and product quality monitoring provide early warning of emerging quality issues
- Systemic solutions are implemented rather than ineffective shortcuts
- Small problems are habitually fixed to prevent their accumulation into costly, complex problems

Red Flags for Regulators

- Manual processes
- No complaints, deviations or out-of-specification investigations
- No archival data (i.e., microbiological test results, thin layer chromatography, titration)
- Rushed/increased first-to-file applications
- Firms with a large volume of applications
- Disconnection within critical units at site
- Limited or no QU over site of CGMP functions activities

Special Note

Contractors

Data integrity is not only about ensuring your data is accurate and reliable, but also ensuring that your contractors' data is accurate and reliable.

Common Data Integrity Problems

- Not recording activities contemporaneously
- Backdating
- Fabricating data
- Copying existing data as new data
- Re-running samples
- Discarding data
- Incomplete or altered data
- Testing into compliance

Common Data Integrity Problems

- Releasing failing product on basis of a passing result with no investigation to justify invalidating failing result.

- Conducting trial injections or pre-official testing of samples and reporting the best or only passing results

- Testing of samples outside the oversight of the QU

Common Data Integrity Problems

- Failure to review source electronic data
- Loss of data during changes to the system
- Failure to retain raw data
- Turning off audit trail capabilities
- Password sharing
- Inadequate controls for access privileges
- Manipulating integration parameters

5th Most Common Citation

- Your firm did not document laboratory activities ***at the time of performance*** Cited in 3 warning letters
  - Pre-dating or backdating laboratory records
  - Occurred for assay, loss on drying, sample weighing, and stability testing

4th Most Common Citation

- Your firm failed to maintain ***complete information*** relating to the production and control of each batch
- Cited in 5 warning letters
  - Records for 23 batches did not contain batch numbers, manufacturing dates, expiration or retest dates
  - Approximately 75 ripped batch production records (BPRs) were found in the garbage (some with failing results)

4th Most Common Citation

- Ten bags of torn or partially destroyed original records including CAPAs, preventative maintenance forms, and calibration records were found
- Raw data was written on scratch paper and sometimes differed from the data in the BPR
- Correction fluid was used on production records

3rd Most Common Citation

- Your firm failed to thoroughly investigate any unexplained discrepancy or failure of a batch or any of its components to meet any of it specifications, whether or not the batch has already been distributed
  - Cited in 9 warning letters

6th Most Common Citation

- Your firm blended out-of-specification API batches with passing batches to meet specification.
  - Cited in 3 warning letters
  - Failing results were often kept in separate folders and the failing data was not considered when making release decisions

3rd Most Common Citation

- The following discrepancies or failures were not investigated:
  - 4 batches of failing API were used in fifteen finished dosage batches
  - Failing assays were repeated until passing results were obtained (occurred at numerous firms)
  - Environmental monitoring results were recorded as zero but actually had growth

2nd Most Common Citation

- Cited in numerous warning letters:
  - Audit trails were disabled
  - A shared username and password was used by many analysts
  - Users were able to manipulate, delete, or overwrite electronic raw data
- Firm's laboratory practice is to print chromatograms and delete electronic raw data files

Most Common Citation

- Your firm failed to ensure that laboratory records included ***complete data*** derived from all tests necessary to assure compliance with established specifications and standards

- Cited in 21 warning letters

Most Common Citation

- Cited in numerous warning letters as failure to retain complete data:
  - "trial" sample injection data was not kept as part of the data for a batch
  - Sample weights, sample preparation and sample dilutions were not retained
  - Deleted data detected in audit trails
  - Overwriting data
  - Ripped up data found in the garbage

Most Common Citation

- Microbiological data missing:
  - Not reporting microbiological counts
  - Hundreds of environmental monitoring samples were not collected
  - Some microbiological sample plates/tubes were missing from the incubator
  - No microbiological testing was conducted; however, microbiological test results were reported on the certificate of analysis (COA)

Most Common Citation

- Certificates of analysis missing data:
  - Data on the COA sent with the batches was different than the COA the firm retained on file
  - COA retest date was changed to an expiration date and listed as eleven months later
- No raw data in support of results reported on COA
- Samples with no identification were discarded during the inspection

Most Common Citation

- Firm deleted all electronic raw data supporting HPLC release testing
- Standards were injected and used as sample results
- Duplicate logbooks were kept
- Complete raw data to support test method validation was not retained
- Integration parameters for HPLC analysis were not retained

Data Integrity Deficiencies Example (WLs)

- Quality Control Data
  - Test results for one batch were used to release other batches
  - Occurred for at least 3 batches
  - This happened at three unrelated firms

Data Integrity Deficiencies WL Example

- Quality Control Data
  - Destruction of raw data not meeting specification
  - Missing raw data
  - Re-writing laboratory notebooks
  - Unjustified invalidation of data and re-testing without a laboratory investigation
  - Refused to allow FDA to talk to employees

Data Integrity Deficiencies WL Example

- Microbiological testing
  - Growth on microbiological plates was observed and recorded as no growth
  - The plates were double checked by a second employee
  - This happened at three unrelated firms manufacturing sterile finished dosage forms

Data Integrity Deficiencies WL Example

- Making up records during an FDA inspection
  - Batch records
  - Training records

Data Integrity Deficiencies WL Examples

Recent examples:

- Invented sterility test data
- Invented media fill data
- Invented WFI system testing
- More lab work assigned than could possibly be done
- Out of Specification results not investigated

What is a regulator to do when he or she finds deficiencies like these?

Data Integrity Case Study

- 16 HPLC “trial” runs were discovered prior to the sample assay
  - In at least one case the trial run failed while the sample assay passed
  - Trial runs were not reported with assay results
  - Trial and sample runs differed significantly in assay result
  - All other trial runs were deleted prior to the inspection (encompassed 12 instruments)

Data Integrity Case Study

- All HPLC systems were stand alone systems that had a pop-up window that would present the option to delete a file
  - Included 16 HPLC systems
  - There were no audit trails or record of deletion
  - Back-ups occurred once a month
  - Common accounts with shared passwords

Data Integrity Case Study

- Production operations were not documented at the time of performance
  - Observed by the investigator
  - Operator admitted to the practice

What Can Data Integrity Problems Mean for Your Firm?

- Patient Harm/Recalls
- Warning or Untitled Letter
- Import Alert/Injunction/Seizure
- Application Integrity Policy Invocation
- Criminal Investigation
- The Agency has recently been using consent decrees as a way to address data integrity problems

How Can You Be Part of the Solution

- Look for gaps in how you control your records
- Ensure employees have appropriate user privileges
- Audit your data in a risk-based manner
- Verify the authenticity of your contractors' data
- Appropriate and redundancy check and balance/more QU oversight

Rebuilding Confidence

Regulatory Expectation Prior to Moving Forward

Remediation – Step 1

FDA requires a ***comprehensive evaluation*** of data integrity deficiencies.

Competent third party consultants highly recommended. Necessary to have experience in:

- assessing data integrity
- crafting remediation plans
- regulatory agencies' expectations- FULL TRANSPARENCY
- must be qualified and impartial

Comprehensive Evaluation 1

*"…a **comprehensive evaluation** of the extent of the inaccuracy of the reported data. As part of your comprehensive evaluation, provide a detailed action plan to investigate the extent of the deficient documentation practices. . ."*

~ recent FDA warning letter

Comprehensive Evaluation 2

What is FDA looking for in a comprehensive evaluation?

- Detailed description of strategies and procedures for finding scope of problem
- Comprehensive, thorough, and complete evaluation of all systems
- List of records, applications, and other documents that have been/will be examined

Comprehensive Evaluation 2

Examine organizational structure and personnel responsibilities:

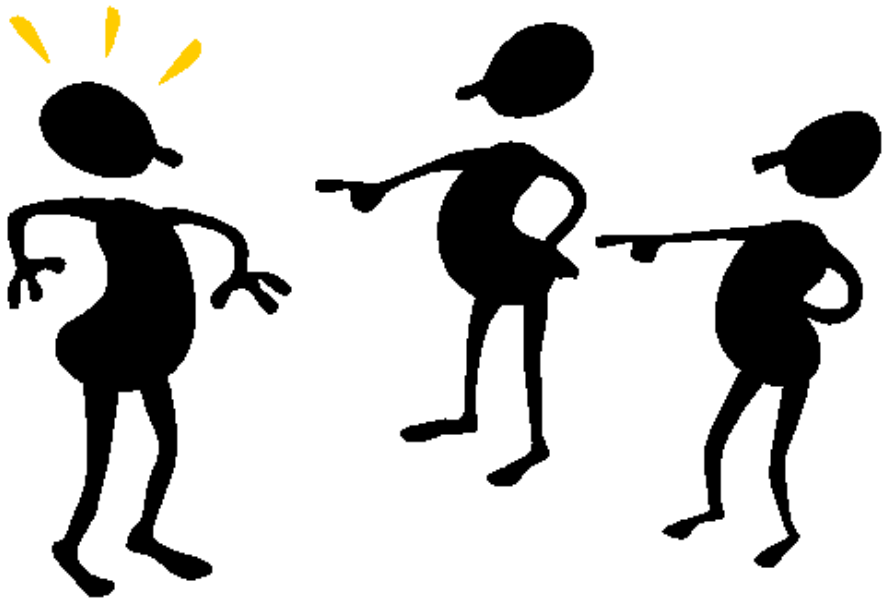
- Nature of management's involvement
- SOPs (Standard Operating Procedures)

(changing an SOP is not enough-gap analysis of what went wrong and why is needed)

- Contract agreements

Comprehensive Evaluation 4

- Who and what is the real source of the problem?
- Temptation is to blame one employee or a small group of employees.
- Firing people who were not responsible for creating the problem will not help.



Comprehensive Evaluation 5

Scope of evaluation

- People – interview people identified by FDA and by consultant.
- Systems – involved in the data integrity breach and other related systems that could have the same problems:
  - raw materials, components and ingredients
  - testing records
  - production and process records
  - equipment

Comprehensive Evaluation 6

- Removal of employees may be necessary but not the sole solution.
- Immediate firing of employee may limit your root cause determination (employee may have attempted to report the wrong doing)
- Assessment of resources available (# of products to make, infrastructure
- Assessment of competency if critical units

Comprehensive Evaluation 7

- Determine the scope of the problem
- Implement a corrective action plan (global)
- Remove individuals responsible for problems from CGMP positions
- Complete a satisfactory inspection, in occasions several satisfactory inspections may be needed (including from different regulators)

Comprehensive Evaluation 8

- Your assessment should not assume that the DI problem was isolated or affected only one system.

- Regulators expect sustainable CAPA throughout the corporation and all its facilities

Remediation – Step 2

Risk assessment of potential effect on drug product quality

Determine effect of deficient documentation practices on the quality of the drug product released for distribution.

Issues:

- Were Out-of-Specification (OOS) drugs shipped?
- If yes, what is impact on patients?
- Even if no OOS drugs were shipped, it is important to maintain appropriate preventative controls.

Remediation – Step 3

"…A **management strategy** that includes the details of your global **corrective action and preventative action plan**."

> "Describe the actions you have taken or will take, such as contacting your customers, recalling product, conducting additional testing, adding lots to your stability programs to assure stability, monitoring of complaints and/or other steps to assure the quality of the product manufactured under the violative conditions."

~ FDA Warning Letter, March 2015

Con't Remediation Step 3

Develop a shot and long term remediation process (1st focus on patient safety, product impact)

Region of products impacted and need to notify different regulatory authorities NOT only the authority who found the problems

Management Strategy

"As part of your corrective action and preventative action plan, describe the actions you…will take, such as revising procedures, implementing new controls, training, or re-training personnel, or other steps to prevent the recurrence of CGMP violations, including breaches of data integrity."

~ FDA Warning Letter, March 2015

Management Strategy 2

- analysis of findings
- consultant's recommendations
- corrective actions taken
- timetable
- identification of responsible persons
- procedures for monitoring the plan

Management Strategy 3

- *Clear accountability* for data integrity in the future
- Consider implementing an enhanced ethics program
- Data integrity problems are not always intentional – sometimes they result from poorly controlled systems.

Data Integrity Remediation Goals

What is the goal of a successful remediation?

We want **you** and the regulators to be able to reconstruct the manufacturing process through records.

We want certainty there is no:

- false data
- omission of data
- hiding of data
- substitution of data

Data Integrity

Applications for FDA approval of new drugs and generics

- FDA investigators may focus on “submission batches.”
- Data integrity breaches in application data can be particularly difficult for companies. Put controls in place to avoid this at all costs.

Closing Comments

- Only request a reinspection when you are ready, as additional similar findings will only delay your process.
- Focus on implementing a sustainable and mature quality culture and not on a quick fix to resume manufacturing.
- Quality has a cost…….

Closing Remarks

Last step in the journey – re-inspection

- Investigators will look at corrective actions.
- Failure to implement corrective actions as promised may:
  - prevent FDA from lifting an import alert
  - create uncertainty about drug applications

Closing Remarks

- **If You Find a Data Integrity Problem**
- Disclose it to regulators.
- Determine the scope of the problem and commit to voluntary remediation.
- FDA – much more willing to work with firms that voluntarily disclose and commit to fixing problems.

Closing Remarks

- Data integrity is in everyone's interests.
- Patients' interests and the firms' interests are very well aligned.
- Interruption of drug supply is difficult for:
  - the firm
  - patients
  - regulators

More Closing Remarks

Unreliable data

- difficult to achieve efficient, reliable, and robust systems
- risk of regulatory action

"I intend to make Alcoa the safest company in America. I intend to go for zero injuries."

— Paul O'Neil, former Alcoa CEO

Alcoa focused on reducing workplace injuries resulted in better managed and more efficient facilities.

Last Word

O'Neil's focus on safety created change that rippled through the whole culture.

- focus on worker safety
- examination of inefficient processes

Same is true for data integrity.

- zero-tolerance approach to data integrity
- benefits beyond patient safety

Good data can help illuminate whether operations are efficient and under control

Questions?

FDA compliance information online:
www.fda.gov/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDER/ucm081992.htm

Quality (Q) Management

1. Q is everyone's responsibility
2. Manufacturers should establish, document, and implement an effective system for managing quality
3. The system for managing quality should encompass the organizational structure, procedures, processes and resources, as well as activities to ensure confidence that the API will meet its intended specifications for quality and purity

Q Management

3. Not being aware of on-going data integrity practices does not exempt one from the responsibility .

WL Language- API Site

SM informed FDA investigators that they were unaware of information generated at the XXX plant that may have an impact on the quality of API. Your SM, at the local and corporate levels, is responsible for assuring that strict corporate standards, procedures, resources, and communication processes are in place to detect and prevent breaches in data integrity, and that such significant issues are identified, escalated, and addressed in a timely manner.

Q- Management

4. All quality-related activities should be recorded at the time they are performed

5. Any deviation should be documented and explained

Q Management

6. Critical deviations should be investigated, and the investigation and its conclusion should be documented.

Common phrase found under the responsibility of the QU/Production in Q7 is: "MAKING SURE" (MS)

1. MS critical deviations are investigated, resolved, conclusions recorded

2. MS that quality-related complaints are investigated and resolved

3. MS that effective systems are used for maintaining and calibrating critical equipment

One of the most common phrases found in Q7 is: "MAKING SURE" (MS)

4. MS that materials are appropriately tested and the results are reported

5. MS that there is stability data to support retest or expiry dates and storage conditions on APIs and/or intermediates, where appropriate

One of the most common phrases found in Q7 is:

"MAKING SURE" (MS)

6. MS that all production deviations are reported and evaluated and that critical deviations are investigated and the conclusions are recorded

7. MS that production facilities are clean and, when appropriate, disinfected

8. MS that the necessary calibrations are

One of the most common phrases found in Q7 is: "MAKING SURE" (MS)

9. MS that the premises and equipment are maintained and records kept

10. MS that validation protocols and reports are reviewed and approved

11. MS that new and, when appropriate, modified facilities and equipment are qualified

What is DI

Data is complete and trustworthy

Data is reliable, consistent and accurate

Therefore,

Your inability to detect and prevent poor data integrity practices raises serious concerns about the lack of quality system effectiveness. It is imperative that the data generated and used to make manufacturing and quality decisions at your firm is trustworthy and reliable.

Q7 Language to Ensure DI

1. Computerized systems should have sufficient controls to prevent unauthorized access or changes to data.
2. There should be controls to prevent omissions in data (e.g., system turned off and data not captured).
3. There should be a record of any data change made, the previous entry, who made the change, and when the change was made.

Key to Prevent & Detect DI

1. Is the data reliable, trustworthy and verifiable.

2. Was the data generated following GMPs ?

3. Is the data traceable and/or referenced to original raw data and reviewed by a reliable quality structure ?

4. Are the appropriate controls in place to ensure that all data is reported?

Key to Prevent & Detect DI

5. How long in a process can an employee go w/o direct oversight?

6. How do you know all the data is available?

7. DO you have mechanisms to ensure the data is authentic, retrievable?

Key to Prevent & Detect DI

8. Where critical data are being entered manually, there should be an additional check on the accuracy of the entry. This can be done by a second operator or by the system itself.

Key to Prevent & Detect DI

9. An SOP regarding retaining all appropriate documents.

10. Laboratory control records should include complete data derived from all tests conducted to ensure compliance with established specifications and standards, including examinations and assays

Key DI Topics

1. Who-When-What- How:

   Is Data collected ?

   Is Data processed?

   Is Data reviewed?

   Is Data reported?

How do we Know there is a DI Situation?

1.Intent to deceive VS a mistake ?

Ex.

Failure to Protect Computerized Data from authorize changes or access

Is this a DI issue, a GMP issue, or both?

2. DI problem, GMP or Both ?

"Your QC Chemist admitted that, under the direction of a senior colleague, he had recorded false visual examination data in the logbooks for reserve samples…Your firm's failure to prevent, detect, and rectify the falsification of your GMP documentation is concerning."

DI problem, GMP or Both ?

Failure to document the mixing time in your Batch Production Record?

Torn Batch Production Record were found in a trash can, and when examined, batches had been found to failed the blend uniformity test?

DI, GMP or Both?

"Out-of-specification or undesirable results were ignored and not investigated"

Samples were retested without a record of the reason for the retest or an investigation. Only passing results were considered valid, and were used to release batches of APIs intended for US distribution.

DI, GMP or Both ?

Unacceptable practices in the management of electronic data were also noted.

The management of electronic data permitted unauthorized changes, as digital computer folders and files could be easily altered or deleted.

So, if Q7 is Clear, What's Happening?

1. Superficial or ineffective controls
2. NO checks and balance
3. Management lacking expertise or competency to detect the problems
4. Audit trail manipulation-NO true security
5. Accuracy, authenticity and integrity is assumed and not verified
6. Poor security management, no Back UP-Archive

What's Happening ?

7. Are users prevented from deleting electronic records from within the software or outside the software application?

8. Can the use alter the time/date stamp for the system?

9. Does the system have computer-generated audit trails in place to track changes and deletions of critical data?

What's Happening ?

10. Are user rights restricted to ensure users cannot turn on/off the computer-generated audit trails?

11. Is someone from management verifying the electronic records/files for possible deletions or alterations.

DI Examples

1. Electronically stored HPLC (high performance liquid chromatography) data was not a part of the official test records .

2. Missing or No Records Available

3. Performing “trial” sample analysis for HPLC analyses prior to acquiring the official sample result

DI Examples

4. …our investigator noticed that the "trial" related to…rendered an…(OOS) result for the X&Y assay. It appears that…did not pass the trial analysis but met specifications when the official sample was tested shortly thereafter.

5. …our investigator noted some of the "trial injection" data was not kept on HPLC drives because you deleted them.

DI Examples

6. Your firm deleted multiple HPLC data files acquired in 2013 allegedly to clear hard drive space w/o creating back-ups.

7. Your management confirmed there is no audit trail

DI Examples

8. Top site management admitted both, testing and manufacturing operations that occurred outside of the quality system, but assuming no responsibility. Usual Response by firms:

-It was 1 or 2 employees cutting corners

-This has never happened before, isolated event

-Management not aware of these practices

-Quality is not compromised

DI Examples

9. API failing impurity specifications was mixed with other API batches to make an API batch that would pass the test. Management claimed not being aware of such practice

10. Instrumentation and records had been removed from the site expressly to avoid their becoming a part of the inspection.

DI Examples

11. Selection of only passing results from HPLC and GC (gas chromatography) data, while failing test results are disregarded, ignored, and more concerning, not investigated. This practice was noted during the testing of raw materials, finished drug release and stability studies.

DI Examples

12. Undesirable electronic raw data related to GC testing were found in the PC “Recycle Bin”.

13. Partially destroyed hardcopy records of equipment maintenance and instrumentation calibration data were found, as well as 5,000 deleted HPLC data files.

DI Examples

14. Indiscriminate retesting of raw materials, intermediate drug products, and finished API in order to produce acceptable test results.

15. Failures were not reported or investigated to find the cause.

Concluding Remarks

1. We need to know the difference between falsification and poor/bad GMPs.
2. Existing systems should be able to ensure data integrity , traceability and reliability.
3. Companies who outsource operations should have systems in place to verify and compare the data generated by their contractor

Concluding Remarks

4. Once DI Practices are found, known or uncovered, A CHANGE TO AN SOP OR FIRING AN EMPLOYEE IS NOT ENOUGH!!!!

5. QRM approaches to prevent, detect and control potential risk are esential

6. If it looks to good to be true, it probable is not

Our kids assume the drugs they take will make them feel better!!!!

Questions?