

# The ECRIN Data Centre Certification system

Steve Canham

## The Data Centre Certification Programme

Origins, rationale,  
Very brief history, the role of national networks  
Nature of the standards, audits  
Relationship to GCP inspection  
Nature of the certification process

Questions...

## The Standards

Scope, Form, and Types  
Recurrent themes – Validation, DB development, Sub-contracting  
Reviews  
? Data standards (CDISC etc.)

Questions...

## Who am I?

- Now a part-time consultant for ECRIN
- I've worked in IT / DM in clinical trials since 2002
- Worked with or for ECRIN since 2009
- Was involved in the initial construction of the ECRIN standards and system, led by Christian Ohmann from Düsseldorf, but involving many others
- Was secretary to the Certification Board, 2011 -2018
- Carried out 29 audits, re-audits and reviews, in 17 centres
- Chaired the reviews of the standards in 2012, 2015 and 2017-18

## Origins and Rationale

Kuchinke et al. *Trials* 2010, **11**:79  
<http://www.trialsjournal.com/content/11/1/79>



RESEARCH

Open Access

### Heterogeneity prevails: the state of clinical trial data management in Europe - results of a survey of ECRIN centres

Wolfgang Kuchinke<sup>1\*</sup>, Christian Ohmann<sup>1†</sup>, Qin Yang<sup>1</sup>, Nader Salas<sup>2</sup>, Jens Lauritsen<sup>3</sup>, Francois Gueyffier<sup>4</sup>, Alan Leizorovicz<sup>5</sup>, Carmen Schade-Brittinger<sup>6</sup>, Michael Wittenberg<sup>6</sup>, Zoltán Voko<sup>7</sup>, Siobhan Gaynor<sup>8</sup>, Margaret Cooney<sup>8</sup>, Peter Doran<sup>9</sup>, Aldo Maggioni<sup>10</sup>, Andrea Lorimer<sup>10</sup>, Ferràn Torres<sup>11</sup>, Gladys McPherson<sup>12</sup>, Jim Charwill<sup>13</sup>, Mats Hellström<sup>14</sup>, Stéphane Lejeune<sup>15</sup>

*Could we define ‘standards of good practice’, at a very practical, pragmatic level, to help reduce the heterogeneity and bring everyone up to the standards of the best?*

12-15 years ago...

Heterogeneity...  
of systems,  
of practice

Little guidance  
from GCP

Some material,  
e.g SCDM, but not  
public

Perceptions of a  
2-tier system?

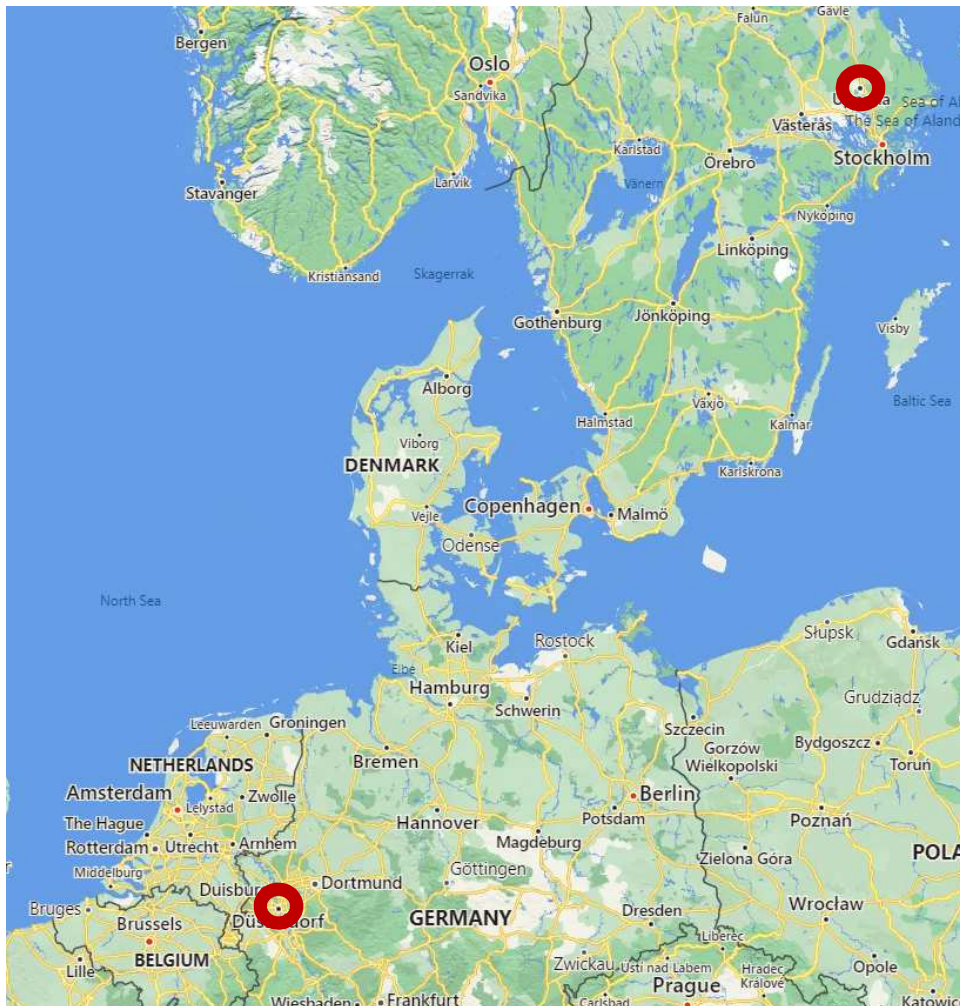
## The initial intentions, for standards and certification...

- To provide standards that represented practical suggestions for good practice, not just statements of principle.
- To use audits against those standards to identify and 'badge' high quality units in Europe
- To try and develop a network of high quality units, to be used for ECRIN related work (but how many would be needed?)
- To take the guesswork out of any audit process, by making the standards freely available to anyone, basing the audit only on the standards.
- To encourage debate and help develop expertise around IT and DM management, and to act as a general resource on this topic.

## But audits are *not* a GCP inspection (or even part of one)...

- ECRIN has no formal power
- Scope is limited to IT and DM (but detailed within that scope)
- Regulatory authorities would never give up their rights to assess all aspects of a unit, including IT and DM
- We hope, therefore, that ECRIN certification audits are challenging but less intimidating – more of a free consultation!
- Not designed to be a preparation or practice for a GCP inspection – though it can certainly help.
- Emphasis is on how the unit can help itself to obtain benefits in day-to-day activity, and assure its own management that things are as they should be – not on a one off inspection by external people.

## Initial pilots and revisions



Initial pilots in Uppsala  
and Dusseldorf, late 2011

Far too many  
standards!

Rapid initial  
revision in 2012 –  
from 240 to 140

Pilots completed  
late 2012

Gap of 2 years while  
the legal status of  
ECRIN established

## Certification gets underway...in Europe



2014-15: Milano, Coimbra,  
Bordeaux, Roma, Freiburg

2016-17: Lyon, Marburg,  
Mainz

2018-19: Dresden, Oslo,  
Roma(II), Leipzig, Heidelberg

2020: Köln, Basel

In process: Paris, Nantes,  
Rennes, Madrid, Barcelona

To come: Galway, Milano (II)

■ Certified (15)

■ 'In the process' (5)

□ To be audited (2)



## While elsewhere...



Kobe (2018) and Nagoya  
(2020)

Seoul (2020)

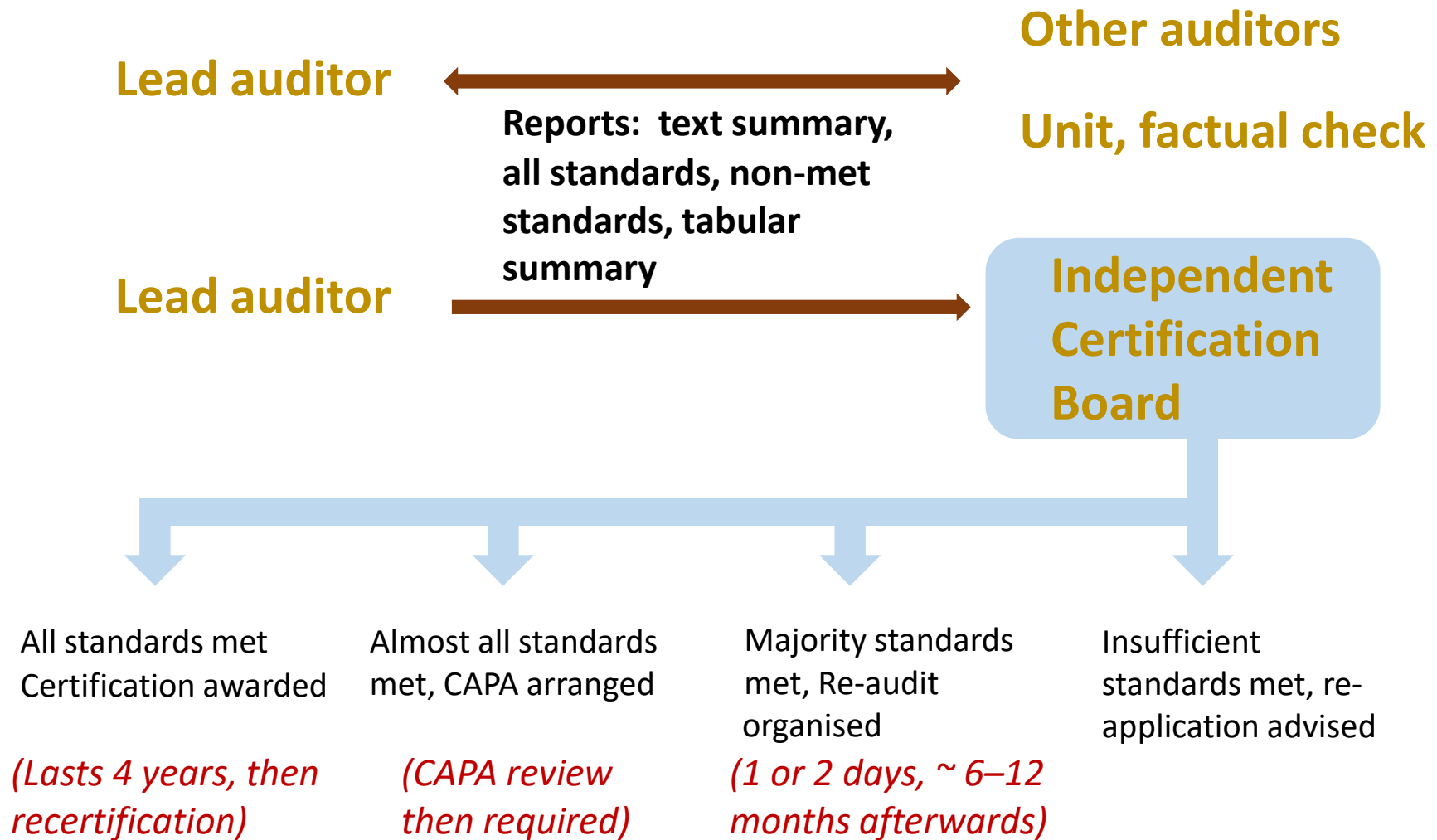
In discussion -  
Maputo

Longer term  
future outside of  
Europe?  
To be resolved

## Nature of an (initial) audit

- The audit team - a team of a lead auditor and 2 co-auditors, with at least one native speaker, though discussions are in English. Co-auditors help develop discussion, keep notes of evidence documents, review and reference, lead some sections.
- Auditors are experienced senior staff in their own units, approved by the Board. Ideally – one DM, one IT, one QA. (About 17 currently available).
- An initial audit normally takes two and a half days. Splitting the audit team is unusual but can be done if time is short.
- Process goes through the “checklist” of 106 standards (reduced each review). For each, auditors decide if ‘Met’, ‘Almost Met’, ‘Not Met’
- An audit report created on that basis (using a standalone MS Access system to record results and generate detailed reports).

## Nature of the certification process



## The outcomes of certification

- 15 units in Europe and 3 in east Asia certified, excluding 2 in the pilot, 5 are still 'in progress', but the process for any individual unit can take a year (sometimes more) between initial audit and certification.
- Only 4 units have been awarded certification immediately (Bordeaux, Freiburg, Mainz, and Kobe). Certification is possible but challenging – as we think it should be! Only 1 unit has been asked to re-apply at a later date – normally reviews or re-audits are requested.
- The idea of an 'ECRIN network' of high quality units has **not** really worked – sponsors and investigators generally use their 'own' units, and in any case numbers have taken a long time to build to a sufficient size for such a network.
- Audit experience is extremely important for the periodic review and continued evolution of the standards.

## The impact of certification

- Remains part of a general attempt to raise standards and quality in data management... in Europe and beyond. Feedback relating to that and the audits has been mostly very positive.
- Offers an opportunity for national networks to manage / monitor and upgrade IT and DM management. In practice national networks have been the main factor in deciding when and how many units are put forward for certification.
- The impact on auditors should not be under-estimated. The audits allow auditors to discuss issues at length with those in similar roles, and compare practice, as well as making them very familiar with the standards. Ideas and practice can be fed back into their own units and networks.
- Direct impact on the unit's income is low – it is a quality assurance mechanism rather than an immediate marketing boost.

## The future of data centre certification

- On-site audits and re-audits have been seriously impacted by the COVID pandemic, and now by a lack of staff. The momentum of certification has, unfortunately, suffered.
- Recent audits have shown the importance of prior self-assessment against the standards. Self assessment can also reduce the time and costs of certification and so is likely to increase in the future. Any assessment will still need, however, to be evidence based.
- A risk-based re-certification process was introduced but has not yet been taken up by all units who are due re-certification. The advantages of long term certification status are not clear (personal opinion!).
- The main future of certification and audits (as opposed to the standards) will probably remain as a quality assurance / improvement mechanism, available to national networks. This may be of particular use in the future in Eastern Europe, as well as outside Europe.

Any questions or comments?

Before moving on to the standards...

Any questions about the certification process?

## 106 mandatory standards, in 16 lists

### General Standards (4)

GE01 Centre Staff training and support (4)

### IT Standards (41)

IT01 Management of IT infrastructure (9)

IT02 Logical Security (7)

IT03 Logical Access (7)

IT04 Business Continuity (6)

IT05 General System Validation (9)

IT06 Local Software Development (3)

### Data Management Standards (61)

DM01 Data Management Planning (1)

DM02 CDMA's - Design, Development and Validation (8)

DM03 CDMA's - Change management (7)

DM04 Site Management, Training & Support (9)

DM05 Data Entry and Processing (7)

DM06 Managing Data Quality (12)

DM07 Managing Data Transfers (5)

DM08 Delivery and Coding of Data for Analysis (8)

DM09: Long Term Data Storage (4)

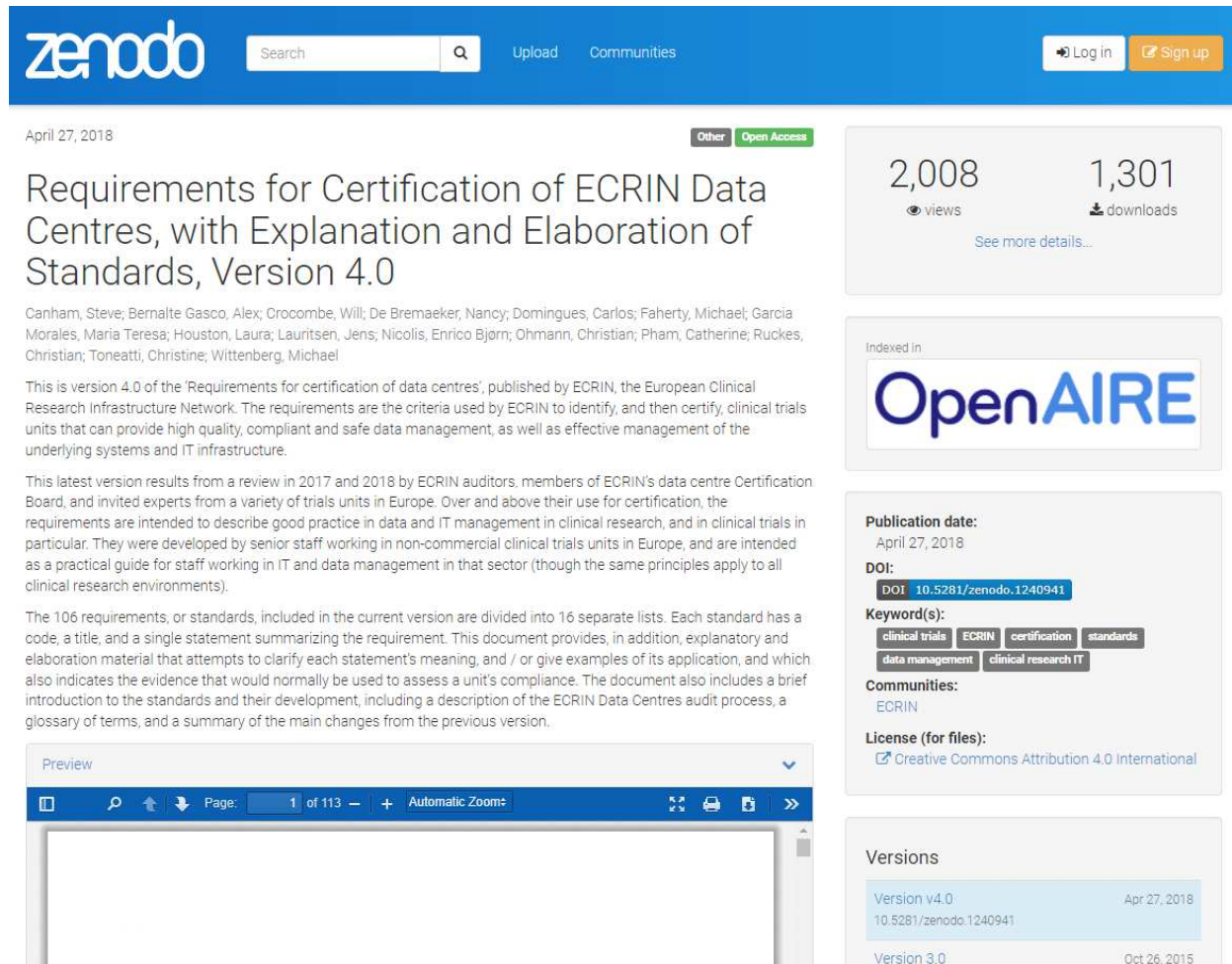
### Optional Standards (9)

ST01: Treatment Allocation standards (9)



## Standards available at ...

<https://www.zenodo.org/record/1240941>



**zenodo** Search [ ] Upload Communities Log in Sign up

April 27, 2018 Other Open Access

### Requirements for Certification of ECRIN Data Centres, with Explanation and Elaboration of Standards, Version 4.0

Canham, Steve; Bernalte Gasco, Alex; Crocombe, Will; De Bremaeker, Nancy; Domingues, Carlos; Faherty, Michael; Garcia Morales, Maria Teresa; Houston, Laura; Lauritsen, Jens; Nicolis, Enrico Bjorn; Ohmann, Christian; Pham, Catherine; Ruckes, Christian; Toneatti, Christine; Wittenberg, Michael

This is version 4.0 of the 'Requirements for certification of data centres', published by ECRIN, the European Clinical Research Infrastructure Network. The requirements are the criteria used by ECRIN to identify, and then certify, clinical trials units that can provide high quality, compliant and safe data management, as well as effective management of the underlying systems and IT infrastructure.

This latest version results from a review in 2017 and 2018 by ECRIN auditors, members of ECRIN's data centre Certification Board, and invited experts from a variety of trials units in Europe. Over and above their use for certification, the requirements are intended to describe good practice in data and IT management in clinical research, and in clinical trials in particular. They were developed by senior staff working in non-commercial clinical trials units in Europe, and are intended as a practical guide for staff working in IT and data management in that sector (though the same principles apply to all clinical research environments).

The 106 requirements, or standards, included in the current version are divided into 16 separate lists. Each standard has a code, a title, and a single statement summarizing the requirement. This document provides, in addition, explanatory and elaboration material that attempts to clarify each statement's meaning, and / or give examples of its application, and which also indicates the evidence that would normally be used to assess a unit's compliance. The document also includes a brief introduction to the standards and their development, including a description of the ECRIN Data Centres audit process, a glossary of terms, and a summary of the main changes from the previous version.

2,008 views 1,301 downloads [See more details...](#)

Indexed in **OpenAIRE**

**Publication date:** April 27, 2018  
**DOI:** DOI 10.5281/zenodo.1240941  
**Keyword(s):** clinical trials, ECRIN, certification, standards, data management, clinical research IT  
**Communities:** ECRIN  
**License (for files):** Creative Commons Attribution 4.0 International

**Versions**

Version v4.0 10.5281/zenodo.1240941	Apr 27, 2018
Version 3.0	Oct 26, 2015

And also at ...

<https://ecrin.org/sites/default/files/Data%20centre%20certification/Standards%20v4%20201804.pdf>

Just over a 100 pages



## Each standard has...

### **DM03.03: Change and risk analysis**

A risk analysis is conducted and recorded when considering any change.

← A code & title  
← The standard 'statement'

The change management process must include an assessment of the potential impacts and risks associated with a proposed change. For relatively trivial changes (addition of additional categories to a code list for instance) these impacts may be small; for large changes, e.g. the addition of a new eCRF, they may be considerable.

Changes that would risk orphaning data already in the system (e.g. dropping questions or categories) or making existing data invalid (e.g. changing the type of a question) should not normally be allowed and the change request should be rejected.

Any change will impact the CDMA itself, but there may also be impacts 'downstream', for instance on the data extraction process or the scripts used during statistical analysis, or on system documentation and / or user training. A CDMA change may also imply a change to the protocol (see DM03.07).

It is important that all these aspects are taken into account. Some centres use a 'change checklist' approach to structure the assessment of risk and to help with its documentation.

Evidence that the standard had been met would be the inspection of the risk assessment documentation against a range of proposed CDMA changes.

← Some E & E (explanation and elaboration) material that usually includes a suggestion for evidence

## Some examples and issues ...

a) Relatively straightforward standards...

Coding (e.g. using MedDRA), an example of the need for controlled documents

b) Three areas that are quite often problematic...

- i. Validation
- ii. Sub-contracting
- iii. Study database development

## Coding I ... (Part of DM08: Delivery and Coding of Data for Analysis)

### **DM08.07: Policies for coding**

If data coding is carried out, controlled documents are in place detailing the procedures to be used.

In many data centres some data is coded using international standard systems, usually as an aid to reconciliation, classification and analysis of data. The best known example is MedDRA for adverse events (and in some case medical history) coding, but other coding systems include the WHO ICD system for mortality and morbidity data and the WHO Drug Dictionary sometimes used for concomitant medications.

Using such systems involves more than the simple application of codes to matching terms. Code allocation may be ambiguous, and the standards exist in different versions, so policies and procedures must be developed to support consistency in coding and to stipulate the versions to be used, or at least how decisions about versions should be reached.

Autocoding mechanisms generate much discussion. While they may make the coding process quicker many staff feel they can too easily blur the distinctions that often have to be made between coding in one trial and in another. For that reason some staff prefer to use autocoding only within one trial at a time, and others are suspicious of them in general. Clear policies should therefore also exist to govern the use of autocoding mechanisms, if any are used.

The relevant evidence would be the controlled documents themselves.

## Coding II ...

### **DM08.08: Coding training**

If data coding is carried out, it is carried out only by personnel trained on the relevant systems with access to authorised trial specific support material.

Because applying codes is not straightforward the staff that do it need to be properly trained to carry out that task.

In addition it is often necessary to supply such staff with support material, e.g. in MedDRA coding, a list of commonly linked symptoms that should be coded as a single entity, and a list of such symptom pairs that should be coded separately.

Common adverse events which can be classified in different ways (i.e. in MedDRA terms allocated to different system organ classes) may need to be listed against the classification that should be used — usually on a trial by trial basis.

The responsibility for authorising such support material would normally fall to the sponsor / investigator, but the centre needs to ensure that such material is prepared and that the staff know how to use it.

Evidence that this standard had been met would be:

- relevant training records for the staff involved;
- examples of authorised trial specific material to support coding.

## Validation I ...

### **IT05.01: Validation policies**

Controlled documents should be in place covering system validation approaches, responsibilities and processes.

### **IT05.02: Validation system inventory**

The centre should have an inventory of all the IT systems in scope for validation, the risks associated with each, and, in summary, the validation strategy for each.

### **IT05.03: Periodic review of validation**

The centre should have mechanisms in place for periodic reviews of the risks associated with systems, with possible subsequent revalidations.

### **IT05.04: Validation Detailed Evidence**

Detailed validation documents should exist for any particular system, detailing the validation carried out, including any test data and protocols, and the results obtained.

### **IT05.05: Validation Summaries**

A signed and dated summary of the results of each validation should exist.

### **IT05.06: Change Management Policies**

Controlled documents should be in place defining risk-based change management mechanisms.

### **IT05.07: Change and risk evaluation**

Changes in IT systems in scope for validation should be documented, and include a documented risk assessment as well as any necessary revalidation results.

### **IT05.08: Validation of extracted data and reports**

Extracted data, however formatted, and the underlying data extraction processes, should be assessed using a risk based approach to decide upon the level of validation needed to ensure accurate extraction.

### **IT05.09: Validation of data transformations**

Data transformation processes should be validated, using a risk based approach.

## Validation II ...

- Validation is for the benefit of users and the unit – not auditors or inspectors – assuring everyone that things work as they should. In an ECRIN audit all systems, including ‘non-GCP’ systems, should be considered for validation.
- Decisions about validation strategy are not just technical – they involve resources, sometimes substantial ones, and they therefore need to involve management. Not just an IT issue!
- There needs to be an overarching SOP – summarising the process, risk assessment strategy, deliverables, and referring to local personnel, expertise and allocating roles and responsibilities (**and not be yet another summary of GAMP!**)
- A ‘Master Validation Plan’ or ‘Validation System Inventory’ - a ‘living document’ (or spreadsheet, wiki or web page) should exist that summarises the validation strategy for each system, based on assessments of associated risks.
- The verification of individual systems should also be risk based – it is impossible to check everything. (But equally, not necessarily limited to supplied scripts).
- Put simply, we are looking for the application of ‘professional intelligence’ to the validation tasks.



## Validation III ...

- Looking for the detailed evidence that has supported validation decisions – which should be dated and attributable.
- Looking for a final sign off into production use. Does not necessarily need 100% functionality. Some problems can have ‘work-arounds’ and / or lead to requests to the system’s creators. Sign-off is another risk-based decision.
- Change management a key process, and with mature systems probably represents the bulk of system validation – again needs to involve risk-based and documented decisions about the strategy / level of validation to be employed.
- Feature creep and validation – especially for new reports and extractions. Formal validation not always required but needs to be considered.
- Periodic review and validation – context and staff changes need to be considered. Incorporate in the Master Validation Plan.
- Put all those elements together and there is a robust system validation regime in place!

## Sub-contracting I ...

Subcontracting of the IT infrastructure: sometimes as PaaS – to ‘central IT’, sometimes as SaaS  
Increasingly popular approach – make sense in many ways

**But**, it is becoming too easy for the units to abdicate their responsibilities.  
Not conforming to GCP...

GCP E6(R2) - Section 5.2.2

“The sponsor should **ensure oversight** of any trial-related duties and functions carried out on its behalf, including trial-related duties and functions that are subcontracted to another party by the sponsor’s contracted CRO(s).”

*(my emphasis)*

... more importantly, not maintaining the unit’s own quality management systems

We are not the only ones running into this problem.

The EMA has also identified a wide range of identified issues around oversight of subcontracted IT services

## Sub-contracting II ...

ECRIN approach summarised by:

“... Even if a centre is not carrying out the operational day-to-day tasks involved in an activity because they have sub-contracted it to some other organisation, or some other part of their own organisation, **they remain responsible for its proper operation and must provide evidence that:**

- The sub-contracting organisation is performing its operations to the standard required,
- ‘the standard required’ is based on a written and mutually understood definition of responsibilities, and
- the data centre has an oversight mechanism in place to ensure that the standard is being met.”

**N.B. The need to retain a level of IT expertise within the unit, or brought in as independent input - at least enough to have the conversation!**

## Sub-contracting III ...

An example...

### **IT04.03: Back up frequency**

Backups must be taken using a managed, documented and automatic regime that ensures new or changed data is backed up within 24 hours, and which allows the centre to check that the system is operating properly.

This standard on back up frequency reflects the fact that back up regimes are usually sophisticated enough to identify and only process data that actually needs backup because it has been changed or newly inserted.

If a centre is managing its own data backups it is relatively straightforward to monitor that the process is operating properly. If backups are the responsibility of an IT host organisation the centre still needs to assure itself (e.g. by receiving reports or periodic copies of the logs) that the backup process is operating properly. Ideally this would also be every 24 hours but it is accepted that this may not always be easy to arrange. In such cases the centre will need to take a risk based decision on what level of monitoring is acceptable, given their knowledge of the internal systems within the hosting organisation and the contractual agreements that are in place. External hosts that are unwilling to provide any form of monitoring data or access should be avoided.

... ..

The evidence that the standard has been met includes:

- documentation describing the backup regime and how it is managed, either from the data centre or the IT host organisation;
- logs of the backup process and / or periodic summary reports indicating the backups are proceeding as required.

## Study database development I

Perhaps surprising... But a lot of units have some very confused, or sub-optimal systems

Everyone starts with the protocol, then has some form of iterative multi-disciplinary process to develop a provisional system, which is tested, and then somebody decides it is OK for production use.

But there is huge variation in exactly how that process works, who is involved, and when testing and approvals take place.

The ECRIN standards have tried to clarify the process we expect to see (we even included a diagram!)

## Study database development II

Some 'Pain points'

- Rarely explicit documentation of how a protocol is translated into annotated CRFs or an initial version of the system, and who is involved.
- Not enough attention paid (at least explicitly) to ensuring data minimisation, i.e. not collecting too much data. The role of the statistician as the key data consumer often not clear.
- Links to the DMP often unclear – e.g. for any deviations from SOPs, e.g. in query management, coding systems, data standards, long term storage / re-use.
- 'User Acceptance Testing' often confused – the phrase should be banned.
  - Which users? – people use the term differently
  - End users neither 'accept' anything nor test systematically – they provide feedback
  - End user feedback feeds into the *design phase*, should be risk based (it might not be needed at all).
- Systems are tested while they are still changing - Validation needs a fixed target.
- Prototypes can often generate documentation but are not always fully used.
- Detailed validation planning needs intelligence and experience. Validation does not, only attention to detail plus supervision.

## Study database development III

### **DM02.01: CDMA development and validation policies**

Controlled documents covering the development of CDMA's and CRFs, including their validation, should be in place.

### **DM02.02 : The CDMA and the protocol**

Processes exist to ensure the CDMA specification fully supports the outcome measures and safety requirements in the protocol but does not ask for unnecessary data.

### **DM02.03 : Creating a full functional specification**

A CDMA design and full functional specification should exist identifying each data item on each CRF (including field names, types, units, data checking logic, conditional skipping, and derivation logic).

### **DM02.04 : Isolation of CDMA's in development**

CDMA's in development should be isolated from, and clearly differentiated from, the CDMA's used in production.

### **DM02.05 : Input into CDMA development by end users**

Procedures are in place to secure feedback from selected end-users, on the practicality and ease of use of the CDMA, and to decide when and how such feedback will be sought.

### **DM02.06 : Cross-disciplinary approval of the functional specification**

The CDMA's design and functional specifications are signed off and dated by signatories representing a cross-disciplinary team.

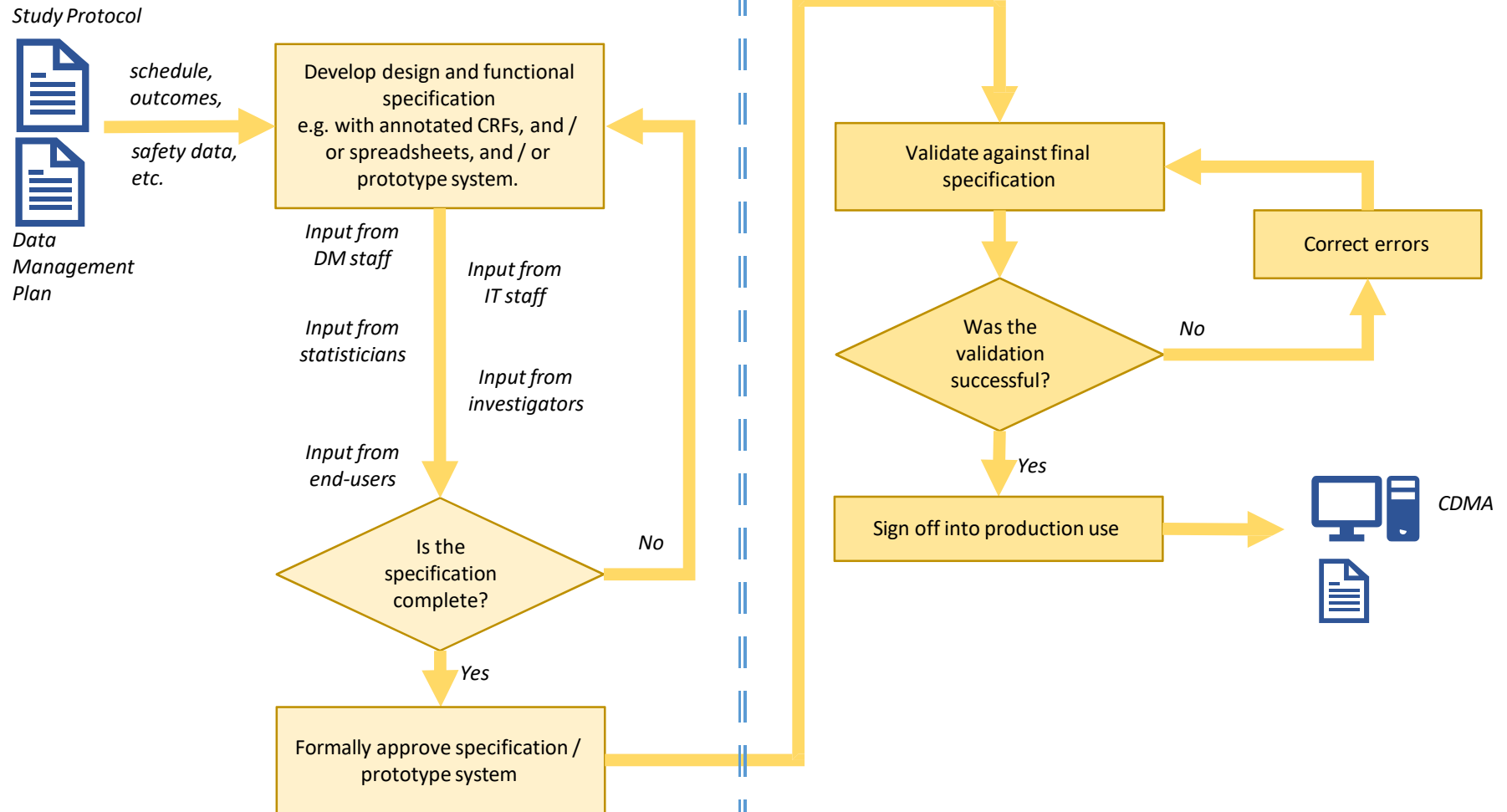
### **DM02.07 : CDMA validation against the functional specification**

Systematic, detailed testing is carried out against the functional specification for each CDMA before deployment to the production environment.

### **DM02.08 : CDMA final sign off into production**

Each CDMA should be formally approved, dated and signed by the relevant signatories, before production use.

## Study database development IV





## Need for further review and revision

- Standards were reviewed in 2012 (v2), 2015 (v3) and 2017-18 (v4).
- Next review overdue but the pandemic and other dislocations have postponed this.
- As always need to consider feedback from audits and auditors
- Need to consider very useful feedback received from BfArM.
- Need to consider changes in legislation
- Need to consider changes in practice, especially around re-use of data, de-identification etc.
- The hope is to start a new review this Autumn.

## The question of “data standards”

- One particular issue has been debated since the standards were first developed.
- The standards are almost entirely about the facilities, services and operational policies within trials units – they do not cover the organisation of the data itself.
- In particular the use of CDISC standards – especially CDASH – has never been a requirement.
- But should it be? Is this now a realistic expectation? (in the past it was thought to be unrealistic). Is it a necessary part of ‘high quality practice’?
- If so at what level? What would be ‘sufficient’ use of, or familiarity with, the CDISC standards?
- What do people think?

## Future of the standards

- People do seem to find them genuinely useful – we have had a lot of positive feedback about them – and they have been adapted in other contexts.
- As the standards have evolved they have gone from an initial long list of statements to a more focused set of recommendations, with much more supporting material.
- Should that trend continue – should we try and write a text book, (and then maintain it)?
- One problem is the lack of empirical evidence for many of the assertions made, in the ECRIN standards and similar recommendations – the standards tend to represent ‘distilled wisdom’ rather than ‘scientific fact’. Should we lobby for funds to improve that situation?
- Should we also develop more self-assessment material around the standards?
- Should we try to make them more global – they currently make assumptions based on the European context (which is highly variable, but Asian or African centres introduce new issues). Should we make them more ‘open’ within Europe – reaching out to non ECRIN members and other organisations.

Lots of questions and possibilities... but limited resources

Any questions or comments?

about the standards...

*Vielen Dank!*

[stevecanham@outlook.com](mailto:stevecanham@outlook.com)