ALCOA AND DATA INTEGRITY: PAST AND FUTURE

Marina Figini, PCA S.p.A./Aschimfarma

Data Integrity: reliability, quality and competitiveness factors of API manufacturers

Pavia, 10 Novembre 2017

DATA INTEGRITY: WHAT ABOUT?

Good data management practices influence the integrity of all data generated and recorded by a manufacturer and these practices should ensure that data is accurate, complete and reliable.

Data integrity is the maintenance and the assurance of the accuracy and consistency of data over its entire life-cycle.

Data management and governance should be incorporated into a firms' Quality Management System.

ABOUT DATA GOVERNANCE

Data governance is the sum total of arrangements which provide assurance of data integrity. These arrangements ensure that data, irrespective of the process, format or technology in which it is generated, recorded, processed, retained, retrieved and used will ensure a complete, consistent and accurate record throughout the data lifecycle.

The data lifecycle refers to how data is generated, processed, reported, checked, used for decision-making, stored and finally discarded at the end of the retention period. Data relating to a product or process may cross various boundaries within the lifecycle. This may include data transfer between manual and IT systems, or between different organisational boundaries; both internal (e.g. between production, QC and QA) and external (e.g. between service providers or contract givers and acceptors).

The data governance system should ensure controls over data lifecycle which are commensurate with the principles of quality risk management.

WHY DATA INTEGRITY COMPLIANCE IS IMPORTANT?

- **Lack of integrity undetermines the assurance and confidence in safety, efficacy and quality of drugs**
- **Data integrity problems break trust**
- **Data integrity problems can highly affect the business**

RESPONSABILITY

Data integrity is an area where every employee of the company has a role to play in documentation of laboratory results, completion of batch records and other record required by GxP rules.

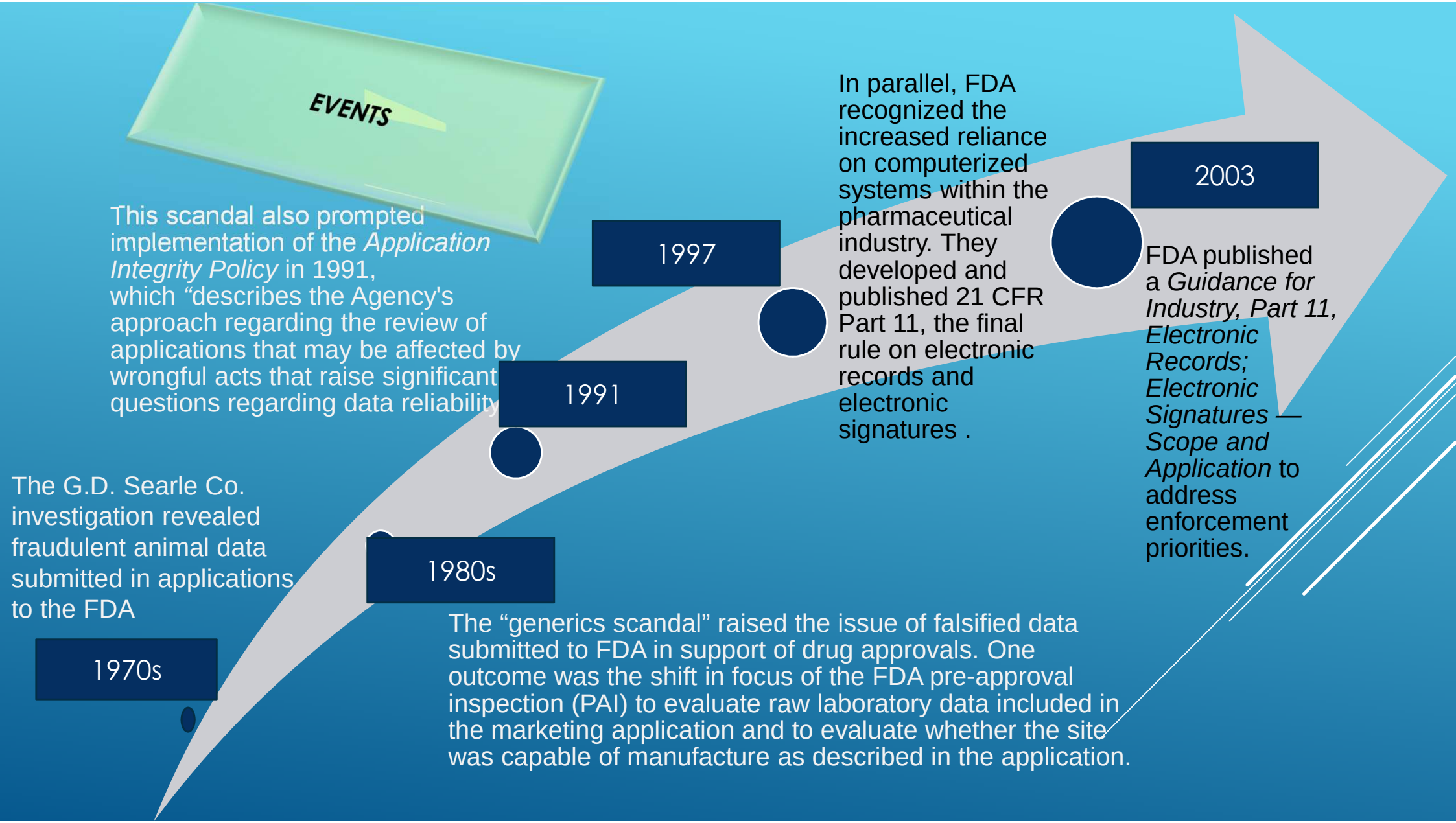
If the integrity of data is questioned, then the whole regulatory process is questioned. If the data are proved false and misleading, then the regulatory decisions may be wrong.

What it did give origin to the focus on data integrity by the Regulatory Authorities?

The attention to data integrity represents an evolution since 30+years coming from the technology enhancing and learning from GMP inspections.

Lapses in data integrity are not limited to fraud or falsification, they can be unintentional and still pose risk. Any potential for compromising the reliability of data is a risk that should be identified and understood in order for appropriate controls to be put in place.

A JUMP INTO THE HISTORY


EVENTS
1970s
The G.D. Searle Co. investigation revealed fraudulent animal data submitted in applications to the FDA
1980s
The "generics scandal" raised the issue of falsified data submitted to FDA in support of drug approvals. One outcome was the shift in focus of the FDA pre-approval inspection (PAI) to evaluate raw laboratory data included in the marketing application and to evaluate whether the site was capable of manufacture as described in the application.
1991
This scandal also prompted implementation of the *Application Integrity Policy* in 1991, which "describes the Agency's approach regarding the review of applications that may be affected by wrongful acts that raise significant questions regarding data reliability
1997
In parallel, FDA recognized the increased reliance on computerized systems within the pharmaceutical industry. They developed and published 21 CFR Part 11, the final rule on electronic records and electronic signatures .
2003
FDA published a *Guidance for Industry, Part 11, Electronic Records; Electronic Signatures — Scope and Application* to address enforcement priorities.

RECENT EVENTS

In the 2000s there has been a resurgence of data integrity issues found by regulatory authorities all over the world leading to increased information sharing amongst regulatory authorities.

The MHRA announced in December 2013 their expectation that pharmaceutical firms assess data integrity as part of their self-inspection program including outsourced activities. This will be covered during MHRA inspections.

The FDA and EMA announced in December 2013 the Generic Drug Initiatives to facilitate regulatory actions against non-compliant companies through the sharing of inspection information and bioequivalence data. Earlier in the year a large generic drug manufacturers plead guilty to charges of falsifying bioequivalence data in support of several generic drug applications.

On August 21, 2015 the European Commission announced an EU wide ban on sales of around 700 generic drugs due to data integrity. Bioequivalence studies conducted by GVK Biosciences, Hyderabad, India were found to have systematic data manipulation that took place over several years leading to doubt in the integrity of the trials and the data.

The China Food and Drug Administration (CDFA) gave drug manufacturers until August 25, 2015 to conduct self-audits for the purpose of authenticating clinical trial data submitted in applications.

FDA'S ACTIONS

2000, a warning letter issued to Schein Pharmaceuticals cit ed lack of control over computerized laboratory systems including lack of password control and broad ranging staff authority to change data

2005, FDA issued a 15-page form 483 to Able Laboratories in New Jersey . Failing laboratory results were identified that were not reported, and among the observations was failure to review electronic data, including audit trails.

2007, Warning letters citing deficiencies in the broad area of data integrity were issued to *Actavis Totowa LLC* site in the U.S.

2008, Ranbaxy received two warning letters regarding its Paonta Sahib site and one related to its Dewas facility (2008), both located in India.

2010 FDA'S ANNOUNCEMENT

- Based on these compliance actions, FDA announced a pilot program in 2010 to evaluate data integrity as part of routine GMP inspections.
- FDA planned to use the information gained from these inspections to determine whether revisions to Part 11 or additional guidance on the topic were necessary.
- FDA also committed to take appropriate enforcement actions on issues identified during the inspections. The program is described in a slide presented by FDA's Robert Tollefsen at a variety of industry conferences in 2010. In the slide FDA stresses that it will "continue to enforce all predicate rule requirements, including requirements for records and recordkeeping."

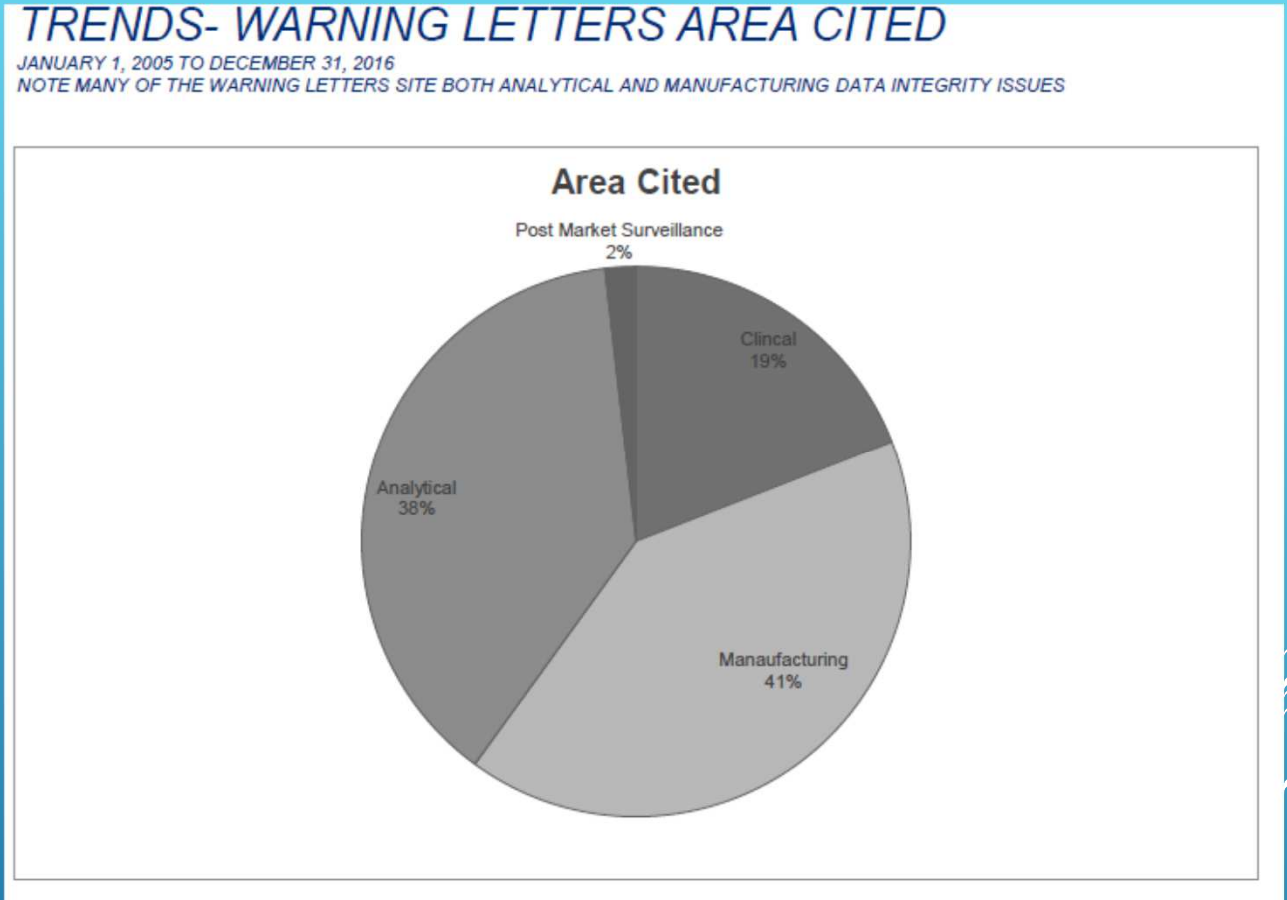
	FY2013	FY2014	FY2015
Total WLs issued	**38**	**22**	**19**
WLs citing data integrity	**10** (26%)	**12** (55%)	**14** (74%)
U.S. site WLs citing data integrity	**0 of 13** (0%)	**0 of 4** (0%)	**1 of 3** (33%)
OUS site WLs citing data integrity	**10 of 25** (40%)	**12 of 18** (67%)	**13 of 16** (81%)

DATA INTEGRITY DEFICIENCIES IN FDA WARNING LETTERS (WLS), FY2013-2015

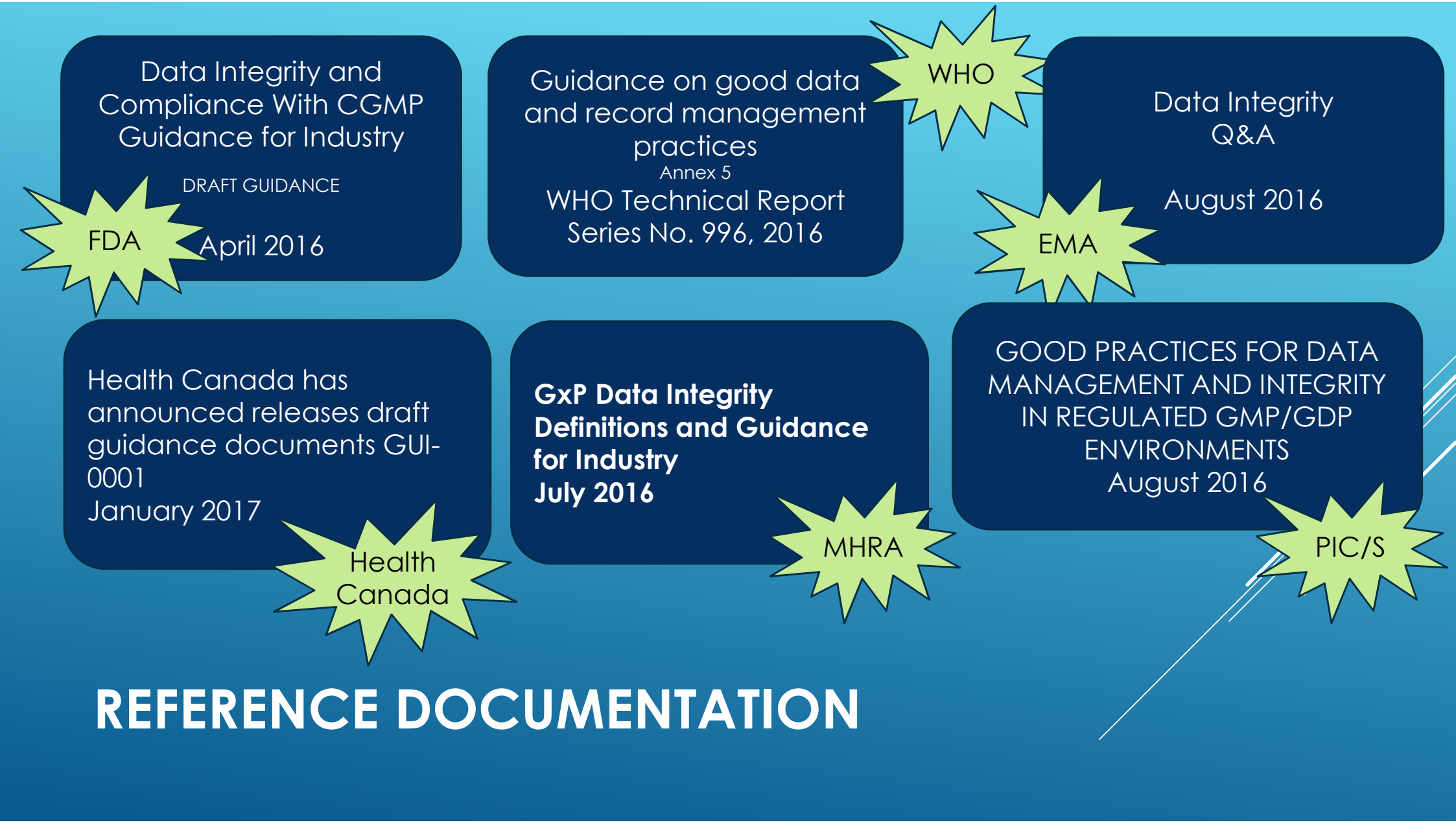
DATA INTEGRITY: SURVEYING THE CURRENT REGULATORY LANDSCAPE

BY BARBARA UNGER, UNGER CONSULTING INC.

James Stumpff, RPh, Principal Consultant, Parexel, August 2017



WARNING LETTERS'TREND



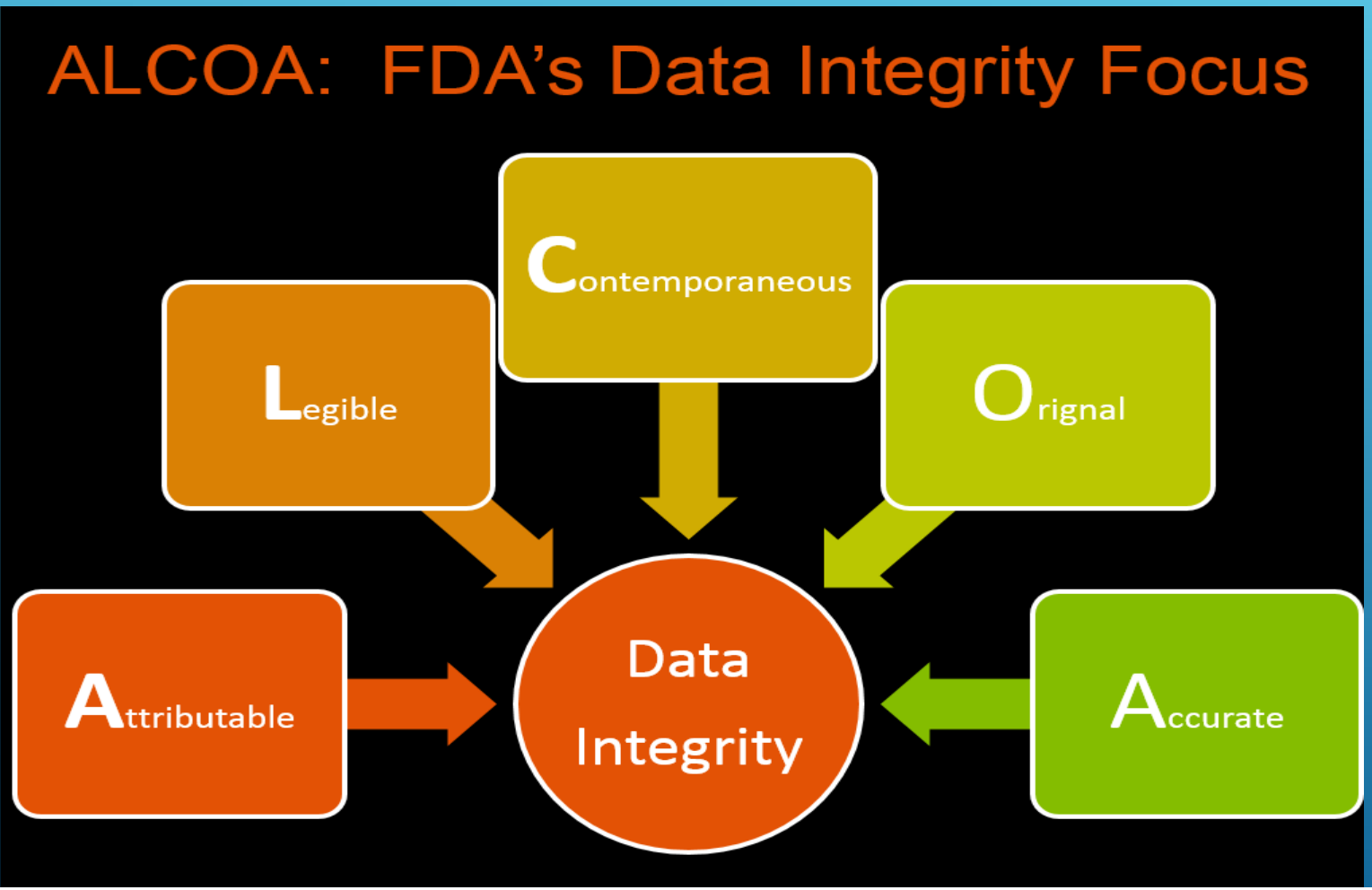
REFERENCE DOCUMENTATION

Historically, data was paper based and thus subject to the integrity of the individuals responsible for recording and checking the data entries. The computer age has introduced electronic data which when properly managed increases the ability to assure the integrity of data.

Data may be generated from a variety of sources including toxicology studies, clinical studies, manufacturing operations and laboratory testing. The data may support regulatory submissions and/or required documentation for current Good Manufacturing Practice (cGMP) activities.

HOW DATA MANAGEMENT IS CHANGED

TRUSTWORTHY RECORD CHARACTERISTICS



The acronym ALCOA has been around since the 1990's, is used by regulated industries as a framework for ensuring data integrity, and is key to Good Documentation Practice (GDP). ALCOA relates to data, whether paper or electronic, and is defined by US FDA guidance as Attributable, Legible, Contemporaneous, Original and Accurate.

These simple principles should be part of your data life cycle, GDP and data integrity initiatives.

All data generated or collected must be attributable to the person generating the data. This should include who performed an action and when. This can be recorded manually by initialing and dating a paper record or by audit trail in an electronic system.

- ✓ During a validation exercise, test results should be initialed and dated by the person executing the test.
- ✓ Adjustment of a setpoint on a process or monitoring system should be made by an authorised user and the details of the change logged in an audit trail.
- ✓ A correction on a lab record should be initialed and dated to show when and who made the adjustment.

ATTRIBUTABLE

Who acquired the data or performed an action and when?

All data recorded must be legible (readable) and permanent. Ensuring records are readable and permanent assists with its accessibility throughout the data lifecycle. This includes the storage of human-readable metadata that may be recorded to support an electronic record.

- ✓ Promote the use of indelible ink when completing records.
- ✓ When making corrections to a record, ensure a single line is used to strike out the old record. This ensures the record is still legible.
- ✓ Controlling your paper records/forms and formatting them such that there is ample room for the information to be recorded.

LEGIBLE

Can you read the data?

Contemporaneous means to record the result, measurement or data at the time the work is performed. Date and time stamps should flow in order of execution for the data to be credible. Data should never be back dated.

- ✓ If executing a validation protocol, tests should be performed and their results recorded as they happen on the approved protocol.
- ✓ Data that is logged, or testing that is performed electronically, should have a date/time stamp attached to the record.
- ✓ Ensure electronic systems that log data have their system clocks synchronised.
- ✓ Consider the use of a master clock system that synchronises to the IT network so wall clocks within labs and processing areas are syncronised.

CONTEMPORAEOUS

Documented at the time of the activity

Original data, first capture of data (not transcribed data), recorded for the first time. This could be a database, an approved protocol or form, or a dedicated notebook. It is important to understand where your original data will be generated so that its content and meaning are preserved.

- ✓ Ensure validation test results are recorded on the approved protocol. Recording results in a notebook for transcription later can introduce errors.
- ✓ If your original data is hand written and needs to be stored electronically, ensure a "true copy" is generated, the copy is verified for completeness and then migrated into the electronic system.

ORIGINAL OR A TRUE COPY

Written printout or observation or a certified copy thereof

For data and records to be accurate, they should be free from errors, complete, truthful and reflective of the observation. Editing should not be performed without documenting and annotating the amendments.

- ✓ Use a witness check for critical record collection to confirm accuracy of data.
- ✓ Consider how to capture data electronically and verify its accuracy. Build accuracy checks into the design of the electronic system.
- ✓ Place controls/verification on manual data entry, for example, temperature results can only be entered within a predefined range of 0-100°C.

ACCURATE

No errors or editing without documented amendments

OTHER PILLARS

ACCURATE

- No errors or editing without documented amendments

AVAILABLE

- For review and audit or inspection over the lifetime of the record

COMPLETE

- All data is present and available

OTHER PILLARS

CONSISTENT

- All elements of the record, such as the sequence of events, follow on and are dated or time stamped in expected sequence

ENDURING

- On proven storage media (paper or electronic)

TRUSTWORTHY

- The data and the record have not been tampered with

Static: fixed data document (e.g., paper record or an electronic image)

Dynamic: record format allows interaction between the user and the record content (e.g., a chromatogram where the integration parameters can be modified)

USE OF "STATIC" AND "DYNAMIC" IN RELATION TO RECORD FORMAT

moving to the other presentations,
thank you for your attention