Archiving and Vendor Assessments in the World of eData and eRecords:

Where do I Start?

Laurel Branstrator
LEB Quality Consulting

Purdue University – Biotechnology Innovation & Regulatory Science Center (BIRS)

Risk of Poor Data

Basic research establishes critical criteria for data collection.

As the purpose of data collection become more relevant to an individual, the data itself become more heavily scrutinized

- Academic (Pure Research)
  - Grant Funding Institutions (NIH, DOD)
- Approval to Market a New Drug (FDA)
  - Affects Public Safety /Health
- New Product Registration (EPA)
  - Affects Public Safety/Health
- Diagnostic Evaluation (CLIA, CAP)
  - Affects an Individual's Health
- Forensics (Dept of Justice, ABFT)
  - Affects an Individual's Legal Rights

Perhaps the Most Critical Concepts for Research Data

In the United States, we pride ourselves on several concepts:

- An individual is considered **innocent** until proven **guilty**
- Patient (consumer) **safety**, **protection**, and **privacy** are paramount

As such, data that are collected for clinical research, diagnostics, product approval and forensics are considered **guilty** until proven **innocent**

Data must be ***proactively*** collected with the intention of ***retrospectively*** proving that the data are:

Accurate

Complete

Relevant

Unbiased

Data Quality vs Data Integrity

A number of attributes are considered of universal importance to source data and the records that hold those data. These include that the data and records are:

Quality

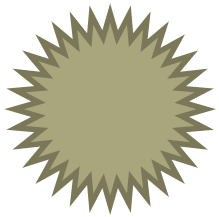
- Accurate
- Legible
- Contemporaneous
- Original
- Attributable

Integrity

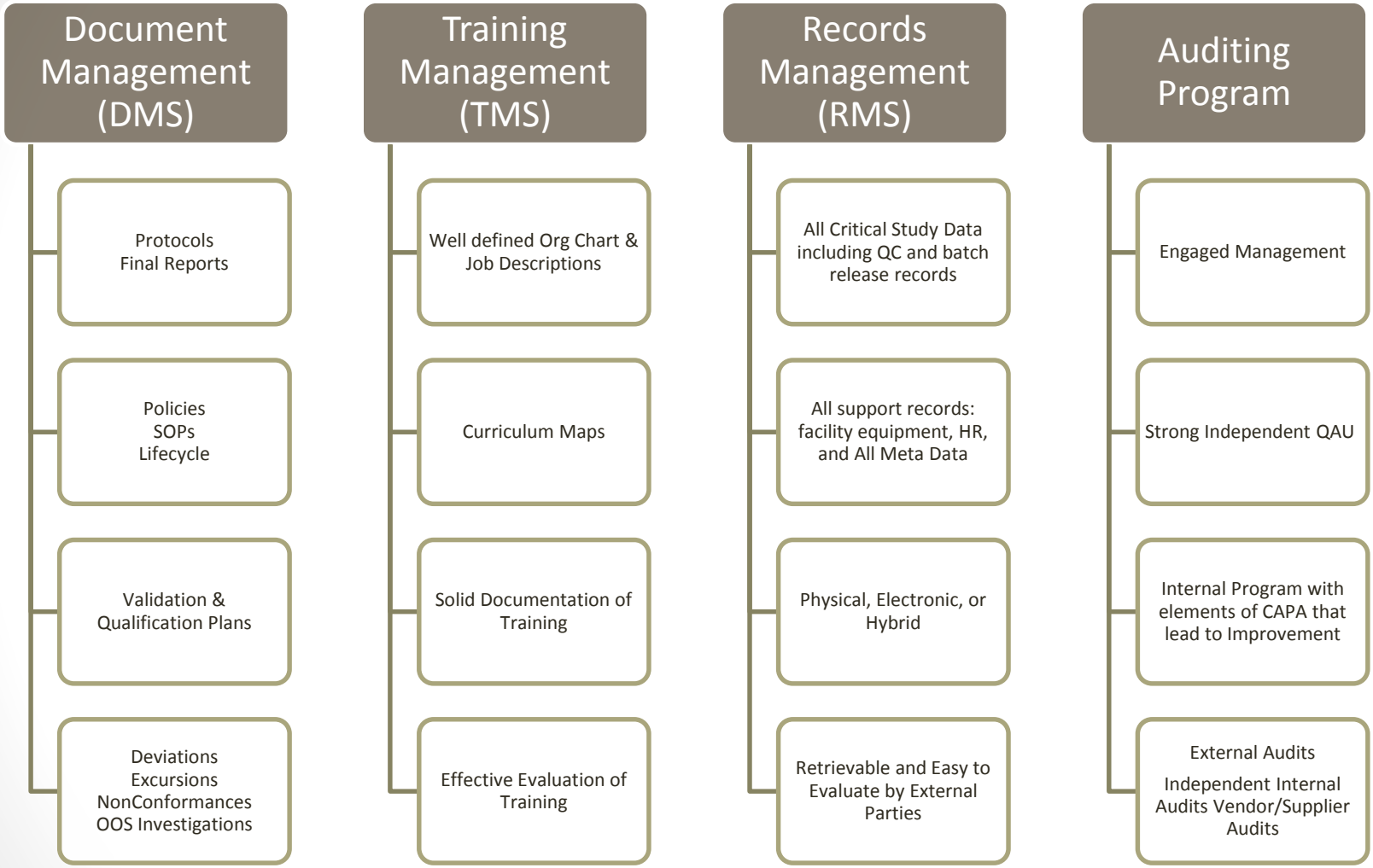
- Complete
- Consistent
- Enduring
- Available
- Accurate through the Data Lifecycle

What is a Quality Management System?

A management system of procedural and technical controls that promote your organization's ability to transparently operate in a state of control.



A solid QMS acquires HIGH QUALITY data and maintains that data with a HIGH DEGREE of INTEGRITY


Document Management (DMS)
Protocols
Final Reports
Policies
SOPs
Lifecycle
Validation & Qualification Plans
Deviations
Excursions
NonConformances
OOS Investigations
Training Management (TMS)
Well defined Org Chart & Job Descriptions
Curriculum Maps
Solid Documentation of Training
Effective Evaluation of Training
Records Management (RMS)
All Critical Study Data including QC and batch release records
All support records: facility equipment, HR, and All Meta Data
Physical, Electronic, or Hybrid
Retrievable and Easy to Evaluate by External Parties
Auditing Program
Engaged Management
Strong Independent QAU
Internal Program with elements of CAPA that lead to Improvement
External Audits
Independent Internal Audits Vendor/Supplier Audits

A QMS that Supports a GxP Ideology is Built Upon:

- Sound Scientific Methodology with robust QC processes
- Policies and procedures that define systems and governing structure
- Robust Protocol/Plan Design and Adherence
- Strong Management Engagement , Authority and Accountability
- Independent Quality Assurance
- Single Point of Scientific or Technical Control
  (e.g. PI/PM/Application Admin)
- Controlled, Organized and Maintained Facilities
- Well Qualified and Maintained Equipment
- Training, Training, Training (and documentation!!)

Additionally, QMS Concepts Promote:

- Total Project/Study/Batch Reconstructability
- Ability to support 'Data Integrity Inspection'
- Efficient Archives
- Appropriate Compliance Statements
- Continued Improvement – be vigilant for the few FDA, EPA, Global, and Industry Guidelines and make your systems relevant
- Orderly Change Control for all Critical Systems.
- External scrutiny by clients and outside regulators

Remember – the goal is to ensure the safety, efficacy, and quality of drugs, devices, and chemical products. Our data is 'guilty until proven innocent'.

A good QMS rests upon 4 'pillars'…..

Records
All Kinds of Records

In keeping with the concept that the **data** are

'*guilty until proven innocent*'

We are responsible to build 'Quality Systems' that support the data. This means formal records, records, records.

'If isn't documented, it didn't happen'.

Formal Standard Operating Procedures

There must be ***a priori*** SOPs to establish a standard approach to routine tasks so as to ensure unbiased quality and integrity of the samples collected and data reported.

- Sample Collection
- Sample Handling
- Sample Storage
- Chain of Custody
- Analytical Methodology
- Sample Destruction?

There must be SOPs to describe the complete archiving process.

Special Considerations for Electronic Data

- Computerized systems must be validated
- Electronic signature use must limited to the owner.
- Must be protected by use of biometrics or unique two part individual ID and secret password
- Proper understanding, use, maintenance of '**metadata**':
  - Data that describe the attributes of other data, and provide context and meaning…. Metadata forms and integral part of the original record. Without metadata, the data has no meaning.
- Audit trails that show the same information changes on paper would (similar to 'single-line-cross-out': original value, new entry, authors, time/dates, reason for change)
- Time and Date Stamps
- Archiving Electronic Records (including the meta data!)

And More….
Special Considerations for Electronic Data

- Written policies must be in place that convey to all staff that their electronic signatures are the legally binding equivalent of their handwritten signatures.
- The system must only be accessed by authorized and qualified personnel – system administrator roles must be defined
- The scope of the ‘system’ must be defined: is it ‘closed’ or ‘open’?
- Must be able to mimic securities of a paper environment.
- Error correction must also mimic paper environment.
- Are records considered ‘static’ (fixed like a photograph) or ‘dynamic’ (format allows interaction between user and record content)

Archiving

References – Check Them Out

- *Faking It – The Case Against Industrial Bio-Test Laboratories,* by Keith Schneider, originally from *The Amicus Journal*, spring 1983 edition, published by the **Natural Resources Defense Council** (NRDC).

- *FDA Good Laboratory Practices* – 21 CFR Part 58
- *EPA Good Laboratory Practices* – 40 CFR Part 160
- *OECD Good Laboratory Practices* – ENV/MC/CHEM(98)17

- OECD Consensus Document 15 – *Archives*
- OECD Consensus Document 17 – *Application of Computerized Systems to GLP*

Basic Archiving 101 - SOPs

- All raw data, documentation, records, protocols, specimens, final reports, pivotal correspondence and supporting QMS documents must be retained (training, equipment, facilities)
- Must have a dedicated archive (secure, environmentally protected)
- Must have an archivist
- Must be indexed – readily retrievable
- Must have appropriate Record Retention Policy
- SD, PI, TFM, QAU coordinate transfer of data
- Data must ‘endure’
- Gets complicated in multi-site environment

E-Archiving
The Same Rules Apply!

Where are the data?

Perform routine internal Data Integrity Inspections

- How are the data transferred from the SD to the Archivist?
- What is the role of IT? Is IT = Archivist?
- What does it mean to 'lock down the data' - is this enough?
- How are the data 'indexed' for retrieve-ability?
- What about data migration over time? Software upgrades?

You must learn and understand how data are archived within individual software systems. LIMS, ELN, data acquisition – all different and YOU have the responsibility to understand them and operate in a state of control through the data lifecycle.

Archiving the Data

This means different things to different professions. Archiving and data retention requirements vary and are specific to the needs of the data and the purpose of the investigation

- How long should the data be retained?
- How do you maintain security?
- How do you allow access but disallow changes, modifications or deletions?
- How do you maintain data integrity (without degradation) over time?
- Who pays for this?

Raw Data and IT

IT is the guardian of all our electronic raw data. IT controls:

- Ability to accurately collect the data
- Ability to back up and restore the data
- Ability to move the data
- Ability to retrieve the data
- Ability to do all of these things with security and attributability.

IT must be engaged and vested in the regulatory nature of our business. “Better, Faster, New” must be managed and controlled correctly.

How does this change in a ‘cloud-based’ environment?

IT vs Regulated IT

IT has its own raw data that it generates

- Server logs (back-up/restore)
- Controlled access logs to secure server rooms
- Network diagrams
- Can these records be presented to clients and regulators? Would IT staff be willing/able to present their records?

IT personnel are accountable for their part in study conduct

- IT staff should have appropriate Training!!!
- IT must work in concert with Management and QA to support Laboratory (or clinic or manufacturing)

Data Integrity Inspections

Where do we start?

Data Flow Questions Electronic or Paper

Where are the original records acquired?

How are data transferred (manually or digital interface)?

At each point, who has access to the data?

Who can alter or delete records at each point?

How are data held during processing?

How are data held if re-processed or re-integrated?

Are there any data silos?

How are data backed-up? Is there appropriate virus protection?

Are there any differences to the security of the data at each point of the lifecycle?

How are the data ultimately archived?

Are the metadata archived as well?

Audit Trails

A secure, computer-generated time-stamped electronic record that chronicles the events relating to the *creation*, *modification* , or *deletion* of an electronic record.

- Critical to assure that Audit Trails are configured correctly audit logs to track changes with appropriate justification
- Review audit trails often at the record level (batch or study)
- Also review the system level for attempts to access files or to rename or delete records.

- Remember IT and the System Administrators are Your Best Resources!

Vendor Assessments in an Electronic Environment

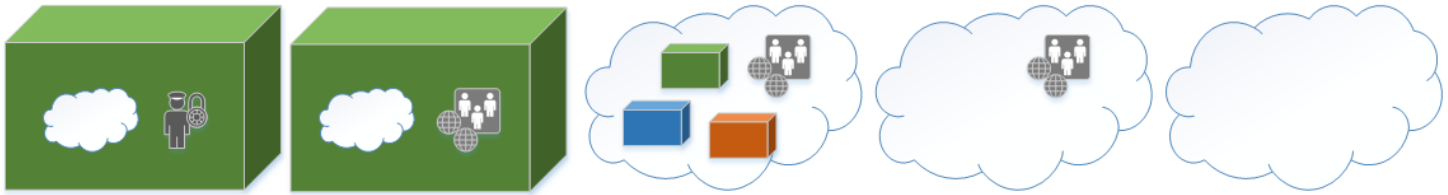
Data Center Deployment Models

← **Control – Private**

IT support and capabilities are provided as an internal function via an INTRANET within the enterprise and behind a firewall.

→ **Control – Public**

IT support and capabilities are provided by an external vendor as a service to the enterprise via the INTERNET .



Data Center Held and Internally Managed Within the Enterprise	Data Center Held at Enterprise but Managed by Vendor	Data Center Externally Hosted as Private Cloud	Data Center or Software Solution Externally Hosted within Community Cloud	Public Cloud Services for Help Desk, Software Applications, Data Warehouse, etc.

Financial Obligation

Overall Risk

Types of Vendors to be Assessed

- Hardware and Software Vendors
- Network Support Vendors
- Helpdesk Vendors
- Hosted Solution Providers (the ‘Cloud’)
- Off-site archives

Vendor Assessment Plan

Prep for Vendor Assessment – Be very clear about your INTENDED USE

- Ask for as much specific information as possible prior to your arrival . Use your in-house SMEs to develop questionnaire.
- Be prepared: these companies are not like us
- Do your homework and be sure to understand their responses
- Ask for certifications – then understand what those certifications are!
- Are there multiple data centers? Where is your data going to reside. Do not assume that every data center is the same
- Take a IT Representative with you if possible

On-Site Tour of a Hosted Solution Provider – My Experience

- Be prepared to be shooed out the door
- Be prepared to be in awe of their facility and their hardware
- Be sure to ask lots of questions along the way
- Be prepared to not get every answer
  - SOPS
  - Facility Walk Through
  - Who owns the actual building? How long is their lease?
  - Security– who owns it who controls it
  - Environmental (HVAC) – who owns/controls
  - Power Resiliency
  - Fire protection and supression
  - Telecommunications
  - Back-up/Restore
  - DR/BCP
  - Training
  - Qualification/Validation of systems – do they have it? Maybe not but may have something. Do they have an alternate strategy that may mitigate the gap of what you are expecting.

On Site QMS Review of a Hosted Solution Vendor

What I was looking for:

- Basic QMS structure (DMS, TMS, RMS, Archive, Change management) with formal evidence of execution

What I was presented with instead – 'Attestation Certificates'

- from and independent CPA firm confirming that the SITE:
- had been evaluated by standards set by the National Institute of Standards and Technology (NIST) and also to controls related to the Health Insurance Portability and Accountability Act Security Rule of 2003 (HIPAA) and the Health Information Technology of Economic and clinical Health Act (HITECH). Additional standards utilized (e.g. Payment Card Industry Data Security Standard);
- was capable to execute effective administrative safeguards, physical safeguards, technical safeguards, and breach notification procedures that support regulated data environments;
- maintained, in all material respects, effective controls over the security and availability of the data center services system to provide reasonable assurance that:
- the system was protected against unauthorized access, use, or modification;
- the system was available for operation and use as committed or agreed.

The Disconnects – Culture & Vocabulary

- Reminded me of the 90's in our industry and software validation/Part 11 world fell upon us.
- These vendors are NOT tailored to our industry
- My questions dismissed as unimportant
- Very arrogant –with good reason – but still arrogant much like a university environment
- Multi-tenant environment? Hypervisor?
- Configured/controlled by CRO NOT host (good/bad)
- CRO responsible to verify that daily data transfers were robust so why did they have to be involved? Not a bad question
- They are good/smart with a good reputation. What else did I need?
- They chronically refused to completely answer questions – or provided very high-level response – claiming confidentiality issues. Especially around the BCP.

So What Do We Do?

This service is important and will be more important in the future unless each company is able to maintain their systems as 'closed'. Very expensive. I don't have a good answer yet.

- My final take was to 'recommend with restrictions'
  - Required notification to my client if there are personnel changes at the highest level of THIS site
  - Do not transfer my client's data to another site without notice
  - Be aware that hardware changes will not be announced and will be fairly invisible to CRO
  - Did NOT recommend for anything EXCEPT catastrophic recovery
  - All data back-ups ONE WAY. Do NOT use for routine file recovery
  - Move to more controlled environment asap (either in-house or a hosted solution provider that understands Pharma

Questions?

Thank you for your attention!

Laurel Branstrator

LEB Quality Consulting

lebranstrator@yahoo.com