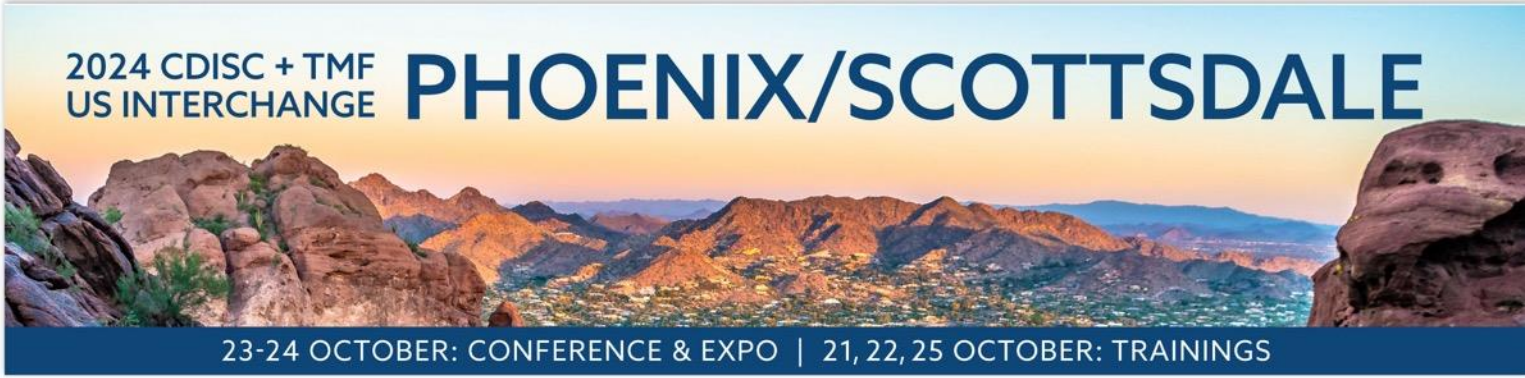


GCP Record Retention: Guidance and advice on what you need to know

Presented by Ashley Avery, Senior Specialist, Quality Documents and Archival, Cerevel Therapeutics and Tom Lynam, Marketing Director, Arkivum

Meet the Speakers

Ashley Avery

Title: Senior Specialist, Quality Documents and Archival

Organization: Cerevel Therapeutics

Tom Lynam

Title: Marketing Director

Organization: Arkivum

Disclaimer and Disclosures

- *The views and opinions expressed in this presentation are those of the author(s) and do not necessarily reflect the official policy or position of CDISC.*

- *Cerevel Therapeutics (recently acquired by AbbVie) is a customer of Arkivum*

Additional Disclaimers

- We are in wrong track (sort of)!
- We are not regulatory experts
- Strongly recommend seeking guidance on your specific requirements
- Focus of this session is:
  - Highlight requirements to consider
  - How to manage your records and data in line with good practice and regulatory guidelines

cdisc

Agenda Points

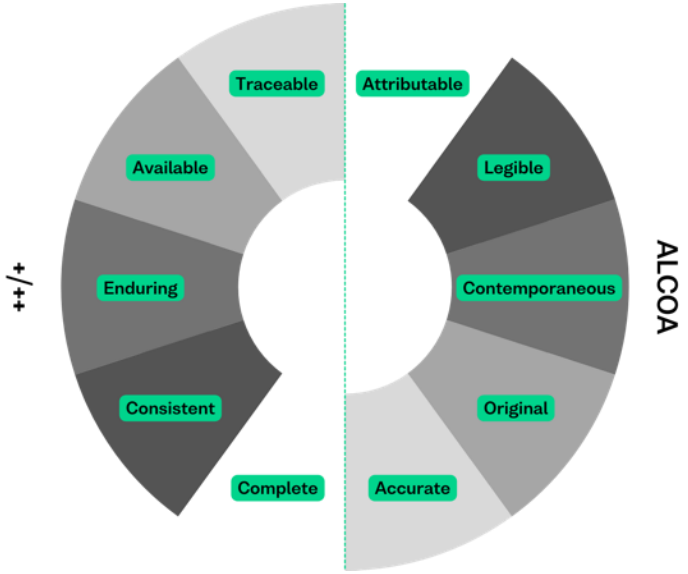
1. An overview of key retention guidelines.
2. Good practice approaches to digital archiving, including alignment to ALCOA+.
3. How to write a retention policy through providing examples of real-life policies.
4. How to manage legal holds.
5. What to do with physical records, including digitizing records and creating certified copies.
6. How to approach document and record destruction

TMF Retention Requirements

Region	Regulator/ Authority	Relevant Regulation(s)/ Guideline(s)	Last Updated	What is the retention period?
USA	FDA	CFR 21 Part 312.57	2002 (1987)	"A sponsor shall retain the records and reports required by this part for 2 years after a marketing application is approved for the drug"
Canada	Health Canada	SOR/2003-196	2022	"The sponsor shall maintain all records referred to in this Part for a period of 15 years."
EU	EMA	EU CTR (officially EU Reg 536/2014)	2014	Sponsor & investigator retain the TMF for +25 years – readily available for inspection and legible
UK	MHRA	Medicines for Human Use (Clinical Trials) Regulations 2004	2004	Currently 5 years, but new regulation proposed. Proposed change: "…a proportionate Trial Master File, that must be directly accessible to MHRA inspectors, that it is retained for a minimum of 25 years, but that more detailed aspects, such as proportionality in the retention period, are covered in guidance."
Global	ICH	ICH E6 R3	2024	Refer to local/regional regulators' retention requirements

What can we learn from these requirements?

- Varied retention periods:
  1. Follow local retention rules
     - Where the trial was run & where the drug will be sold
  2. Use the longest relevant retention period as the '**highest lowest common denominator**'
- General themes:
  - More recently updated regulations tend to have longer retention periods
  - Inspection readiness crucial
  - Direct and indirect reference to ALCOA+ throughout



Good practice approaches to digital archiving

Including alignment to the ALCOA+ principles

A risk-based approach to GxP retention

Likelihood of Data Integrity Failure

- Data is corrupted or lost
- Backup failures
- Accidental or deliberate alteration of records
- End of Life systems, data cannot be migration
- Proprietary formats, vendor lock in
- Suppliers go bust, no BCDR plan
- Cyber attacks and ransomware
- Formats not supported, data can't be accessed
- Audit trails expire or are deleted
- Data migrations are not validated
- Data is distributed and can't be found
- Systems are not validated for archiving
- EoL systems not secure, no recommissioning
- No checksum evidence that data hasn't changed
- No one understands old data formats
- No understands obsolete applications

Consequences/Impact of Data Integrity Failures

- Health and safety of study participants and patients
- Failed inspections & CAPAs
- Rejection or delay to marketing application
- Removal of drug from the market
- Financial Penalties
- Quality issues with products
- Cost of doing repeat work
- Cost of doing additional work
- Reputation damage
- Delayed sales or MNA
- Ethical issues

Probability	Harm Severity			
	Minor	Marginal	Critical	Catastrophic
Certain	High	High	Very High	Very High
Likely	Medium	High	High	Very High
Possible	Low	Medium	High	Very High
Unlikely	Low	Medium	Medium	High
Rare	Low	Low	Medium	Medium
Eliminated	Eliminated			

Application of long-term digital preservation (LTDP)

Retention period: up to 5 years

- **Risks:**
  - Lower risk to data degradation or obsolescence
- **Considerations:**
  - How and where to store the data – how accessible is it?
  - Recommended migration out of source system
  - Physical storage media is unreliable, requires hardware interface and not validated
  - ALCOA+ still applies!

Average Lifespan of Physical Media*

Media	Average Lifespan (ideal conditions)	Annual Failure Rate (AFR) (from new)
USB Stick	~10 years	1-2%
CD-R/ CD-RW	5-100 years	Significant differences by brand and type
Hard drive - HDD	3-5 years	2-8%
Hard drive - SSD	Less than 10 years	0.5-1.6%

*15 minutes research on Google from various sources – manufacturers, researchers & membership organisations. Huge differences depending on make and type of hardware used.

Retention period: Up to 15 years

- **Risks:**
  - High risk of hardware failure
  - Increasing risk of software/data endurance issues (e.g. corruption)
  - Maintaining access to data
  - Vendor lock-in/end of life systems
- **Considerations:**
  - Digital safeguarding practices
  - Access processes & planning
  - ALCOA+ still applies…

Retention period: At least 15+ years

- **Risks:**
  - Higher risk of endurance & access issues
  - Increased risk of software/file format obsolescence – ensuring legibility
- **Considerations:**
  - Active long-term digital preservation (LTDP)
  - And of course…ALCOA+ still applies!

Don't start planning 15 years into the retention period!

Table of Recommended File Formats for Long-Term Data Curation

Content Type	High probability for long-term preservation	Medium probability for long-term preservation	Low probability for long-term preservation
Text	• Plain text (encoding: USASCII, UTF-8, UTF-16 with BOM) • XML (includes XSD/XSL/XHTML, etc.; with included or accessible schema) • PDF/A-1 (ISO 19005-1) (*.pdf)	• Cascading Style Sheets (*.css) • DTD (*.dtd) • Plain text (ISO 8859-1 encoding) • PDF (*.pdf) (embedded fonts) • Rich Text Format 1.x (*.rtf) • HTML (include a DOCTYPE declaration) • SGML (*.sgml) • Open Office (*.sxw/*.odt) • OOXML (ISO/IEC DIS 29500) (*.docx)	• PDF (*.pdf) (encrypted) • Microsoft Word (*.doc) • WordPerfect (*.wpd) • DVI (*.dvi) • All other text formats not listed here
Raster Image	• TIFF (uncompressed) • JPEG2000 (lossless) (*.jp2) • PNG (*.png)	• BMP (*.bmp) • JPEG/JFIF (*.jpg) • JPEG2000 (lossy) (*.jp2) • TIFF (compressed) • GIF (*.gif) • Digital Negative DNG (*.dng)	• MrSID (*.sid) • TIFF (in Planar format) • FlashPix (*.fpx) • PhotoShop (*.psd) • RAW • JPEG 2000 Part 2 (*.jpf, *.jpx) • All other raster image formats not listed here
Vector Graphics	• SVG (no Java script binding) (*.svg)	• Computer Graphic Metafile (CGM, WebCGM) (*.cgm)	• Encapsulated Postscript (EPS) • Macromedia Flash (*.swf) • All other vector image formats not listed here
Audio	• AIFF (PCM) (*.aif, *.aiff) • WAV (PCM) (*.wav)	• SUN Audio (uncompressed) (*.au) • Standard MIDI (*.mid, *.midi) • Ogg Vorbis (*.ogg) • Free Lossless Audio Codec (*.flac) • Advance Audio Coding (*.mp4, *.m4a, *.aac) • MP3 (MPEG-1/2, Layer 3) (*.mp3)	• AIFC (compressed) (*.aifc) • NeXT SND (*.snd) • RealNetworks 'Real Audio' (*.ra, *.rm, *.ram) • Windows Media Audio (*.wma) • Protected AAC (*.m4p) • WAV (compressed) (*.wav) • All other audio formats not listed here

Digital preservation bit list

Rationale of why ‘Commercial Software’ is considered **‘Critical Endangered’:**

“This is a new Bit List entry…to draw attention to the particular challenges of content and software preservation for commercial software products.

The entry focuses on the distinct risks relating to the availability and access to software and code, and lack of preservation interest or mandate, by companies that publish them, creating challenges to preserve digital content and software in source code form.”

CRITICALLY ENDANGERED

PRACTICALLY EXTINCT

ENDANGERED

VULNERABLE

Creating a retention policy

Table

Record Type	Retention Period	Disposition Method
Financial Records	10 years	Secure Shredding
Employee Records	Employment + 5 years	Secure Shredding

Records Retention Schedule

The Records Retention Schedule is a documented guidebook that defines how long organizations retain records, both physical and electronic, before they are either destroyed or transferred to an archive. The purpose of a Records Retention Schedule is to ensure that records are kept for as long as they are needed for business, legal, or regulatory purposes, to facilitate their timely and appropriate disposal when they are no longer required.

Benefits of a Records Retention Schedule

- Compliance with Legal and Regulatory Requirements
- Efficient Use of Storage Space
- Cost Savings
- Improved Information Management
- Mitigation of Legal Risks
- Preservation of Corporate Memory and History
- Facilitation of Audits and Inspections
- Enhanced Data Security and Privacy
- Regulators and Stakeholder Confidence

Lifecycle of Records and it's Records Retention Schedule

- Review governing body compliance and regulations:
  - FDA
  - EMA
  - 21 CFR Part 11
  - GMP
- Identify record types
  - SOPs
  - Reports, logs
  - Protocol records
  - Patient data
- Describe archival process
- Describe access and security
- Describe disposition of records
- Periodic Reviews
- Identify when you should begin schedule creation

cdisc

Records Retention Schedule Example

Managing Information Systems	Managing Information Systems – Records related to the development, qualification/validation, implementation and management of computerized systems for managing company information.				
Managing Resources	Managing Information Systems	Information Technology Infrastructure Management	Records related to the acquisition, installation, testing, operation, validation, and decommission of hardware and its intrinsically linked software.	Change control, Configurations, Decommissioning, Inventory management and asset registers, Planning and reporting, Specifications, Testing	Decommissioned + 5 years
Managing Resources	Managing Information Systems	Software Management - Non-regulated	Records that confirm the operational effectiveness of Company software applications not subject to regulatory inspection. NOTE: Does NOT include records for software applications that are intrinsically linked to hardware.	Access authorization, Change control, Data models, Decommissioning materials, Design, Quality planning and reporting, Service documentation, Source code, Specifications and requirements, Support model, Testing, User acceptance, Validation	Decommissioned + 5 years

Legal holds, physical records, record destruction

Creating Certified Copies

- Create a policy to define the creation of a true certified copy to include the following details:
  - Approved system of record
  - Approved record types based on country regulations
  - ALCOA++ adherence
    - Complete scan
    - Page orientation
    - Correct pagination
    - No duplicates
    - No blank pages that are not in the original set
  - Verification/Validation of copy
  - Documented destruction
  - Reference governing bodies for compliance
    - GAMP Good Practice Guide: Electronic Data Archiving; ISPE, 2007
    - Scan/Declare/Destroy Guidance; Pharmaceutical Records and Information Management Organization; April 2015

Destruction of Records

- Create a destruction policy to include the following details:
  - Internal RIM destruction approver
  - Authorized personnel for onsite destruction
  - Destruction methods:
    - Physical:
      - Secure physical record storage through destruction
      - Must shred to ensure complete destruction
      - Cross cut or micro cut shredding
      - Provide destruction witness
      - Documentation proof of destruction
      - Third party shredding services must also comply
    - Electronic:
      - Use secure data deletion methods like degaussing to ensure no document recovery
  - An electronic log of approved records for destruction

Key takeaways

1. Initiate and enforce a retention policy at the earliest onset of a study
2. Use the longest relevant retention period as the ‘highest lowest common denominator’
3. Leverage a risk-based approach to your retention strategy
4. Ensure your destruction policy to be in compliance with your organization's retention policy

Thank You!

External Links

Regulations and Guidelines:

- FDA:
  - CFR 312.57 – link
  - Original publication – link
- Health Canada
  - Legislation - link
- EU CTR
  - Search for Articles 57 and 58 – link
- MHRA:
  - Current legislation – link
  - March 2023 update – link
- ICH E6 R3
  - Latest draft - link

Other references:

- AbbVie acquires Cerevel Therapeutics
  - Press release - Link
- Georgia Southern University
  - Digital preservation formats – Link
- Digital Preservation Coalition
  - Global 'Bit List' – Link
  - DPC RAM - Link