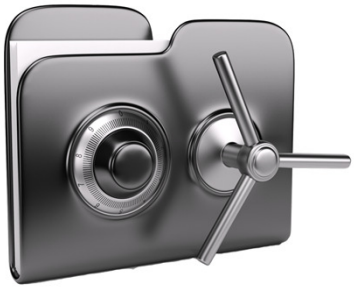
Key TMF Highlights from the MHRA GCP Guide

- Covering The Record Lifecycle & Compliance Challenges of Long Term Data Archiving

Webinar: 5 December 2012 @ 11am

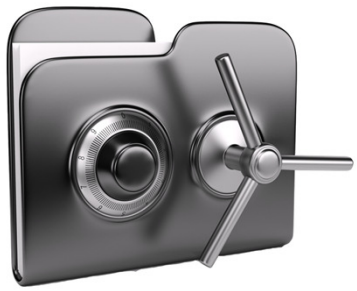


ARKIVUM
ASSURED ARCHIVING

Welcome to everyone – we're glad that you are able to join us today.
Just a couple of housekeeping issues before we get started – please can you ensure that you have your telephones switched to silent and should you need to leave the call at any point please don't place us on hold as this can result in your hold music playing out.

Speakers:

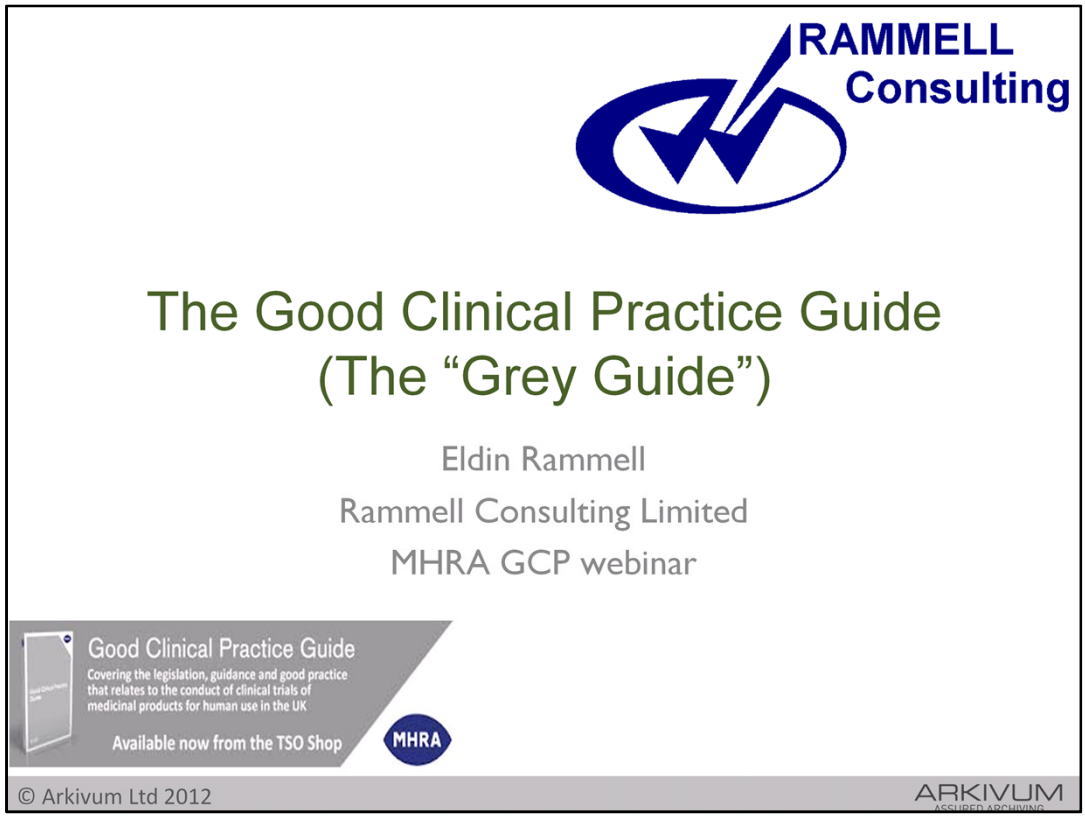
Eldin Rammell, MD, Rammell Consulting
Dr Matthew Addis, CTO, Arkivum



ARKIVUM
ASSURED ARCHIVING

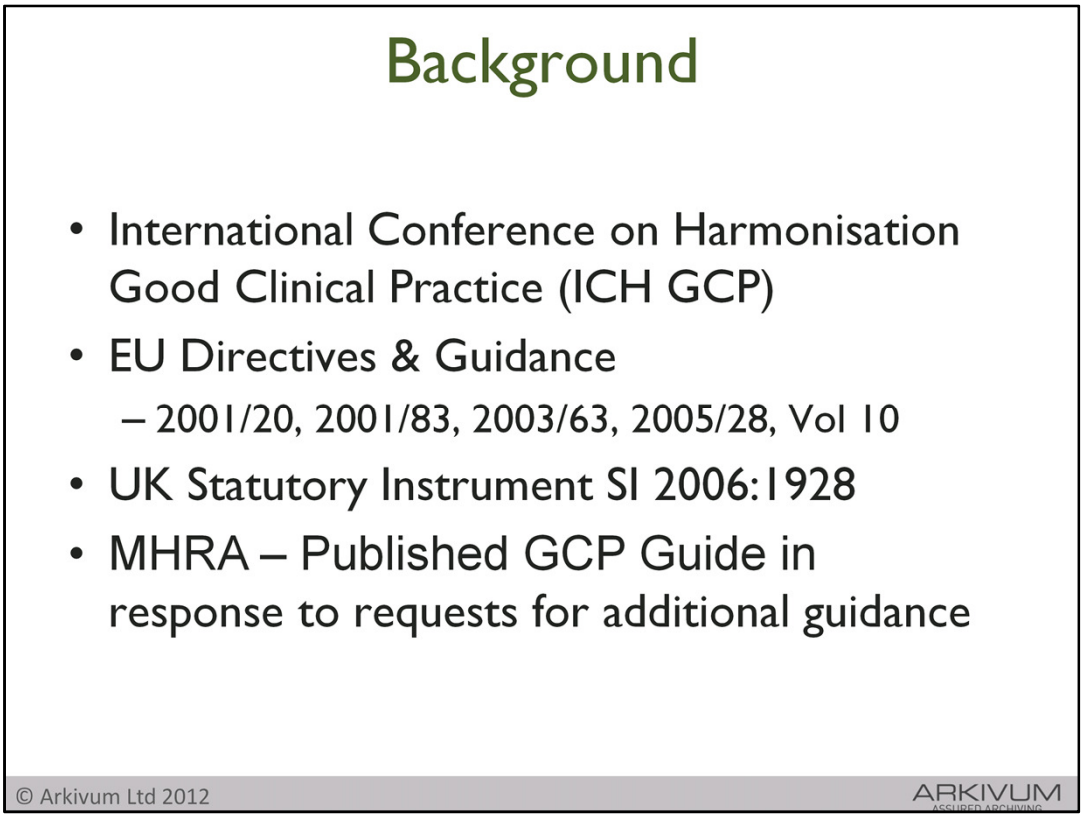
Today we are joined by Eldin Rammell who I am sure is familiar to some of you. Eldin is a record management consultant with a specific expertise in Trial Master File. Eldin will be taking you through the key TMF Highlights from the recently GCP Guide from the MHRA.

I am also joined by Arkivum CTO, Matthew Addis who will be focusing on the challenges long term data archiving with specific reference to TMF.



Let's start this session by looking at the background to this new guidance document.

NEXT SLIDE.



There have been regulations, legislation and guidelines relating to Good Clinical Practice for many years.

ICH GCP was perhaps the first international effort to document requirements for Good Clinical Practice. These were issued in 1996 and have not been revised since except for a minor amendment in 2002. So they are now 16 years old. Within Europe, a number of Directives and guidance documents laid down additional expectations for GCP compliance and these have been transposed into National legislation across the EU. In the UK, for example, we have the revised Medicines Act and associated Statutory Instruments. Equivalent legislation is present elsewhere globally, for example the Federal Food, Drugs and Cosmetics Act in the USA, supported by various Codes of Federal Regulations.

So the MHRA Guide is not new regulation. Rather it gives us an indication of MHRA thinking, based on many years of conducting GCP inspections. Does it have relevance and importance outside the UK? Yes, we believe it does, and we have attendees today from as far afield as the USA. The MHRA is extremely influential within the EMA for example with regards to records management, recently collaborating with Germany & Denmark on eTMF guidance. The MHRA is considered by many to be the most hard-line when it comes to TMF-related issues. The take-away message is that if you gain compliance with MHRA, you should be OK anywhere else!

So let's dip into the content of the guide.

NEXT SLIDE

Scope of Guide

1. Sponsor oversight
2. Clinical trials authorisations
3. Ethical review
4. **Key trial documentation**
5. Pharmacovigilance for clinical trials
6. Investigational medicinal products
7. Monitoring
8. Data management
9. Statistics
10. **Trial master file and archiving**
11. Investigator sites
12. Phase I clinical trials
13. Clinical trial samples
14. Quality systems

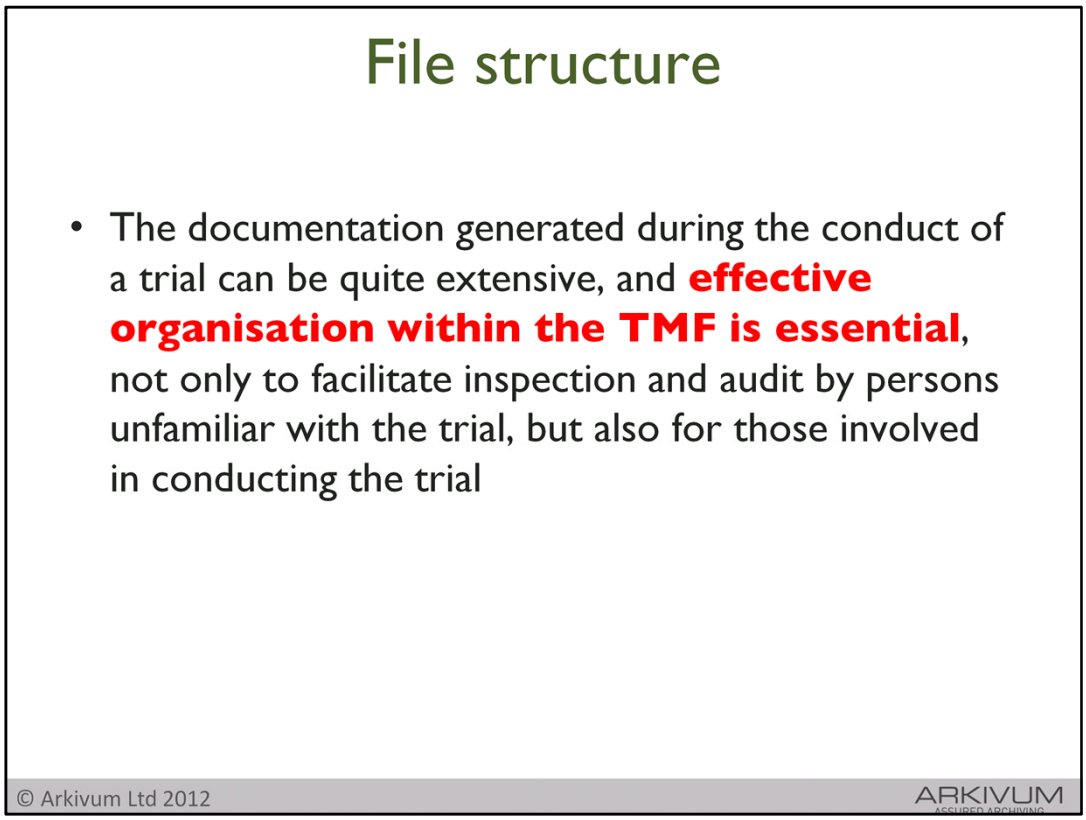
- GCP Inspections
- Legislation / guidance
- Advanced therapies
- IRT systems

ARKIVUM
ASSURED ARCHIVING

The first point to make is that the guide is very comprehensive. This slide shows the chapter headings and annexe headings but for this webinar we will only be focussing on records management topics which are primarily found in chapters 4 and 10.

The time available does not allow us to even cover all topics so we'll pull out guidance which provides the most help in clarifying often misunderstood issues, areas where there has been controversy in the past; and issues most relevant to electronic records and eTMFs in particular, as that is a hot topic for many presently.

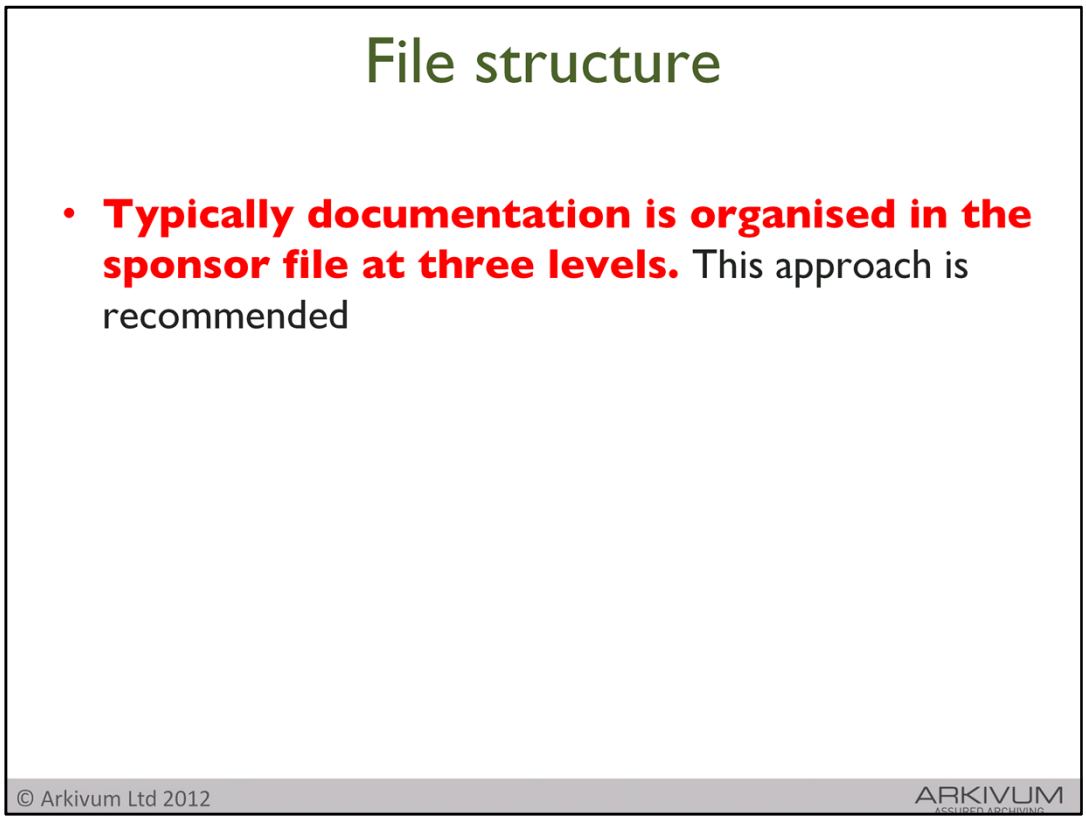
NEXT SLIDE.



The way that TMF content is structured within file systems is very variable across industry and that in itself is not a problem. However, the Guide stresses the importance of having an **effective** organisational structure.

This means having the organisational structure documented; ensuring it is consistently used; and ensuring end-users understand where to file documents and where to go to retrieve documents – in other words to be trained users.

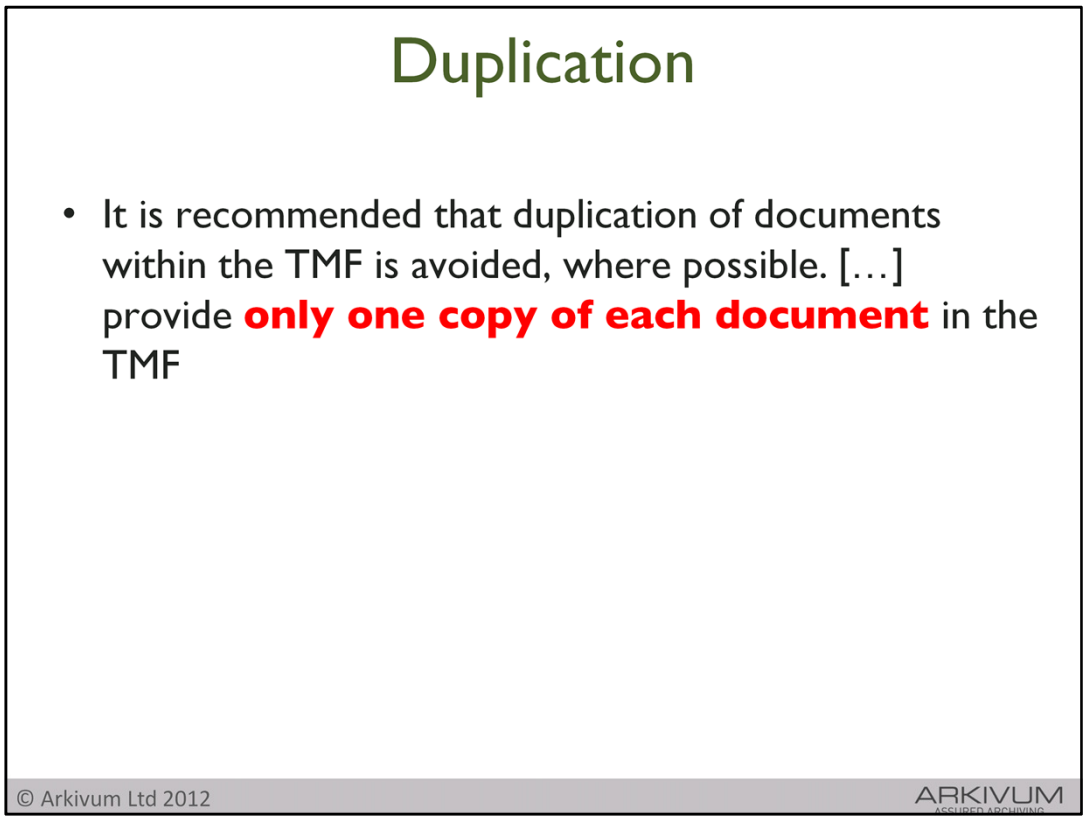
NEXT SLIDE



The most common approach to filing hierarchy is to recognise a trial-level document, a country-level document and a site-level document. Although this is not mandated, the MHRA identify this as being their preferred approach. Given that inspectors are one of our key stakeholders, I guess we should bear this recommendation in mind when it comes to developing an eTMF or purchasing an eTMF.

If we choose a different approach, it is likely that you'll need to be able to justify why you've taken a different approach and you'll need to ensure that navigation through the files is intuitive.

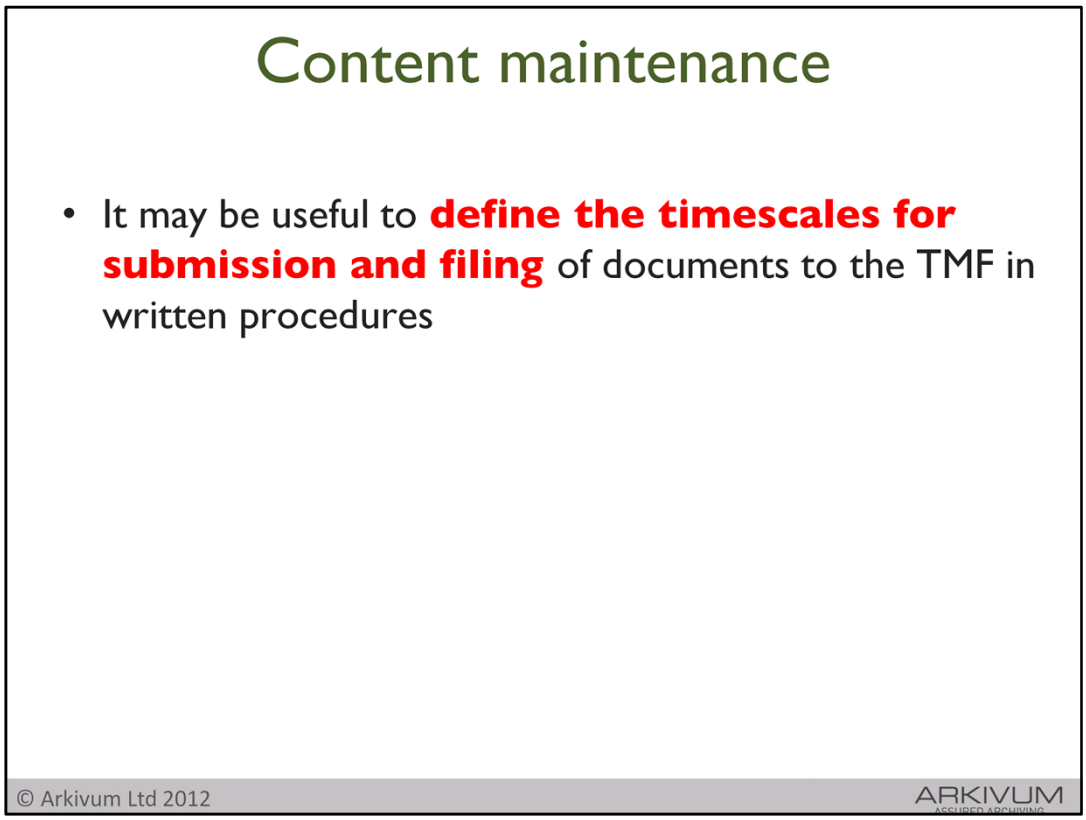
NEXT SLIDE



A trial master file often contains documents that relate to multiple sites, multiple countries or to multiple trial processes and some sponsors address this by filing duplicates across the files. This should be avoided if possible. In a paper file system, this can be achieved with various document location mechanisms. In an electronic file system, or eTMF, we can use the technology to link a single instance of a document to multiple locations virtually.

Just as a cautionary note, do consider how you structure your content for archiving. Although a program level document such as an IB is perhaps best only held in one location during a study, when the TMF is ready to be archived it may be appropriate to also archive a copy of the relevant IBs to avid the need to maintain hyperlinks.

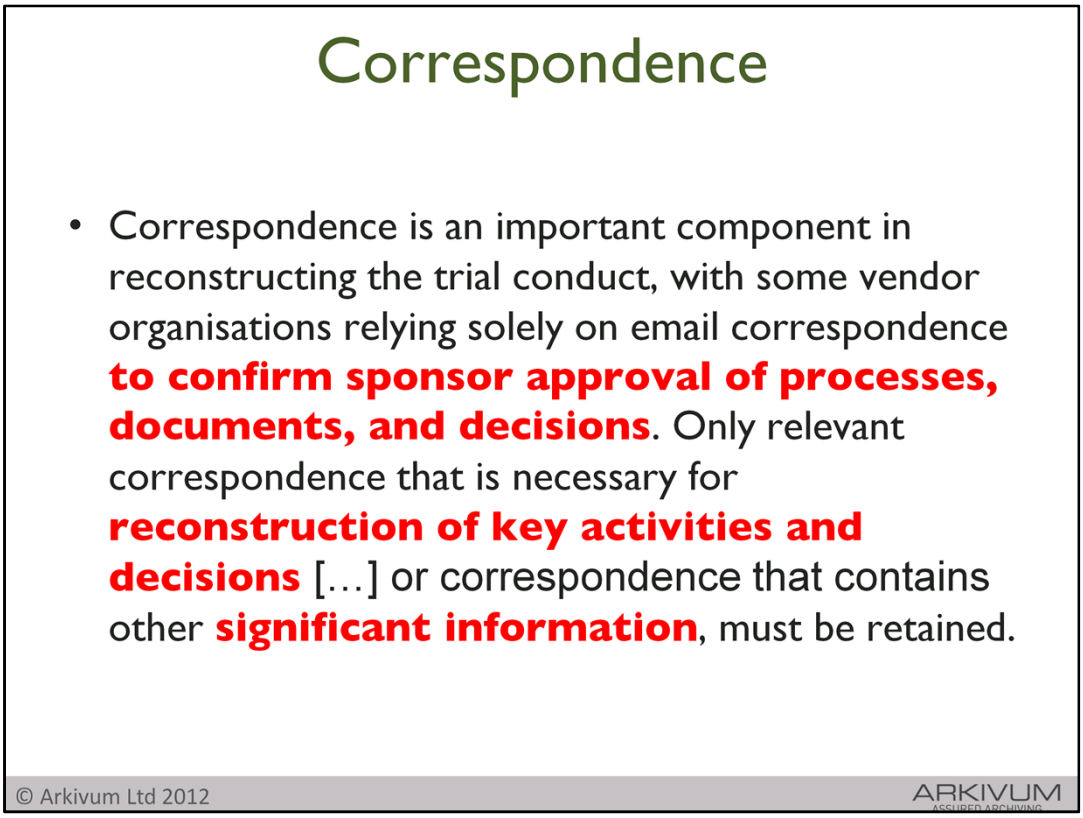
NEXT SLIDE



The timescales for adding content to a TMF are not defined by MHRA but the expectation is that the sponsor will define these timescales and include them in relevant SOPs. During an inspection, you will be expected to be able to demonstrate compliance with those timelines so it is important to think about what audit trail you can capture to show timely filing.

This also links to the concept of “chain of custody” which I will also mention later. How can the timeliness of upload of an external document be demonstrated if no record is kept of when the document arrived into the organisation? So think carefully about how steps in the document chain are being captured.

NXET SLIDE



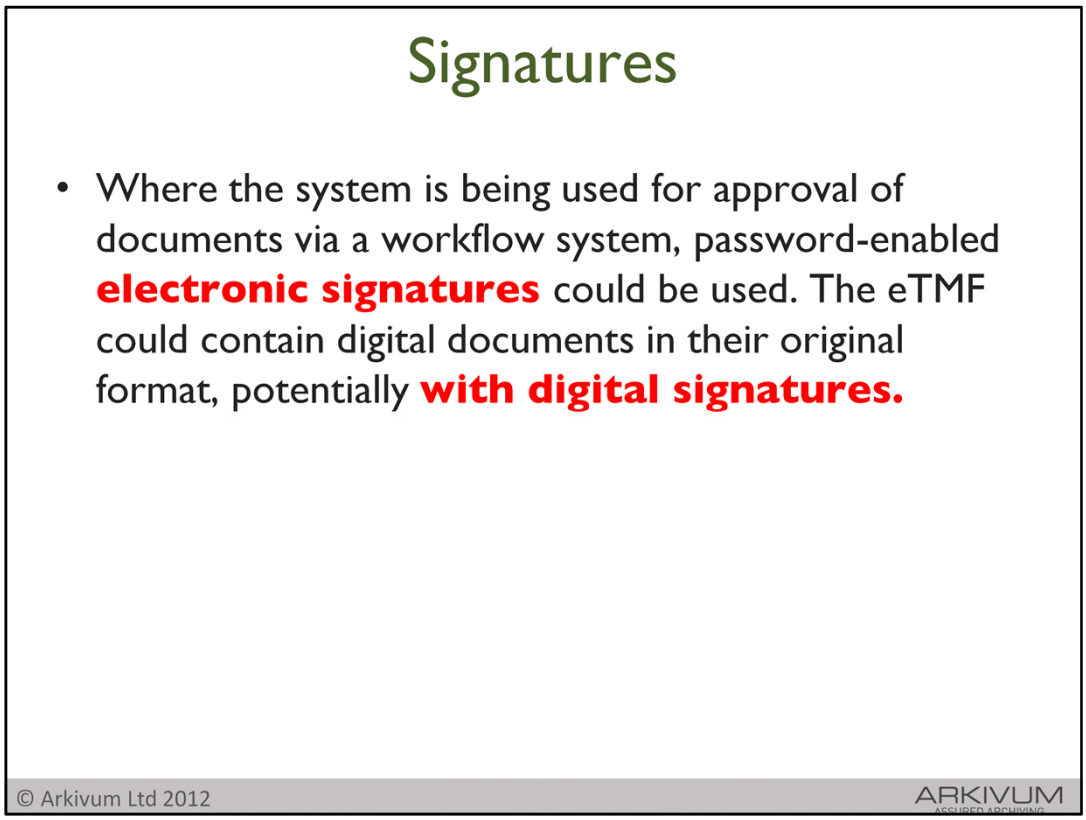
There has been much confusion historically about the management of correspondence. The grey guide provides help on 2 points:

Firstly, it confirms that documents and decisions can be approved using correspondence (e.g. email) rather than a handwritten signature on the document.

And secondly, it highlights the fact that the MHRA are really only interested in correspondence associated with key activities, key decisions and “significant” issues that are not already documented elsewhere.

It is also important not to leave the assessment of importance until the end of the study. It is far more effective to assess correspondence “little and often”! The MHRA also suggests documenting your process for determining what is considered relevant to the trial and further industry guidance on this topic is available from the GCP-RMA website at www.gcp-rma.org.

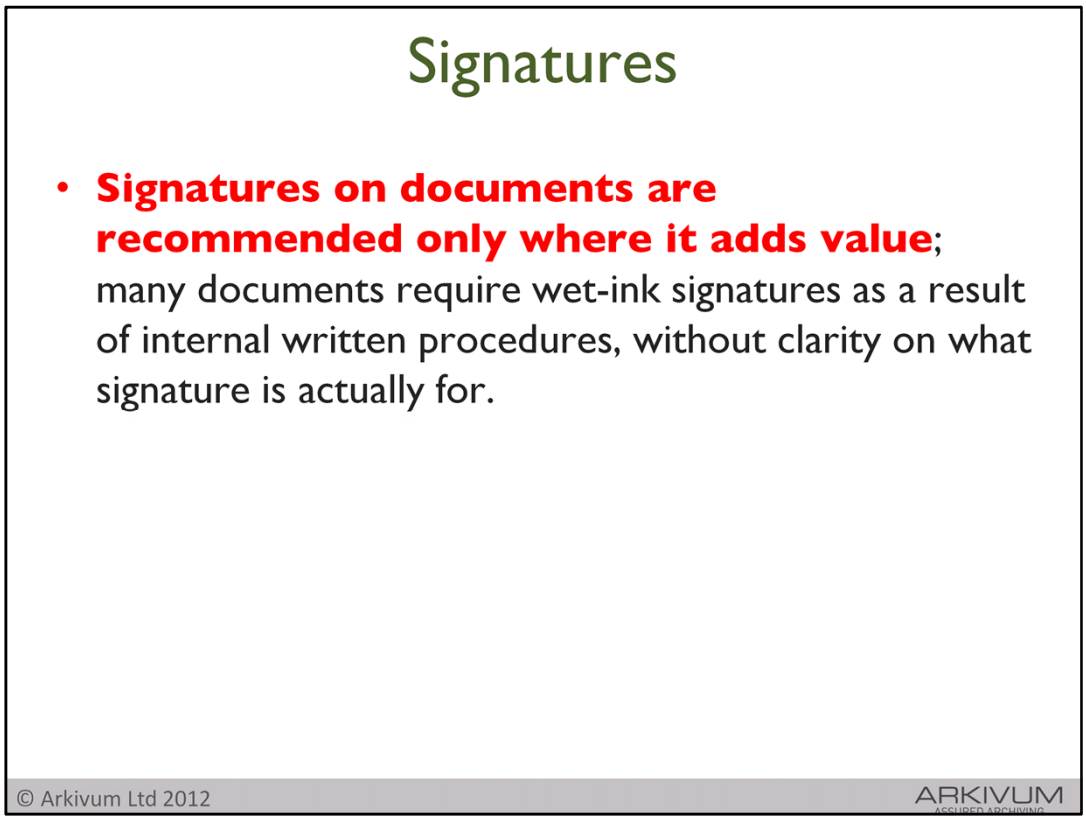
NEXT SLIDE



Legislation in the 3 ICH regions and in many other jurisdictions around the world make electronic signatures as acceptable and equivalent as a traditional wet-ink signature. In Europe, for example, this is provided for by an EU Directive on a framework for electronic signatures with supporting directives and communications. The Grey Guide confirms the acceptability of these manifestations of a signature to the MHRA whether you choose to use a simple electronic signature or an encrypted digital signature.

In terms of which type of signature you should use, simple electronic is potentially easier to implement with a workflow-based eTMF system BUT you do need to think about the long-term preservation of the content. In other words, the need to maintain the integrity of both the document and the electronic signature components inextricably linked to each other for perhaps 20 years or more. For this reason, a digital signature embeded within the document may be the preferred approach.

BUT the MHRA have also thrown in a more fundamental challenge to us on this topic. NEXT SLIDE



The MHRA are highlighting the fact that industry is signing documents without thinking about whether there is a regulatory need to sign or a justified business need to sign.

ICH GCP mentions only 5 documents where a signature is mandated: protocol and protocol amendment; agreements (contracts); informed consent (by investigator); case report forms (by investigator); CRF correction signature sheet.

All other cases therefore need a good business justification. The challenge for us is to ask ourselves "can meaning of a signature be captured in another way to avoid signing TMF documents?"

NEXT SLIDE

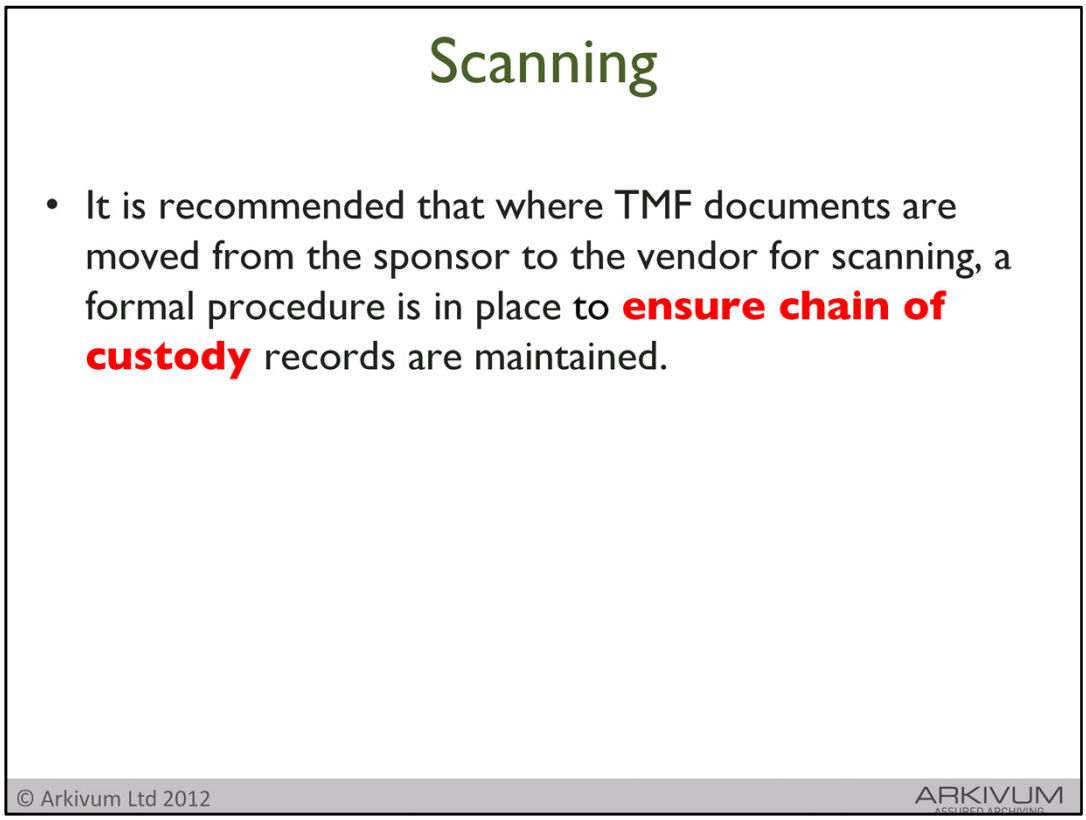
Scanning

- When original paper TMF documents are transferred to an electronic format (or other media) the **system of transfer should be validated.** This does not necessarily mean that the individual reviews every document, but that they have approved the validated system that is being used.

Ideally, our eTMFs would only contain born-digital documents and paper documents would not exist. However the reality is that some hard-copy documents are created and need to be digitised in order for them to be integrated into an electronic repository. The MHRA are saying that this process of digitisation or transfer must be validated to ensure you have a high quality process.

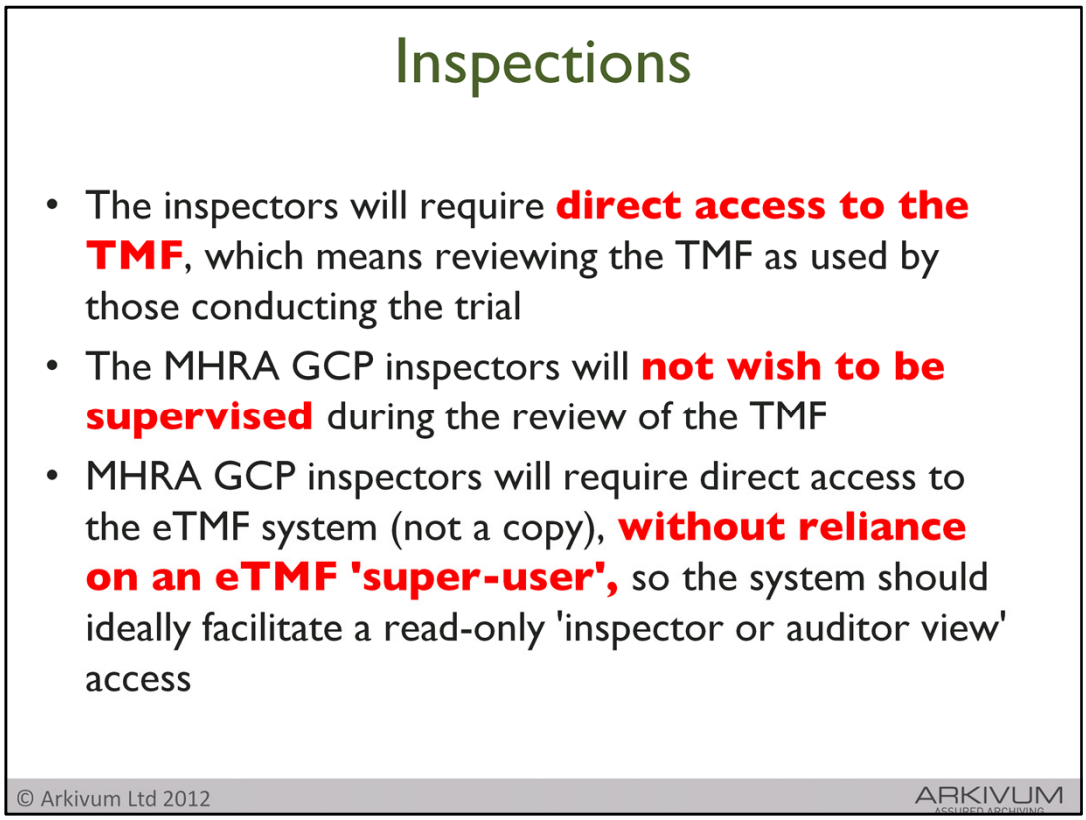
However, they recognise the need to take a risk-based approach to determine the level of quality control needed to provide assurance that the transfer process is accurate and reliable. For example, you may perform a 100% QC of content for new staff or for a small number of critical documents, and perhaps no QC at all for some content once the process has been validated. The MHRA supports this stance.

NEXT SLIDE



Still on the subject of scanning and coming back to the subject of “chain of custody” that I mentioned earlier. The reason this is highlighted by the MHRA is to avoid the possibility that content could have been tampered with between the point of creation – perhaps at an investigator site or at a CRO - and the point of filing in TMF, whether that is paper or electronic. Having an end-to-end audit trail provides an increased level of confidence in the process and therefore in the integrity of the documents.

NEXT SLIDE

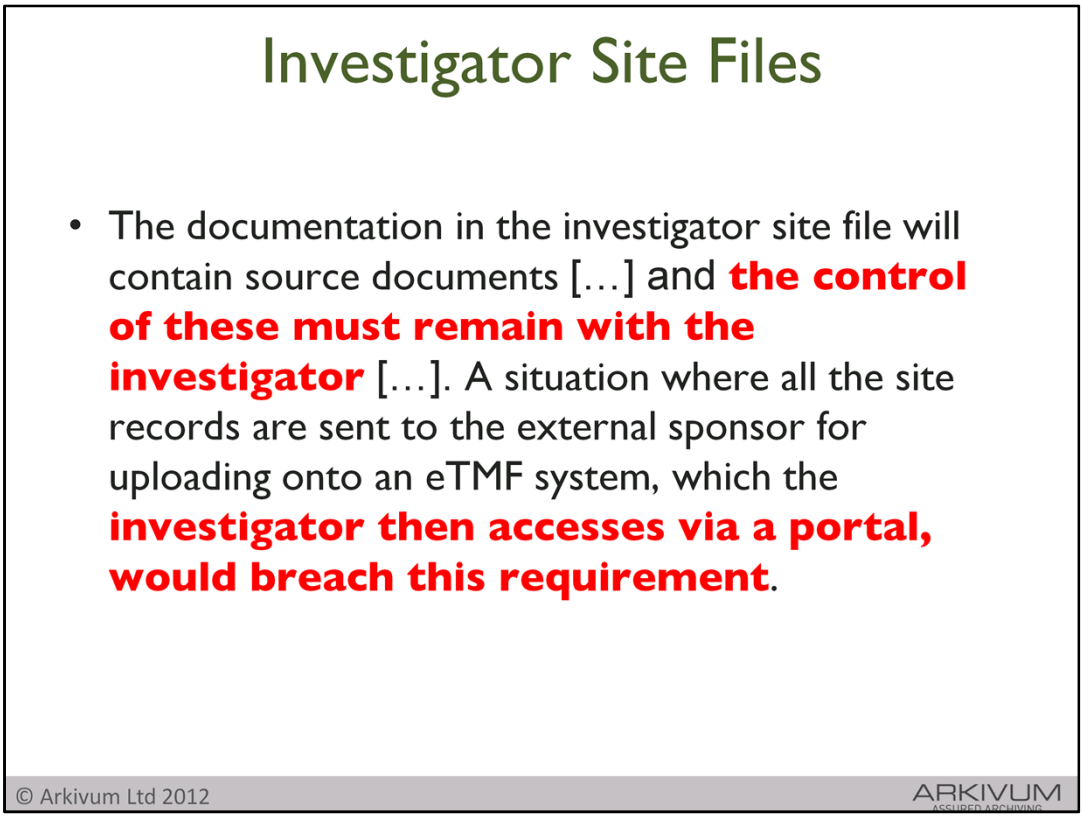


The TMF forms the basis of a GCP inspection so it is important to understand the MHRA's expectations for inspections. The MHRA will ask for direct access to the TMF and this means the TMF that staff are using on a day-to-day basis.

So, if monitors are using an e-repository such as an eRoom, a secure network drive or a SharePoint Site, that is what the inspector considers your eTMF to be and that is what they will want to see. It is unlikely that they will accept a download of content onto a CD or DVD. Neither will they accept a printout of the content.

Their review of the eTMF should be as equivalent to their traditional paper review as possible. This means that they want to see the full content – not just the Clinical Operations section - and they want to be unsupervised. So, think carefully about the usability of your eTMF, the access rights available and the training requirements (the MHRA have mentioned "no more than 1 hour" for training).

NEXT SLIDE



Last but not least, the Grey Guide also talks about the Investigator Site File. They confirm that an eISF is OK but the investigator must be able to demonstrate that he/she maintains control over the content.

You also need to think about what the investigator is going to be provided with following closure of the trial. It is unlikely to be acceptable to make a copy at the end of the study and expect the investigator to sign to confirm it is his/her content.

NEXT SLIDE

Further reading

Good Clinical Practice Guide
£45.00 +VAT +p&p

http://bit.ly/WG7AQw

ARKIVUM
ASSURED ARCHIVING

This webinar has just been a brief overview of the key areas of the guide relating to TMF content. I'd strongly recommend purchasing the guide if you have not already done so.

It should be mentioned that this 542-page book will soon be made available electronically for iPADs and Kindles.

NEXT SLIDE

Thank you

- http://rammell-consulting.co.uk
- eldin.rammell@rammell.com

ARKIVUM
ASSURED ARCHIVING

If anyone wishes to get in touch with me after this webinar finishes to follow-up on some of the topics, please do not hesitate to get in touch.

ARKIVUM
ASSURED ARCHIVING

GCP guidelines: archiving eTMF

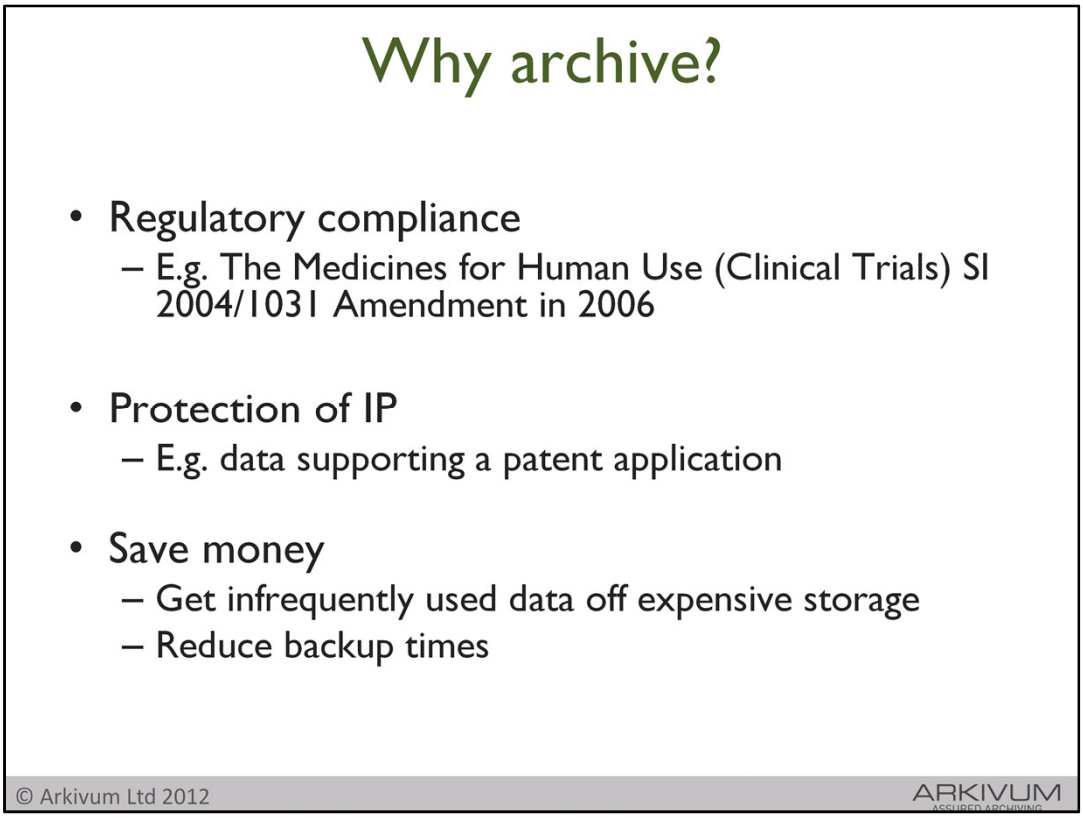
Dr Matthew Addis
Arkivum Ltd
MHRA GCP webinar

Contents

- The need to archive
- What the GCP guide says
- The challenges of long-term data retention
- The Arkivum solution

"Security is of key importance to our business, Arkivum's A-Stor Pharma service allows us to store our encrypted data for the long term in a cost efficient way that is entirely scalable and reduces pressure on our internal IT infrastructure."

Dan Watkins, Oxford Fertility Clinic



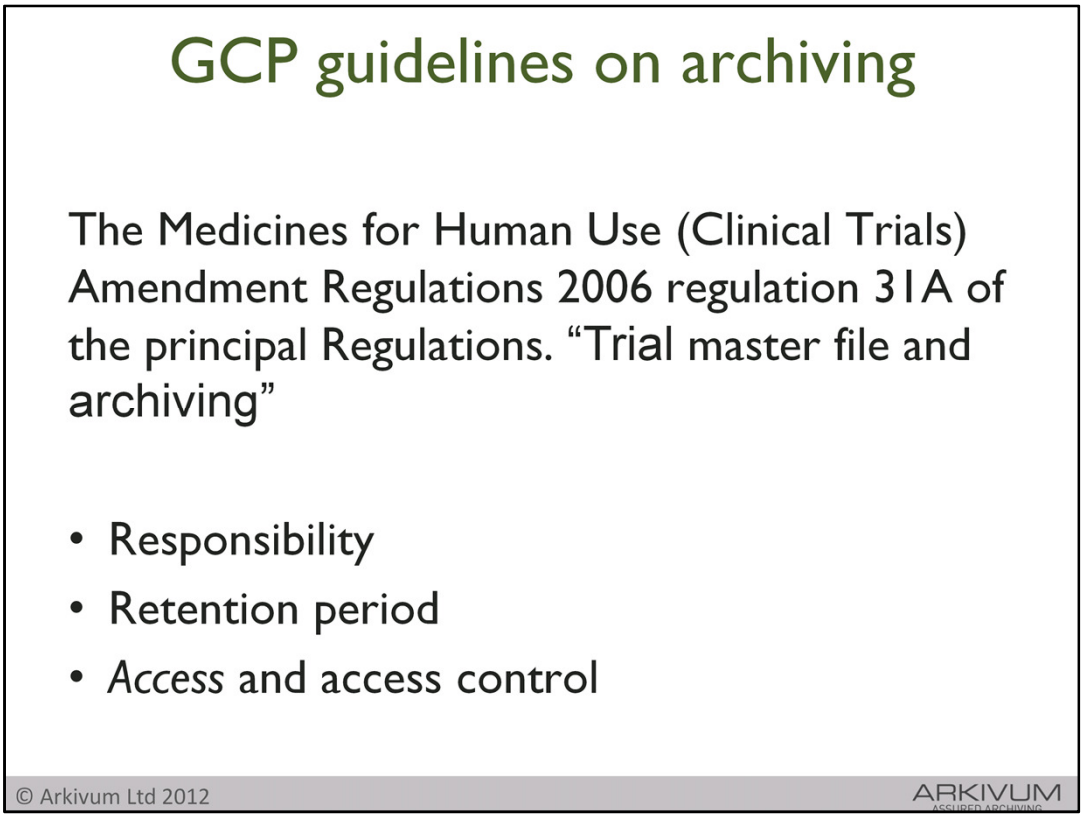
There are several reasons to archive data, which include:

Because you have to, for example meeting legal regulations on clinical trial data.

Or because you have value in the data, for example it supports a patent application

Or because it saves money.

The systems used for holding data when it is first created and processed are really expensive places to store data for the long term. Moving data to a proper archive system can save money, not just by reducing primary storage needs but also in turn by needing less resource for associated maintenance and backup.

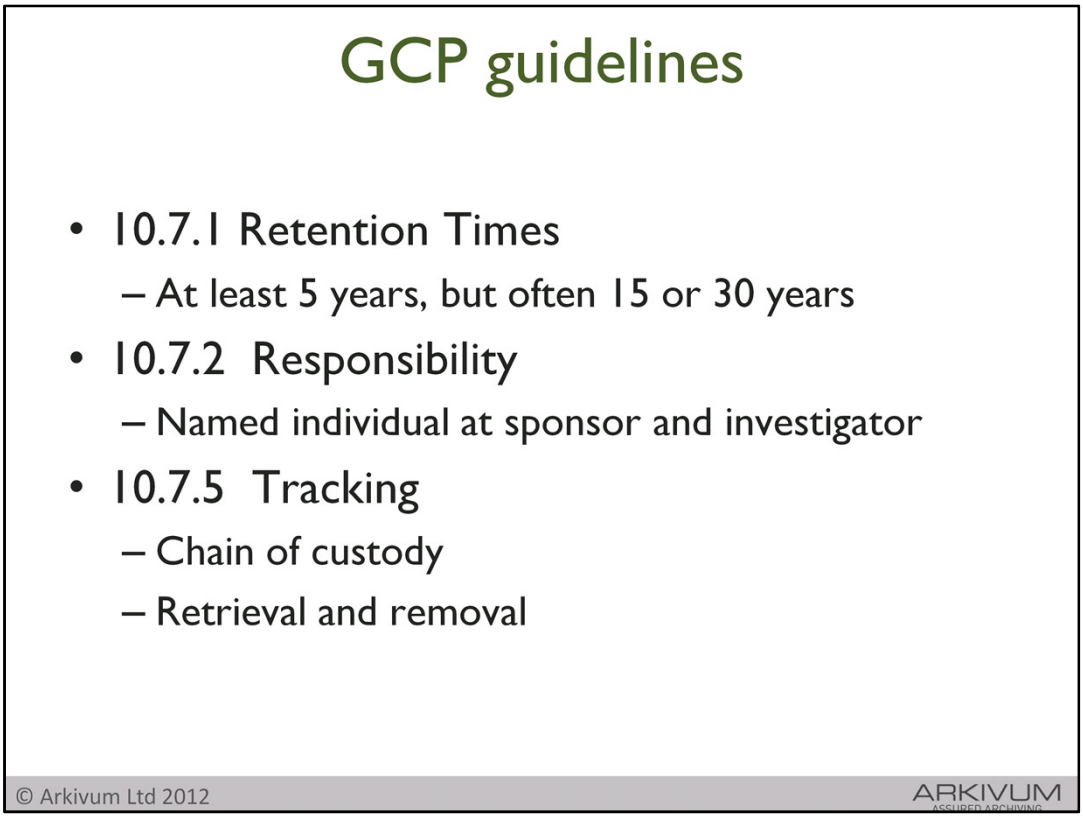


So what does the GCP guide have to say?

The guidelines on archiving come mainly from an amendment made in 2006 to the Medicines for Human Use Clinical Trials Act (SI 2004/1031). The amendment defines the responsibility for archiving, how long data needs to be kept for, who can access it and why, which includes auditors, but most importantly it states that data must be accessible.

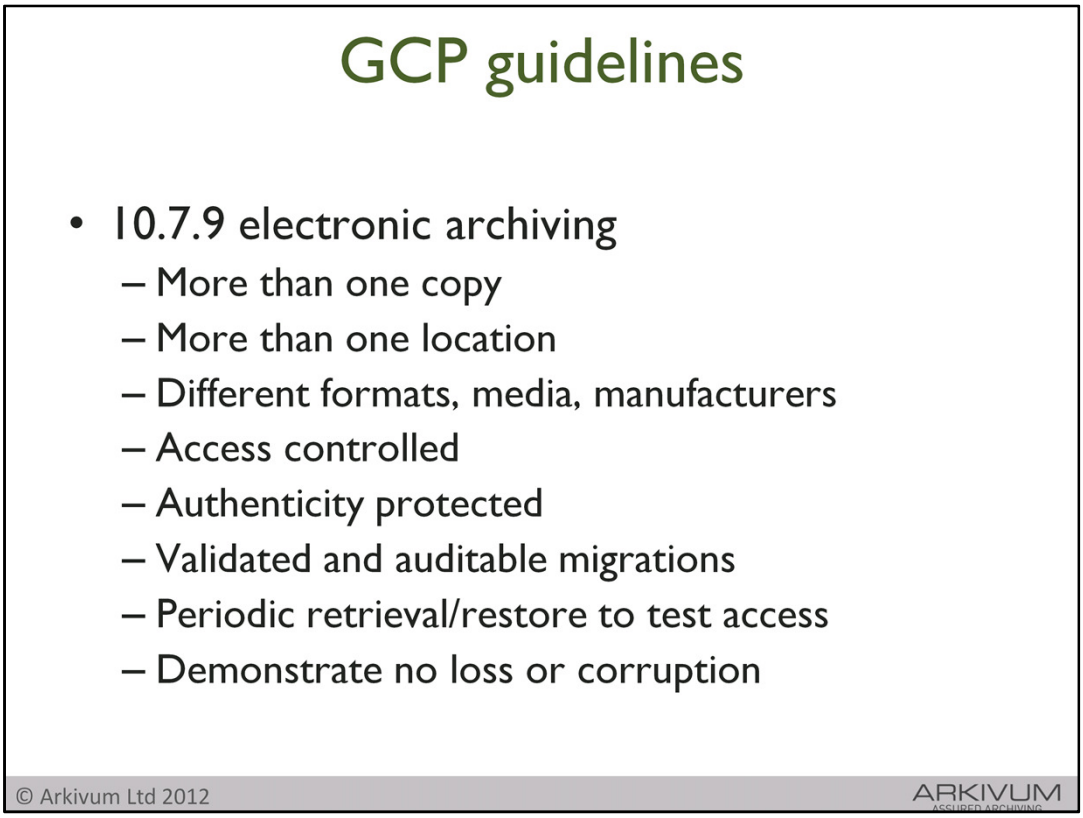
Similar regulations exist outside of the UK, for example EU Directives and FDA regulations. All take a similar line that archiving has to ensure the integrity, authenticity, confidentiality and accessibility of documents for the required retention period.

For the UK statute, the word access is key – which as we'll see has big implications over the timescales for which data has to be kept.



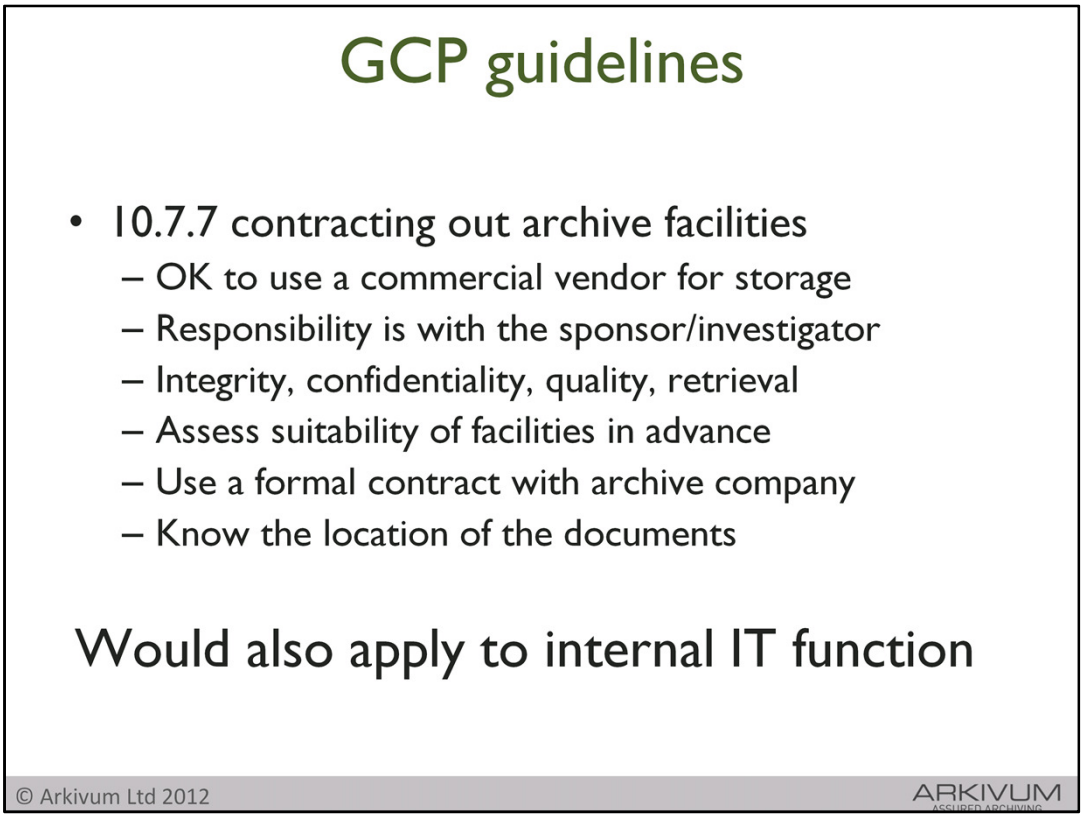
The guidelines then provide recommendations on what needs to be done to meet the regulations, including:

- What retention times will apply and the further regulations that mandate them
- Who is responsible for archiving and the legal requirement for the sponsor to have a named individual (with suggestion that investigator site does likewise)
- And that any documents that are archived are properly tracked, i.e. there is a chain of custody to whoever stores them and that their location is tracked if documents are taken out of the archive



The GCP guide has many recommendations on electronic archiving. These are largely around best practice of how to:

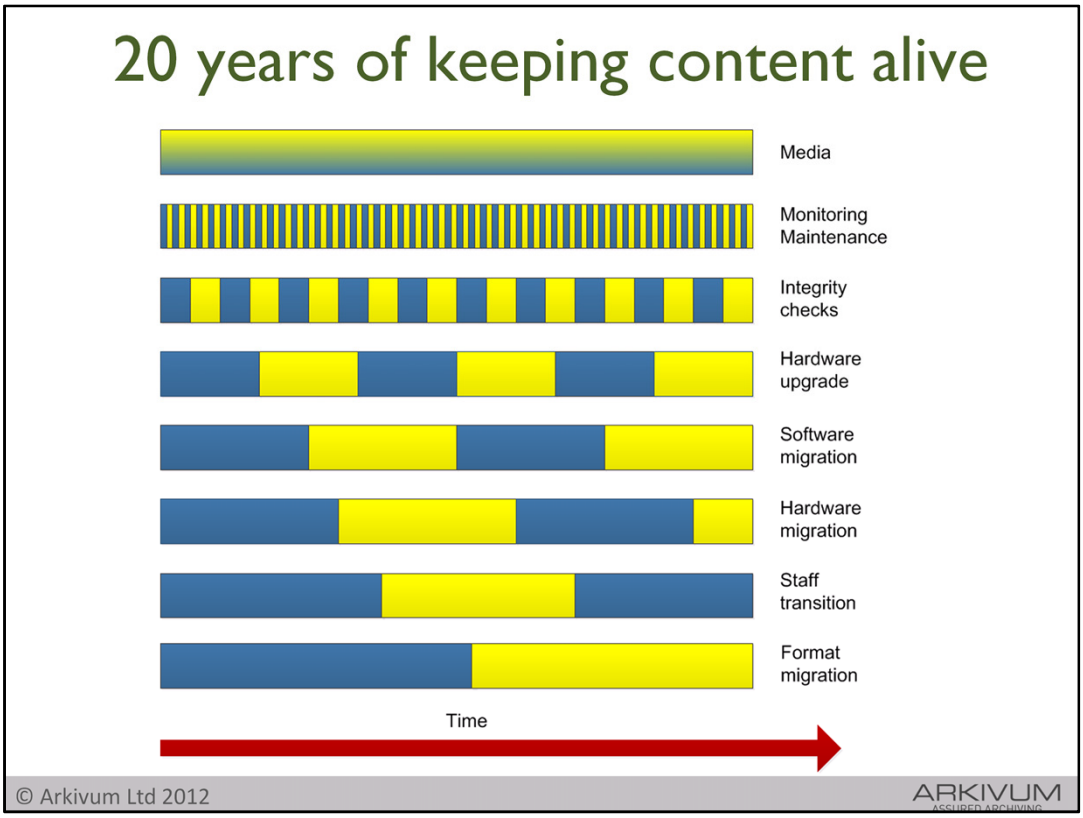
- maintain the ability to access and use documents in the future
- controlling access
- tests/validation that any interventions required to maintain access, e.g. migrating to a new storage system or format have been done properly



There are also specific guidelines on use of third-party archive facilities, which apply to both electronic and paper based documents.

The key things here is that:
- Responsibility remains with the sponsor/investigator
- The sponsor need to assess whether a third-party is able to do the job properly and within the regulations
- What the third-party will do needs to be formalised in a contract
- The sponsor's other responsibilities such as tracking documents still hold

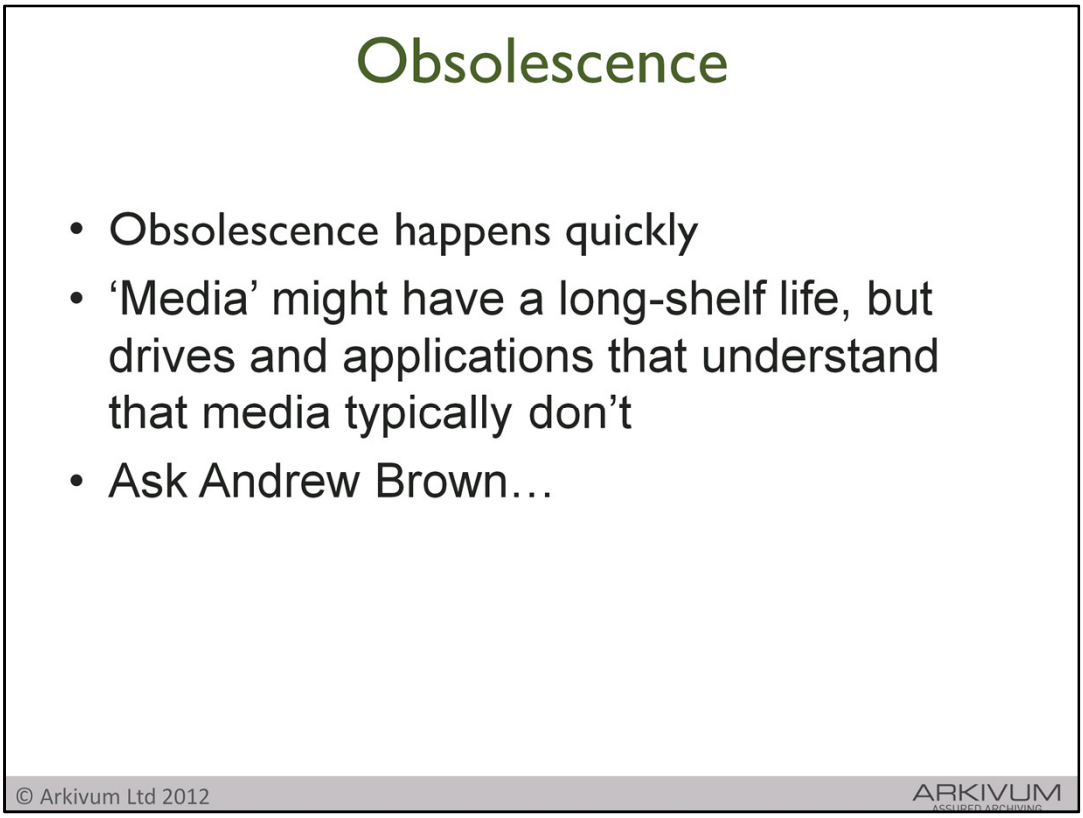
I think it is important to point out that because it's a named individual at the sponsor/investigator that's always responsible, these requirements would hold equally to an in-house set-up, e.g. asking an IT department to archive eTMF data.



So why's keeping archive content accessible so hard? These are just some of the things that will happen over 20 years of trying to retain data.

In the diagram, a change from blue to yellow is when something happens that has to be managed. In a growing archive, adding or replacing media, e.g. tapes or discs, can be a daily process, so is effectively continual. The archive system needs regular monitoring and maintenance, which might mean monthly checks and updates. Data integrity needs to be actively verified, for example annual retrievals and integrity tests. Then comes obsolescence of hardware and software, meaning refreshes or upgrades that will typically be 3 – 5 years, for example servers, operating systems, application software. In addition to technical change in the archive system is managing staff transitions of those who run the system, for example support staff and administrators. Even the format of the data being held may need to change, even long-lived formats such as PDF-A will eventually be obsolete as they are replaced with something better and applications no longer provide backwards compatibility.

The key point is that long-term archiving is an active process and there's always some form of change going on. And when change happens there's always a risk that something goes wrong, and there's always the need to validate that the change has been effected properly. This all requires time, expertise and money. Digital archiving is very different to paper archiving – it's not a case of 'file and forget' rather it's a case of continual interventions to keep content alive and accessible.



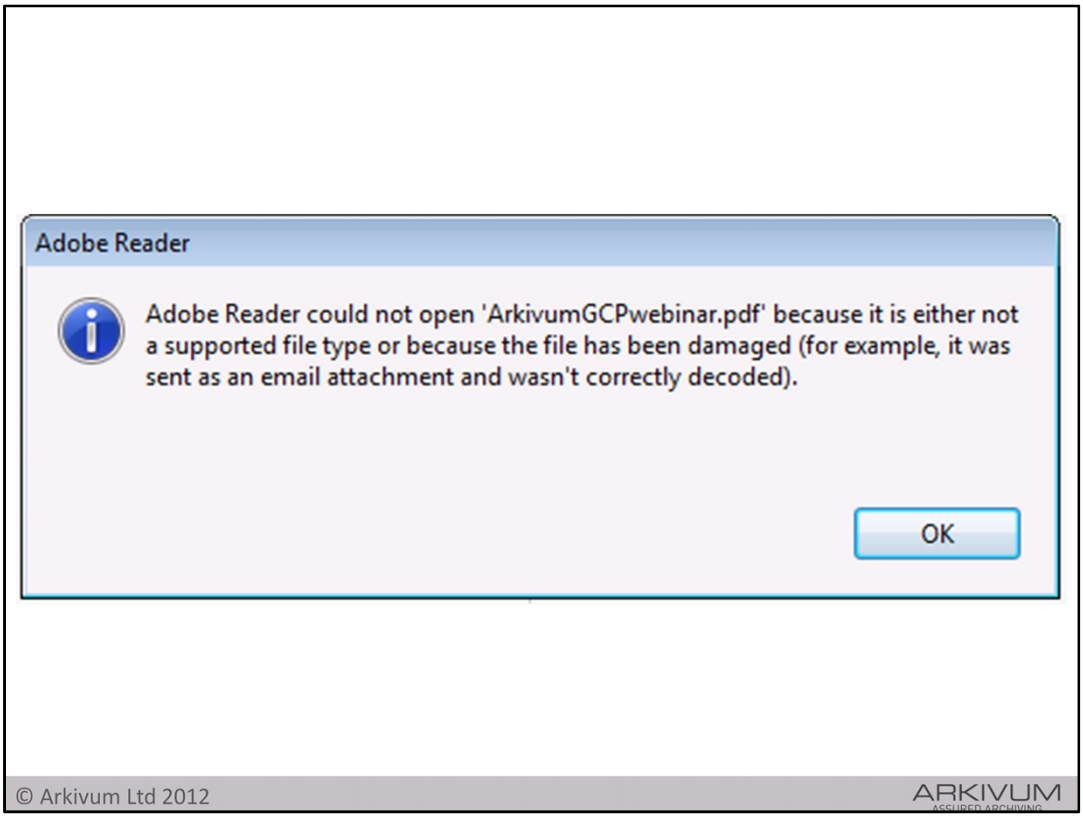
Andrew Brown has found out the hard way why technical obsolescence presents a major threat to the long-term access of digital data. He asked his local hospital for a copy of an echo cardiogram that was performed on him in 2004. The BBC [1] reported that the Worcestershire Acute Hospitals NHS Trust said it would cost £2000 for him to be given a copy of his data. The Register reported that the trust said this "was not a cost-effective use of public money" [2]. The hospital does have his echo cardiogram data, which is stored on Magneto-Optical disk, but the hospital no longer has a drive that can read these disks as they have subsequently installed a new archive system [3]. Their supplier apparently said that they didn't stock the drive anymore as it was no longer in production and they would have to ship a drive in from the United States if the Hospital wanted to read the data. That's technical obsolescense in action – and in just over 6 years. This sort of thing really does happen. One thing to think about carefully is whether apparently 'long-lived' media is the right way forward. It's tempting to think that using specialist storage media that's designed to last for decades or centuries is the answer, including magneto-optical disks and other forms of 'archival grade' storage. But this technology often addresses a niche market, which means it can be harder for the companies who develop and sell it to make a sustainable business. The storage media might last for decades, but the companies who make it might not, or they are forced to move on to develop something new.

[1]http://www.bbc.co.uk/news/uk-england-hereford-worcester-20235193
[2]http://www.theregister.co.uk/2012/11/08/nhs_scan_2k/
[3]http://www.whatdotheyknow.com/request/94658/response/237590/attach/2/attachment.pdf

So suppose you go down the route of using commodity IT storage rather than specialised media that can become obsolete. Well, no storage is 100% reliable, so there's another set of risks to deal with. Hard drives are an example of supreme engineering, but they do go wrong – as a colleague in the storage industry said 'they are designed to be on the edge of not working'. 1% of hard drives simply fail each year – they won't work at all – and those that do work can suffer data corruption issues – even if used in storage systems (e.g. RAID arrays) that are meant to protect against data loss.

If you have data on USB drives on a shelf then worry.

And if you have data on a server, then also worry – but this time about the 10s of thousands of lines of software and firmware code that's in those servers and the bugs that we all know software contains.

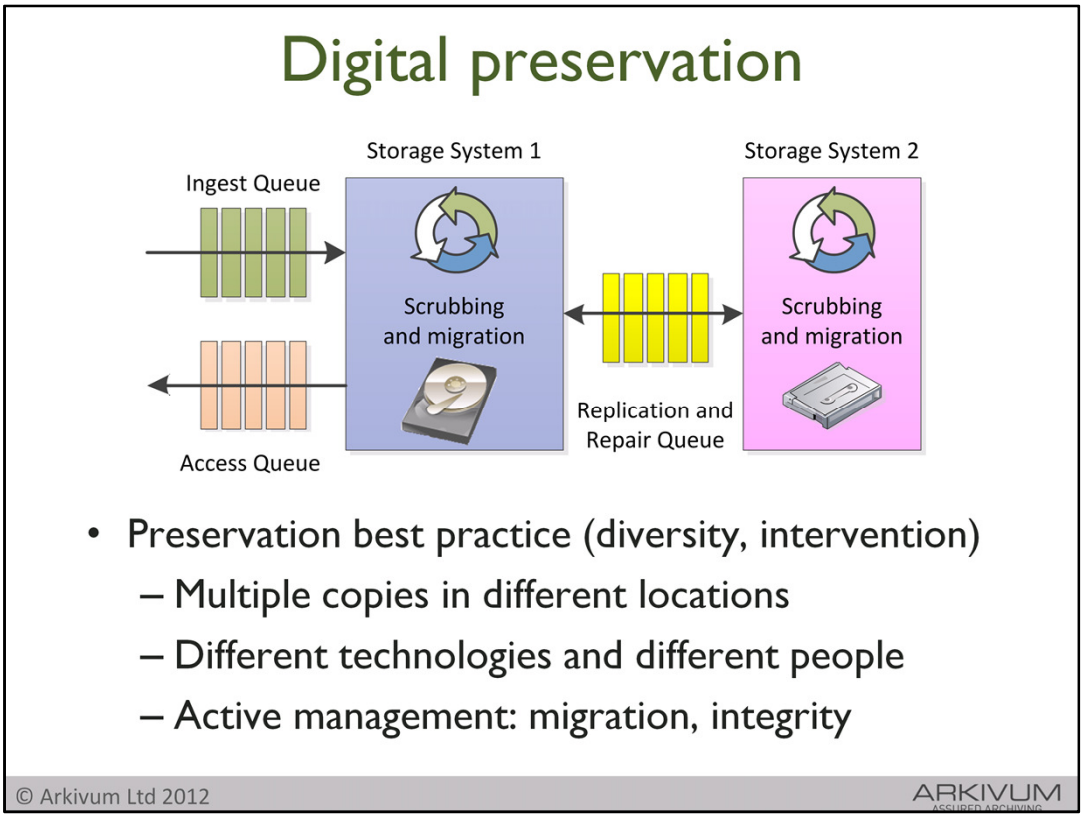


And this is what happens when there's a problem.

It's typically 'all or nothing' when it comes to reading a damaged file. A failure often means heroic (and costly) measures to get the data back – if you can at all.

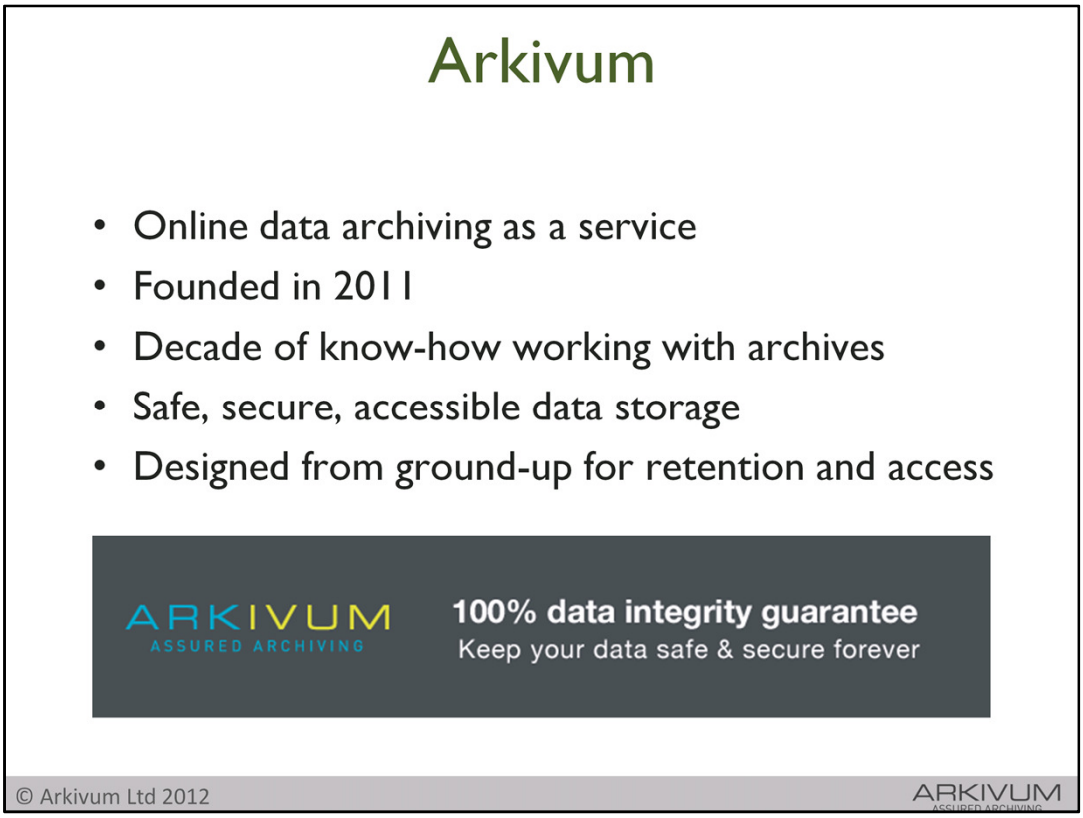
CERN did a test on their storage systems – which had been designed to keep data safe - 33700 files were written to storage and read-back again. (~8.7 TB). 22 were corrupted – and worse still, silently corrupted, i.e. they only knew because they checked each one.

CERN also did a test to see the impact of corruption. They took 10000 compressed files (zip) - 99.8 % wouldn't open if there was just a SINGLE bit error.



So what do you do. The GCP guidelines are pretty good and mirror general digital preservation best practice.

- You make multiple copies of the data and you keep them in different locations.
- You use diverse technologies to spread the risk of failures, which effectively means not all eggs in one basket
- And you actively manage these copies by (a) migrating to new storage or formats to address obsolescence and (b) by regularly checking and repairing any loss of data integrity (which is why having multiple copies is so important – if there is a problem with one of the copies then it can be replaced by replicating one of the other good copies)

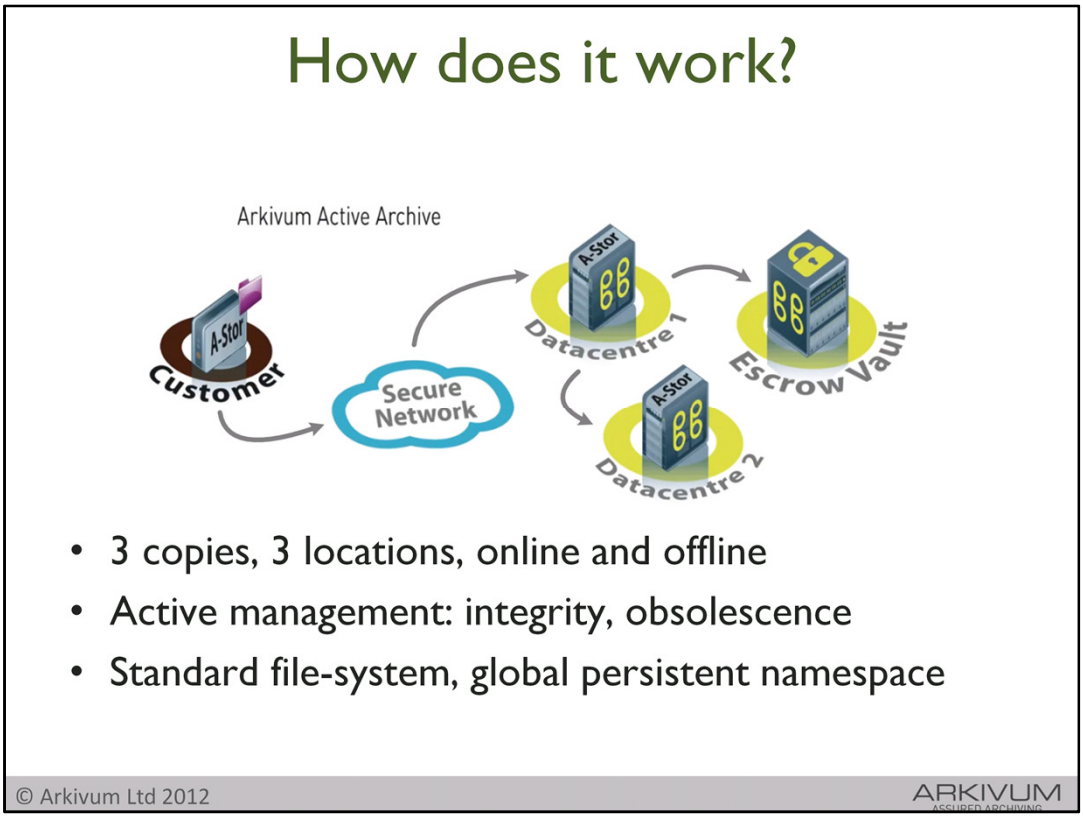


And this is exactly what we do at Arkivum.

Arkivum provides online data archiving as a service for those organisations that need to keep data for the long-term for compliance or reuse. We have customers in construction, life sciences, energy and voice call recording to name but a few.

The company was founded in 2011 as a spin out of the University of Southampton and is based on expertise the founders have from working with large archives, for example national broadcasters, over the last 10 years on how to retain digital assets for the long-term.

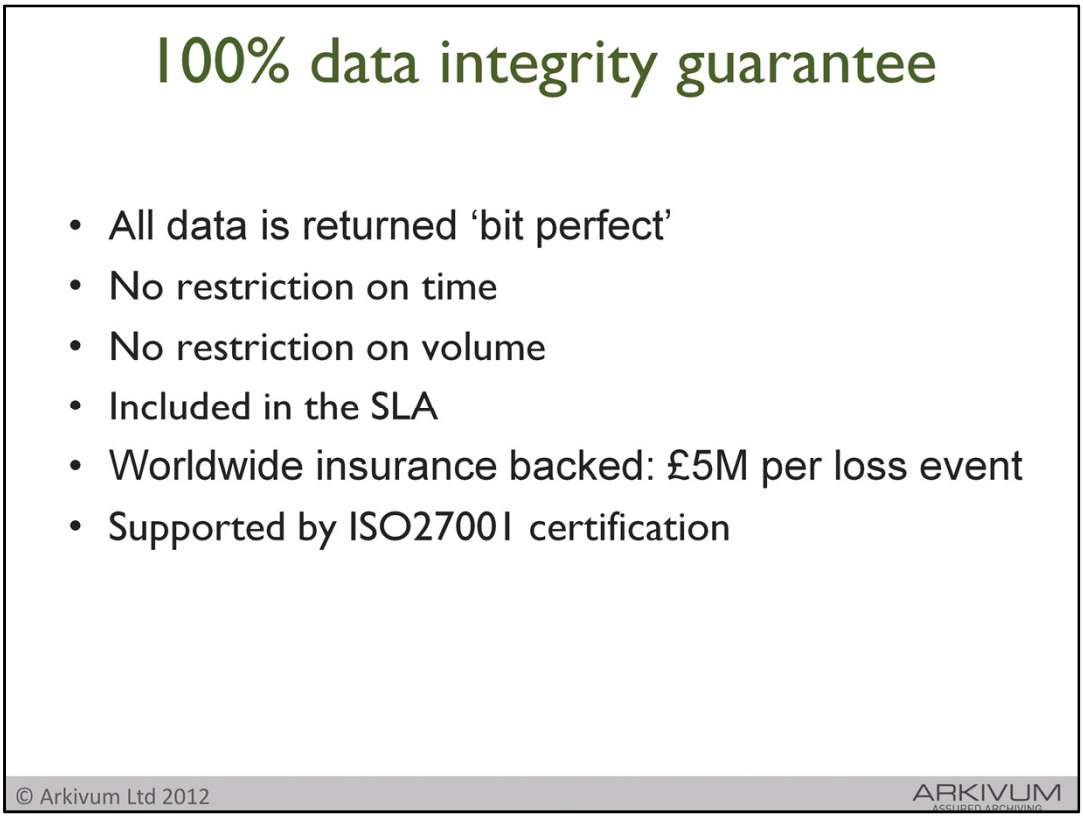
The result is a service that provides safe and secure storage of data that is easy to access whenever it's needed.



Customers use our service through an appliance that sits on their network which provides them with a gateway into our service. The appliance encrypts customer data and generates fixity checksums. Data is then replicated to online data tape libraries in two separate data centres. A third copy is then stored off line with a third-party escrow provider – but more of that in a minute. When we have the three copies in our service then the customer can choose to remove their local copy if they want to.

Three copies of customer data in three locations with two online and one offline allows us to follow data preservation best practice. We use the fixity information to actively manage data integrity through regular checks and we do regular media and infrastructure migrations to counter obsolescence and to ensure costs remain low and performance remains high.

Not only can we deliver this as a service from our facilities, we can also bundle the whole thing up and install and operate it on the customer site or in the customer's data centre if security of legislative reasons require an 'onsite' solution.



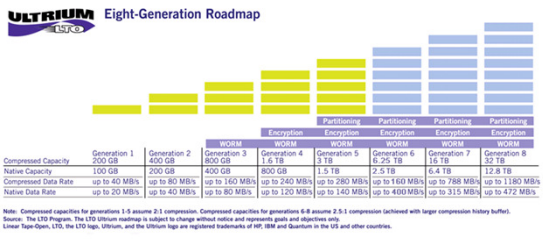
Good preservation practice based on data tape technology, trained staff and very carefully controlled processes also means we can offer a guarantee of data integrity.

All data returned from our service is always bit-for-bit identical to the data the customer supplied, with no restrictions on time or volume.

The guarantee is backed by insurance, is included in our SLA. Furthermore, Arkivum is certified to ISO27001, which is an information security management standard where Arkivum has been audited for the integrity, confidentiality and availability of data assets in our possession. You might want to compare this with other cloud storage providers

Data escrow

- Copy of data offline at third-party escrow site
- LTFS on LTO tape with open source tools
- Customer has access to escrow copy:
  - If we fail to provide the service
  - If the customer decides to leave



	Generation 1	Generation 2	Generation 3	Generation 4	Generation 5	Generation 6	Generation 7	Generation 8
			WORM	WORM	WORM	WORM	WORM	WORM
				Encryption	Encryption	Encryption	Encryption	Encryption
					Partitioning	Partitioning	Partitioning	Partitioning
Compressed Capacity	200 GB	400 GB	800 GB	1.6 TB	3 TB	6.25 TB	16 TB	32 TB
Native Capacity	100 GB	200 GB	400 GB	800 GB	1.5 TB	2.5 TB	6.4 TB	12.8 TB
Compressed Data Rate	up to 40 MB/s	up to 80 MB/s	up to 160 MB/s	up to 240 MB/s	up to 280 MB/s	up to 160 MB/s	up to 788 MB/s	up to 1180 MB/s
Native Data Rate	up to 20 MB/s	up to 40 MB/s	up to 80 MB/s	up to 120 MB/s	up to 140 MB/s	up to 400 MB/s	up to 315 MB/s	up to 472 MB/s

Note: Compressed capacities for generations 1-5 assume 2:1 compression. Compressed capacities for generations 6-8 assume 2.5:1 compression (achieved with larger compression history buffer).
Source: The LTO Program. The LTO Ultrium roadmap is subject to change without notice and represents goals and objectives only.
Linear Tape-Open, LTO, the LTO logo, Ultrium, and the Ultrium logo are registered trademarks of HP, IBM and Quantum in the US and other countries.

ARKIVUM
ASSURED ARCHIVING

Because we use data tape, we can create an offline copy of customer data that is lodged with a third-party under a three-way agreement between us, them and our customers.

Use of LTO and LTFS with open source tools means restoring data from escrow is easy and has no lock-in to hardware or software vendors, including us.

Customers can access the escrow copy of their data if we either fail to provide our service or if the customer decides to leave. This gives customer reassurance and an easy exit-strategy if the need it, which is something you don't see with cloud storage providers.

Transparent pricing

- *Long-term* retention and access
- Pay as you go
- 10 year fixed price
- 25 year fully Paid-Up

ARKIVUM
ASSURED ARCHIVING

Finally, because we specialise in long-term retention and access using data tape, and have full control over our infrastructure, we have predictable and falling costs. This means we can offer a fixed-price for long-term storage, which for say 25 years is about the same as many enterprise cloud storage vendors charge for just one year!

For our customers, this means predictable costs and lower risk that if the money isn't there in the future for storage, for whatever reason, then their content won't be lost.

Thank you

- www.arkivum.com
- matthew.addis@arkivum.com

"Arkivum has helped us to create a robust archiving solution that will allow us to focus our budget on the business rather than yet more storage"

"Archived documents can then be seamlessly accessed from within the document management system, in the same way current documents are".

ARKIVUM
ASSURED ARCHIVING

Thank you

- www.arkivum.com
- matthew.addis@arkivum.com

"Arkivum has helped us to create a robust archiving solution that will allow us to focus our budget on the business rather than yet more storage"

"Archived documents can then be seamlessly accessed from within the document management system, in the same way current documents are".

ARKIVUM
ASSURED ARCHIVING