GCP Audit

Mission of a Sponsor's Auditing Department

A quality management system is established to define quality policy and implement quality management. Quality Control (QC) and Quality Assurance (QA) are implemented in accordance with the quality policy. As part of implementing Quality Assurance, a sponsor's audit is generally performed to accomplish the following missions:

1. To evaluate compliance with the reference documents so as to ensure the reliability of trial data and protection of the subject's rights.
2. To evaluate the effectiveness of the clinical trial system and provide an opportunity for the sponsor to improve it.

It is expected that the results of an audit will be utilized by the auditee as essential information for the improvement of the clinical trial system or by the sponsor's chief executives as material for making a business judgment about the quality of clinical trials. To accomplish the

above objectives, the sponsor is expected to establish an independent auditing department and to ensure that the auditor(s) is(are) appropriately qualified by education and training.

Auditing Department

It is useful for the sponsor to establish an independent auditing department so as to ensure systematic and continuous conduct of audits. To ensure that a sponsor's auditing department functions effectively the sponsor should fulfil the conditions specified in paragraphs 4.1 to 4.4 below, specify the roles and responsibilities of the auditing department, and establish written SOPs for the performance of audits. It is possible for a sponsor to define the responsibilities of a department manager and assign the manager if necessary.

Independent Auditing Department

The auditing department should be independent of the auditees so as to ensure the credibility of its audits. Auditing is part of Quality Assurance and involves independent and objective evaluation of clinical trials. The auditing department fulfils part of the Quality Assurance responsibilities of the sponsor.

Qualified Auditors

The sponsor should establish an auditing department with qualified auditors so as to ensure the proper conduct of audits as part of implementing Quality Assurance. Each auditor's qualification should be documented to verify that he/she is a suitable person

to properly conduct audits, e.g., records of education/training and business experience.

Qualifications of Auditors

The sponsor should specify the qualifications of auditors in auditing procedures and should only appoint appropriate individual(s) as auditor(s) based on consideration of his/her education/training, business experience, and ability. For example:

Knowledge: Necessary laws and regulations, GCP, relevant guidelines, the Declaration of Helsinki, clinical and pharmaceutical knowledge, SOPs, computerized system validation, etc. *Skills:* Communication, writing, language, etc.
Nature: Tenacity, power of observation, analytical capability, decision, sense of ethics, maturity, etc.

Responsibilities of Auditors

The sponsor should specify the roles and responsibilities of the auditor before starting to conduct an audit so as to ensure fair and smooth performance of the audit. The auditor is responsible for maintaining the confidentiality of information obtained during an audit, planning (designing and updating) and conducting the audit, and reporting the audit results.

5 Planning of Audits

Before conducting an audit, the auditor (including the auditing department manager) should establish a written audit plan (such as an annual plan, a monthly plan, and a plan specific to each trial or audit) based on the results of the risk assessment according to the written auditing procedures.

5.1 Establishing the Goals of Audits

One or more objectives are generally established for a trial audit based on the importance of the trial with regard to submissions to regulatory authorities, the type and complexity of the trial, the level of risk to the trial, and any problem(s) identified previous. The most important part of audit planning is to specify the goal(s) of the audit. By establishing the goal(s) of an audit, the subjects and methods of the audit will be determined and the consistent conduct of the audit will be ensured. One or more objectives may be chosen from the following examples:

- Evaluation of the compliance of any organization involved in a clinical trial (pre-qualification).
- Evaluation of the compliance with regulatory requirements and human subject protection.
- Confirmation of the appropriate conduct of a trial, the credibility of data obtained, and the condition of record keeping at a participating medical institution(s) through direct access.
- Confirmation of the conduct of monitoring.
- Confirmation of the credibility of a clinical trial/study report.

- Early detection and correction and prevention of any existing problems or potential problems with a system and/or process.
- Early detection and correction and prevention of any existing problems or potential problems occurring at an institution entrusted with trial-related duties.

Designing and Updating the Audit Plan

Planning is essential to systematically, effectively, and efficiently conduct an audit with consideration of resource management in the auditing department. Audit plans, such as an annual plan, a monthly plan, and a plan specific to each trial or audit, should be established based on consideration of the goal(s), contents (e.g.subjects and methods), and timing of an audit, the progress of the targeted trial, and other relevant factors. The audit plan should be

updated in accordance with progress of the trial or auditing activity. Prior to conducting an audit, the auditors and the auditee will discuss and adapt the audit plan, as necessary.

Determining the Subject[s], Timing, and Method[s] of an Audit

The subject(s) (e.g., a medical institution, CRO, system, clinical trial/study report, computerized system validation, and database), timing (e.g., before the start of the trial, during the trial, after the completion of the trial, or periodically), and the method(s) (e.g., sampling, interview, or tour) of an audit should be determined based on the goal(s) established for the audit.

Information in the Audit Plan

An audit plan should provide the following information, although the contents may vary depending on the type of the plan (e.g., annual plan, monthly plan, or plan for a specific trial or audit).

- The goal(s) of the audit.
- The subject(s) of the audit.
- The scope of the audit.
- The timing of the audit.
- The name(s), title and address of the auditor (s) (and the auditing department manager).
- The reference documents required.
- The person(s) to whom the audit report will be submitted.
- Timelines for the audit(s) and report(s) (if possible）

Conduct of an Audit

Auditing is performed by the auditor in accordance with a written audit plan and procedures, and involves the examination and evaluation of information obtained through investigation of the audit trail (e.g. essential documents and SOPs) and a trial site(s) (e.g. facilities and equipment), as well as interviews with the auditee, etc. It is important to specify reference documents that auditees comply with before performing an audit so as to ensure fair conduct of audit. The auditor evaluates conformity and compliance with these reference documents. The auditor should inform the sponsor

about the conduct of an audit in advance.

Explaining the Auditing Procedures

To efficiently collect accurate information through auditing, the auditor should give the auditee a prior explanation about the conduct of an audit (e.g. the goal(s) and method(s) of the audit).

When providing an explanation for the auditee, the auditor should confirm the subject(s) (i.e. materials and facilities that will be audited), the schedule, and the contact person(s) for the audit so that both the parties obtain the necessary and full understanding about the audit.

Conducting an Audit and Collecting Information

There are two types of sponsor's audit, i.e., auditing of internal trial-related department(s) and auditing of external establishment(s) involved in the trial concerned, e.g., a medical institution, laboratory, and/or CRO. To ensure the smooth conduct of an audit of an external institution, such as a participating medical institution, laboratory, or CRO, it is important to properly perform a preliminary internal audit.

When conducting an audit, the auditor should collect audit observations by reviewing the documents subject to the audit and interviewing the auditee etc. Based on audit observations collected, the auditor should confirm and document whether or not the audit observations are compliant to GCP, all applicable regulatory requirement(s), SOPs, the study protocol, and any other relevant documents and procedures.

Utilization of an audit checklist and a sampling method is useful for the standardization and efficient conduct of auditing activities.

Confirmation and Evaluation of Audit Observations

The auditor should discuss audit observations with the auditee so that the absence of errors can be confirmed. The auditor should then review the confirmed audit observations and further information can be collected if required.

The auditor should examine (within the auditing department) whether the audit observations involve any violations of GCP or applicable regulatory requirements, deviations from the relevant protocol and sponsor's SOPs, or problems with respect to the reliability of clinical data and then should determine the observations to be reported as audit findings. The auditor should also examine whether any of the obtained audit observations could have an influence on other trials, medical institutions, clinical trial/study systems, etc. When audit findings are reported, they may be graded according to the level of importance.

Reporting the Results of an Audit

The auditor should provide written audit results (i.e. an audit report) for the sponsor to make the auditee recognize audit findings and take the opportunity to make improvements. It will be useful to provide an opportunity for the auditor to give an explanation about audit results to the sponsor at the time of submitting the audit report.

To preserve the independence of auditing, the auditor must not be directly involved in the corrective and preventive action (CAPA) process.

7.1 Preparation of an Audit Report

The auditor should prepare an audit report based on the results of the evaluation. When an auditing department manager has been appointed, the audit report should be prepared by the auditor and if necessary reviewed or approved by the manager.

The contents of an audit report will be as follows:

- Information that identifies the trial, such as the chemical name or identification code of the investigational drug, the trial title, and the protocol number.
- The person to whom the audit report will be submitted.
- The date of issuing the audit report.
- The subject of the audit.
- The site of the audit.
- The scope of the audit.
- The name(s), title and address of the auditor(s) (and the auditing department manager).
- The name and address of the auditee.
- The date/period of the audit.
- The results of the audit, including audit findings (grading of the findings may be included).
- A list of all persons receiving a copy of the audit report.

The following information may be contained in an audit report depending on the objective(s) of the audit:

- Suggestions for improvement and advice for CAPA.
- Responses to the audit findings.
- The results of the auditor's confirmation of the auditee's response.

7.2 Persons to whom Audit Reports are submitted

The auditor should submit an audit report to the sponsor. The auditor may give a copy of the audit report to the sponsor's auditee. In such a case, the auditor should pay special attention to ensuring the confidentiality of the contents of the report and should handle the report with due caution. Concerning audit reports, ICH GCP 5.19.3 (d) states the following:

'To preserve the independence and value of the audit function, the regulatory authority(ies) should not routinely request the audit reports. Regulatory authority(ies) may seek access to an audit report on a case-by-case basis when evidence of serious GCP non-compliance exists, or in the course of legal proceedings.'

8 Corrective and Preventive Actions

Implementation of a CAPA plan after the conduct of an audit is necessary to eliminate present and potential causes of non-conformity and prevent re-occurrence or future occurrence. Once the conduct of the audit is complete the auditor should be provided a CAPA plan to the auditee that will be utilized to remediate issues of non-compliance and

potential non-
compliance identified during the audit process. The CAPA plan should, at minimum, require the auditee to identify the root-cause of audit findings and describe whether corrective and/or preventive actions will be necessary to address the audit findings.

9 Completion of an Audit

Upon receipt of the preliminary responses to the CAPA from the auditee, the audit is completed. Follow-up should be performed depending on the significance of the audit findings. CAPA follow-up and subsequent effectiveness verification should be ensured by continued interaction between the auditor and auditee until mutual agreement has been met that the CAPA have been addressed.

10 Audit Certificate

The auditor (including the auditing department manager) should prepare an audit certificate at the request of the sponsor. The sponsor should attach the audit certificate to a clinical trial/study report of the targeted trial.

The audit certificate should contain the following information:

- Information that identifies the trial, such as the chemical name or identification code of the investigational drug, the trial title, and the protocol number.
- The date of issuing the audit certificate.
- The contents of the audit (e.g., subjects and date of the audit, and date of issuing the audit report).
- The name(s), title and address of the auditor (s)(and the auditing department manager).
- The name and workplace address of the auditee.

11 Keeping Audit Records

Audit records should be kept according to sponsor’s SOPs for record keeping. The SOPs should specify the procedures for keeping or destroying audit-related records, as well as the place, subject, and duration of record keeping.

Appendix 01
Risk-Based Approach for Audit Planning

1.0 Introduction/Background

An effective audit function considers risk factors to design an audit programme that is objective, independent of the operational activities and focused on areas where it is likely to have most impact. The impact can be defined in terms of the needs of multiple stakeholders. Any risk-based approach to audit planning should be consistent with the objectives of the overall audit programme, as agreed with audit clients and the audit department's senior management. Risk factors should be pre-defined and be based on multiple sources of information. However, it is important to allow scope for *ad hoc* audit selections based on emerging issues which nevertheless should be identified and recorded for later reference.

Aside from those main goals, targeting audit resource according to risk recognises that it is impossible to audit every aspect of every activity. The need to be independent and to audit by sampling makes the audit department distinct from a quality control function. It also addresses the reality that auditor resources are finite and must be used with the greatest return on investment. Moreover, it acknowledges that assurance of quality can only be provided on systems and processes in which it is built in at the operational level.

2.0 Scope

This guidance sets out a systematic approach towards interpreting the level and nature of risks in audit planning; using a common formula based on severity and likelihood of risks that impact on patient/subject wellbeing and the integrity of clinical trial data.

Many alternatives and possibilities to extend these ideas exist which achieve the same ultimate goals.

3.0 Definitions

The following terms can be used to ensure risk management is understood and interpreted consistently across QA groups and other functions involved. Examples are given to show how the concepts can be used in practice:

- Risk Assessment
- Risk Management
- Hazard
- Severity
- Likelihood
- Risk Weighting

Appendix 01
Risk-Based Approach for Audit Planning

- Risk Assessment – A systematic process of organising information to support a risk decision to be made within a risk management process. It consists of the identification of hazards and the analysis and evaluation of risks associated with exposure to those hazards.
- Risk Management – The systematic application of quality management policies, procedures, and practices to the tasks of assessing, controlling communicating and reviewing risk.
  Risk Management can be seen as:
  - Awareness of all processes/activities per study and understanding where risks are likely to occur based on that study/clinical project
  - Having a clear rationale in determining QA assessments and decisions
  - Prioritising and focusing on aspects that are deemed high risk (defined by risk drivers) to ensure resources are tailored to confirm credibility of all research activities
  - Improving processes and knowing the limitations of sampling activities according to risk
  - Taking a pragmatic and rational approach, "What is the impact on the patient?", "What is the impact on the integrity of the data?"
- Hazard - The potential source of harm. The Hazard is a list of common aspects associated with Clinical Trials. The focus of this list will be determined by the type of clinical activities and will need constant review.
- Severity – A measure of the possible consequences of a hazard

Severity	**High (Red)**	**Moderate (Amber)**	**Low (Green)**
Definition	Risk has severe potential harm to patients (volunteers) and/or integrity of data	Risk has potential for serious impact if not managed appropriately on patient safety and/or integrity of data	Risk has little or no potential impact on patient safety and/or integrity of data

- Likelihood - Probability that harm will be caused by the identified hazard. The probability of harm should be assessed to determine the likelihood of the risk. This will be rated High (H), Moderate (M) or Low (L) within each hazard. This positions the level of risk for each category to produce a risk weighting.
- Risk Weighting - A risk weighting is assigned to each hazard. Where a significant number of hazards are deemed High Risk and are of a severity and likelihood to produce a high risk rating, this will require QA to prioritise its activities and a higher sampling rate may be applied based on the hazards identified.

Figure 1 shows an example of how risk scoring can be applied.

Appendix 01
Risk-Based Approach for Audit Planning

4.0 Content

4.1 Defining Risk Criteria for Prioritisation of Audit Selections

Risk criteria used should be collected and applied consistently and may be based on information already available in the organisation, derived by the audit function itself or both. Wherever possible, objective data should be used but it may be necessary to include subjective judgments as part of the overall assessment.

4.1.1 Stakeholders

In terms of assurance of quality and compliance, the requirements of the following key stakeholders may be considered:

- Clinical study subjects
- Regulatory Authorities and their regulations & guidelines
- Senior management of the audit department

Senior management of the sponsor organisation (auditee management)

4.1.2 Clinical Programme, Study or Investigator Site Prioritisation

Sampling is a tool which must be applied logically if it is to provide independent assurance that processes are fit for purpose. This is an important part of Prioritisation. According to section 5.19.3 of ICH GCP, the audit plan and procedures for a trial audit should be guided by the 'importance of the trial to submissions to regulatory authorities, the number of subjects in the trial, the type and complexity of the trial, the level of risks to the trial subjects, and any identified problem(s).' The ISO10011 standard (Part 1) also provides a useful framework for auditing GCP quality systems and studies. Another standard available to help identify sampling criteria is ISO2859-1.

Figure 2 shows examples of factors that might be used to prioritise and select audit targets at the programme, study and investigator site level. Collectively, they allow for differentiation in risk as perceived by stakeholders affected by the conduct of the study or use of the data to influence decisions about future use of a product or other intervention. A risk-based programme may use some or all of these (and more) depending on the degree of differentiation desired.

4.1.3 System/Process Prioritisation

The planning, conduct and reporting of clinical studies comprises many distinct but related systems and processes. An audit function may

---

conduct audits cyclically on specific systems or processes with a regular frequency. However, certain systems/processes involve inherently more risk than others so more frequent or complex audits are warranted. Risk factors can include

- The importance of the system/process to:
  - subject safety or rights (inc. safety data reporting)
  - data integrity
  - study conduct
  - compliance with GCP and regulations (inc. emerging issues focused on by regulatory authorities)
- Degree of process control (e.g. detailed procedures and controlled documents, level of quality control applied by operational group, QC/metrics data, training)
- Compliance history (e.g. previous audit or inspection findings)
- Process stability (e.g. new or updated processes)
- Time since previous audit

4.2 Documenting & Review of Risk-Based Audit Programmes

It is recommended to record the basis on which a risk-based audit programme is designed, i.e. the risk factors used and results of prioritisation for that time period. This allows for decisions to be revisited periodically and revised in a consistent way as processes and studies change. A record of programme assumptions that reflect the risks in study conduct demonstrates an effective and objective audit approach.

Appendix 01
Risk-Based Approach for Audit Planning

Figure 1: Extended Example of Risk Application

What are the potential hazards inherent in a clinical study? What is the potential severity?
What is the likelihood?
What risk strategy or mitigating action should be put in place to reduce the (1) likelihood of the hazard occurring and (2) possible adverse severity?

For each risk area

- Define a rating Category of Low, Moderate or High & position within that rating based on the category selected (see table 1).
- Refine within the category the likelihood of risk of Low, Moderate of High and position a weighting based on the category selected (see table 2).
- Risk Weighting is calculated by multiplying Severity by Likelihood per hazard
- An overall rating can then be applied to all hazards (see table 2)

Table 1: Risk Key

Severity		Likelihood		Risk weighting
Low	Enter Value	Low	Enter Value	= Severity x Likelihood
Mod	Enter Value	Mod	Enter Value	
High	Enter Value	High	Enter Value	

Example:

Step 1 Assign a Severity indicating the criticality of each activity. This is represented by a range of risk for each category, e.g. Severity Low, Moderate or High.
Assign the appropriate number associated with the end result e.g. Low

Step 2 Assign the Likelihood of the event (e.g. non-compliance) happening. This probability of risk is represented by a range of risk within each category
e.g. Likelihood Low, Moderate or High.
Assign the appropriate number associated with the end result e.g. Moderate

Step 3 Calculate the risk weighting per hazard by multiplying the Severity by the Likelihood

Appendix 01
Risk-Based Approach for Audit Planning

A study could be seen as comprising multiple hazards and each can be represented in a summary matrix from which an overall risk weighting can be derived.

Table 2: Identification of Hazards/Risk Areas (will vary dependent upon the Research activity)

Hazard/Risk Area (e.g.)	Severity H	Likelihood			Severity M	Likelihood			Severity L	Likelihood			Risk Weighting
		H	M	L		H	M	L		H	M	L	
Product Characteristics									X		x		Low
Therapeutic Area					X		x						Moderate
Study Population									X			x	Low
Overall Weighting													**Low**

.

Appendix 01
Risk-Based Approach for Audit Planning

Figure 2: Example of Clinical Programme, Study or Investigator Site Prioritisation

Example risk factors for study/programme selection	Example risk factors for site selection
– Study population (e.g. size, vulnerable subjects, new indications) – Product characteristics (e.g. products that are new or have specific risks) – Therapeutic area – Duration of study – Applicability of regulations (e.g. interventional *vs.* non-interventional studies) – Sponsor obligations (e.g. commercially sponsored *vs.* investigator-initiated study) – Importance of study to future marketing submission (e.g. study phase, pivotal or supporting study) – Level of experience of sponsor clinical team – Confidence in service providers – Number and nature of outsourcing activities and associated interfaces for responsibility – Level of complexity of study and training requirements (e.g. e-system usage/medical device requirements) – Regional distribution of sites	– Number of subjects per site – Number of protocol violations – Number of (S)AEs – Known compliance issues – Other aspects relevant to primary study objectives – Efficacy results from site – Number of subject discontinuations – Geographic location – Level of experience of investigator and/or site – Level and nature of monitoring / monitoring staff turnover – Multiple vendor oversight across sites – Use of SMO (alone or in combination with vendor-selected sites)

.

5.0 References

EMA/INS/GMP/79766/2011 Quality Risk Management (ICH Q9)

ICH Topic E6 (R1) Guidance for Good Clinical Practice - Note for Guidance on Good Clinical Practice

6.0 Recommended Reading

Department of Health Toolkit (UK)
http://www.ct-toolkit.ac.uk/

Ensuring trial validity by Quality Assurance and Diversifying Monitoring Methods – Clinical Trials 2008 http://rds.epi-ucsf.org/ticr/syllabus/courses/26/2009/02/10/Other/readings/Biagent_08.pdf

ECRIN - Risk-Adapted Monitoring in Clinical Trials
http://www.ecrin.org/fileadmin/user_upload/public_documents/News/Activities/ECRIN_proposal_monitoring_final_28012013-1.pdf

EMA Inspectors' Working Group - Reflection paper on risk based quality management in clinical trials
http://www.ema.europa.eu/docs/en_GB/document_library/Scientific_guideline/2013/11/WC500155491.pdf

Institute of Risk Management – Risk Management Standard
http://www.theirm.org/media/886059/ARMS_2002_IRM.pdf

ISO/IEC Guide 73 Risk Management - Vocabulary - Guidelines for use in standards
http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=44651

ISO2859-1 - Sampling procedures for inspection by attributes
https://www.iso.org/obp/ui/#iso:std:iso:2859:-1:ed-2:v1:en

MRC/DH Trial Management and Monitoring – Clinical Trial Risk Assessment http://www.ct-toolkit.ac.uk/routemap/risk-assessment

Risk-adapted Approaches to the Management of Clinical Trials of Investigational Medicinal Products - MRC/DH/MHRA Joint Project http://www.mhra.gov.uk/home/groups/l-ctu/documents/websiteresources/con111784.pdf

.

Appendix 02
Corrective and Preventive Action

4.0 Content

4.1 Escalation of Audit Findings

An integral part of an organization's Quality Assurance/Compliance process should include a means of identifying and escalating significant issues of noncompliance that impact subject safety and/or data integrity. At minimum this process should define procedures which support the identification of GCP driven audit findings; assignment of criticality, and escalation of significant issues through an organization's line management.

Organizations should align their audit finding escalation process with a CAPA process as a means of ensuring that audit findings are documented, tracked and effectively resolved.

4.2 Introduction, Auditor and Auditee Interactions

A CAPA procedure is an essential part of a quality audit process. A CAPA process provides the auditor and auditee with a structured method for the investigation, follow-up, and resolution of issues of non-compliance identified during the audit process. The CAPA process also serves to provide supporting evidence (i.e., documentation) of audit finding closure and the subsequent closure of the audit cycle.

The most effective CAPA process is fielded through interactions between an organization's Quality Assurance/Compliance unit and the auditee, which allows the auditee to define their CAPA; this ensures objectivity is retained within the audit process. Interaction with the auditing organization's auditor and/or Quality Assurance/Compliance unit should consist of guidance and support through discussion with the auditee (especially for auditees that are unfamiliar with a CAPA process). The auditing organization should refrain from providing recommendations (i.e., defining the auditees CAPA) as this introduces bias into the audit process.

In summary, as auditees are most familiar with their processes and procedures, they are the most qualified individuals to field CAPA responses. The Quality Assurance/Compliance unit and quality audit teams may provide guidance, consultation and feedback to the auditee but the CAPA process must *not* be directed or mandated solely from the auditor or quality audit team's perspective.

4.3 Initiation of a CAPA Process

The CAPA process is initiated upon the auditee's receipt of the audit findings from the auditor or auditor's organization. The auditee then begins initiation of the CAPA process by application of the following actions:

- Auditee identification of root cause by performing root cause analysis (RCA) for each finding
- Auditee defines corrective and/or preventive actions based upon root cause
- Auditee defines timing of anticipated CAPA closure(s)
- Auditor and auditee interactions supporting CAPA acceptance, effectiveness verification and CAPA closure. *(Refer to Figure 1 and the Corrective and Preventive Action Plan Table).*

4.4 Root Cause and Root Cause Analysis

Root cause analysis (RCA) is required to identify the basic cause (s) of any undesirable condition within a quality system. There are several techniques which may be utilized to assist an auditee in identifying root cause; two common and effective methods are:

- Five (5) Whys Technique
- Fishbone Analysis (Ishikawa Diagram) or Cause and Effect Analysis

4.4.1 **5 Whys** - The *5 Whys* is a question-asking method used to explore the cause/effect relationships underlying a particular problem. This method is effective in evaluating root cause relating to a single or less complex issue. Ultimately, the goal of applying the *5 Whys* method is to determine a root cause of a defect or problem. The following example demonstrates the basic process:

Example

Problem - My car will not start.

1. *Why?* - The battery is dead. (first why)
2. *Why?* - The alternator is not functioning. (second why)
3. *Why?* - The alternator belt has broken. (third why)
4. *Why?* - The alternator belt was well beyond its useful service life and has never been replaced. (fourth why)
5. *Why?* - I have not been maintaining my car according to the recommended service schedule. (fifth why, a root cause)
6. *Why?* - Replacement parts are not available because of the extreme age of my vehicle. (sixth why, optional footnote)

Solution - I will start maintaining my car according to the recommended service schedule.

The questioning for this example could be taken further to a sixth, seventh, or even greater level which is acceptable but not often required.

4.4.2 **Fishbone Analysis –** This method of RCA is useful in evaluating more complex/multi-factorial issues which have led to issues of non-compliance. The fishbone diagram identifies many possible causes of an effect or problem. It can be used to structure a brainstorming session as it allows a team of individuals to sort ideas into functional categories.

As fishbone analysis allows the user to address more complex issues, it also represents a more complex process. The fishbone procedure is described and illustrated below:

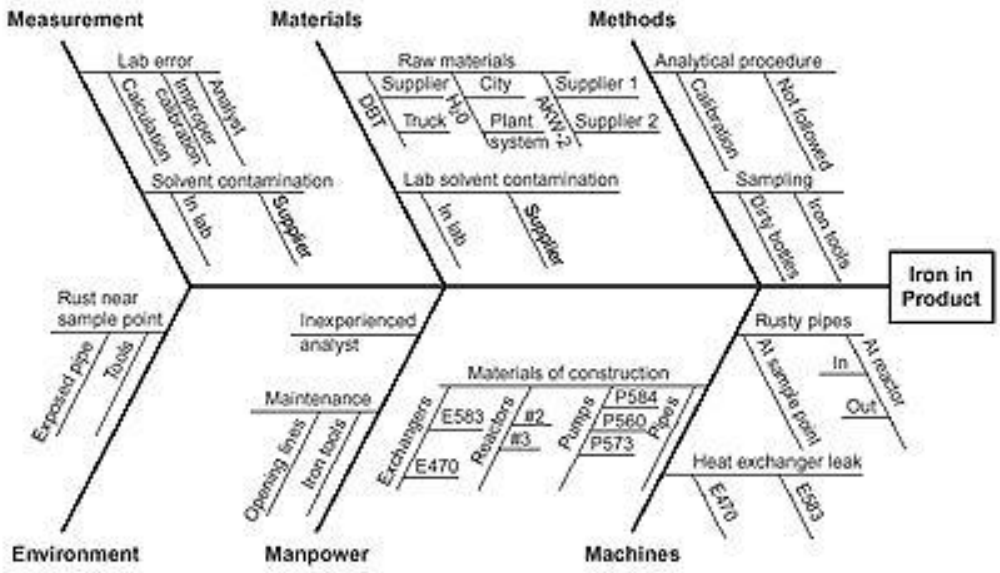
4.4.2.1 Assemble a team consisting of members that have direct insight into the current issue(s)

4.4.2.2 Materials – a flipchart, whiteboard and marking pens

4.4.2.3 The team should agree on a problem statement (effect) and write this in the center right of the chart then establish and brainstorm the major categories that may have attributed to the problem/non-compliance (e.g., methods, equipment, measures, personnel, etc.)

4.4.2.4 Write the categories of causes as branches from the main problem statement and brainstorm all possible causes of the issue. At this point the team should subject each cause identified to the *5 Whys technique* until the final root cause for each issue has been identified to the satisfaction of the team (Reference example below).

Example Fishbone Diagram



4.5 Corrective and Preventive Action

Once root cause is defined, the auditee then proceeds to describe how corrective and/or preventive measures will be defined and applied to address the audit finding(s). It is important to note that not all findings may be subject to both a corrective or a preventive measure. If an issue of non-compliance is identified during an audit and due to extenuating circumstances the finding cannot be corrected (e.g., too much time has elapsed since the problem occurred), then only a preventive measure can be implemented. It also stands to reason that if there is an issue of non-compliance related to a single isolated finding (e.g., a single erroneous entry in a case report) then it can be assumed that only a corrective action can be implemented to close the audit finding.

Once the auditee has defined the CAPA response, the auditee must then define timelines for the completion of the CAPA. The auditee should ensure that realistic timelines for completion of the task at hand are described. Many times inexperienced auditees will describe a time for completion of a CAPA that falls short of the actual time required for implementation. In this case, a member of the audit team may be needed to mentor and guide the auditee to an acceptable CAPA response. Again, care should be taken to ensure that the auditor and audit team only advises and do not directly instruct the auditee, as this will introduce bias into the audit process.

4.6 Effectiveness Verification (EV)

Once the auditor and the auditee have agreed that the defined CAPA and timelines for completion are acceptable to address the issue(s) of non-compliance, then the CAPA moves towards the final completion phase of the audit cycle: effectiveness verification.

Effectiveness verification is the means by which effectiveness of corrective and/or preventive action implementation is verified by a documented and systemic process.

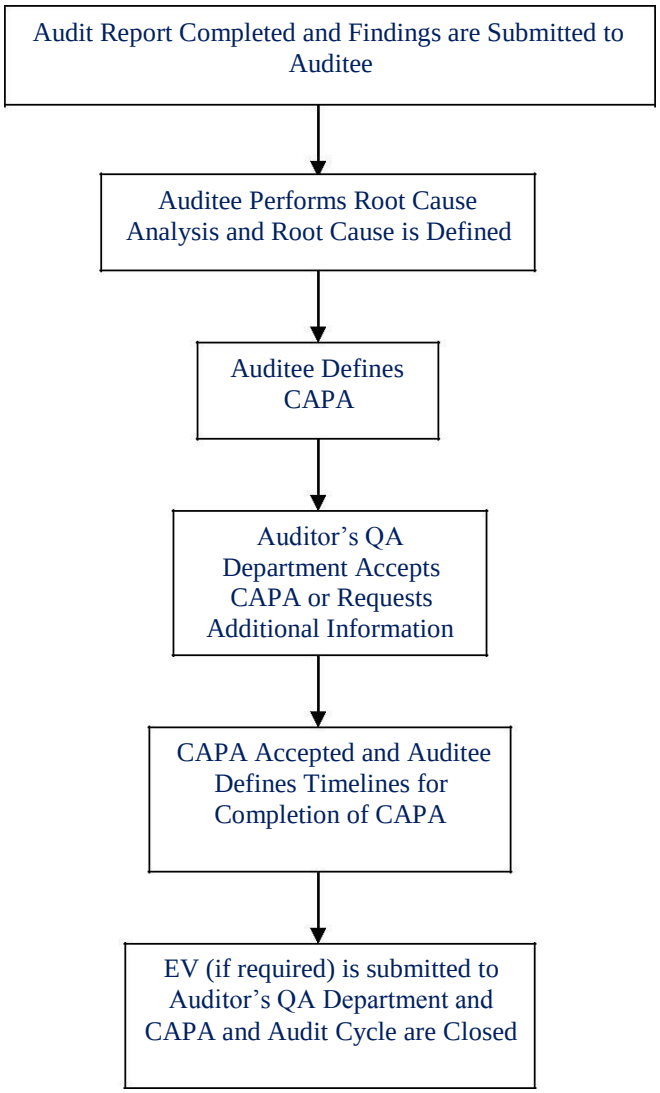
Acceptable effectiveness verification may include the auditee providing documentation which describes evidence of action taken by the auditee which has resolved the audit finding (i.e., Documentation is provided to the audit team which reflects, to a reasonable degree, that actions taken by the auditee have effectively resolved the audit finding and that the issue will not recur). *Note: One should avoid a re-audit as a primary means of effectiveness verification as this is impractical due to the resources involved.*

4.7 CAPA Management and Tracking

To ensure all CAPAs are tracked to closure, Quality Assurance/Compliance units should develop and implement a CAPA tracking system. In many organizations this is linked to their audit management or compliance department systems and ensures that the CAPA and its status (e.g., open or closed) can be determined at any point to satisfy both organization management and/or regulatory agencies.

4.8 CAPA Closure

When all phases of the CAPA process have been satisfied through documented interaction between the auditor or auditor's organization (e.g., compliance unit's document control and management system) and the auditee; and the CAPA process and effectiveness of the CAPA have been confirmed, then the CAPA can be designated as *closed*. The auditor's organization and the auditee should both maintain records to support the CAPA effort in their official files. *Note: As CAPA documentation supports audit activity and defines audit findings, CAPA documentation should not be maintained in files with direct visibility to regulatory agencies.*



Appendix 02
Corrective and Preventive Action

Appendix 03
Grading of Audit Findings

1.0 Introduction/Background

Section 6.3 "Confirmation and Evaluation of Audit Observations," the auditor should evaluate audit observations and report the audit results to the sponsor. The audit findings may be graded according to the level of importance or impact. The purposes of grading audit findings are as follows:

- To clearly indicate the decisions made by the auditor or the auditing department/contractor, and to provide the criteria for the auditee to take necessary action.
- To help the sponsor determine the level of importance of the audit findings and effectively and efficiently take corrective and preventive action to ensure the quality and integrity of data and protect the right, safety or well-being of trial subjects.
- To show trends of non-conformance to the auditee in comparison with the previous ones and/or to compare the outcome of audits, to find systematic deficiency.
- To help focus future audit plans.

2.0 Scope

Proposed grading of audit findings is only applicable for GCP audit. Authorities' grading definitions used for inspection are defined from the view point of authority inspection. So the definition of GCP audit findings is defined for the purpose of sponsor or CRO use.

Grading for other areas of audit, e.g. GMP or Pharmacovigilance audits, should be separately defined according to the relevant regulations.

3.0 Definition

None

4.0 Content

4.1 Grades for Audit Findings

In accordance with the level of importance or degree of impact of the audit findings, audit findings are graded based on the grade classification stipulated in the standard operating procedures (SOP) for audits. Normally, audit findings are classified using three or four grades. As an example, a three- grading scale and the definition of each grade are provided below.

- **Critical**

This applies when the audit findings are considered to adversely affect the rights, safety or well being of trial subjects and/or the quality and integrity of the clinical trial or trial data.

Appendix 03
Grading of Audit Findings

A combination of multiple "major" audit findings may result in a "critical" systemic audit finding even though each of the findings are not "critical."

- **Major**

This applies when, if not managed appropriately, the audit findings has possibility to adversely affect the rights, safety or well being of the trial subjects and/or the quality and integrity of the clinical trial or trial data.

A combination of multiple "minor" audit findings may result in a "major" systemic audit finding, even though each of the finding are not "major."

- **Minor**

This applies to a deviation from the quality management system and/or the principles of GCP, where conditions, practices or processes would not be expected to adversely affect the rights, safety or well being of the trial subjects and/or the quality and integrity of clinical trial and trial data.

4.2 Escalation of Critical Findings

Risk criteria used should be collected and applied consistently and may be based on information already available in the organisation, derived by the audit function itself or both. Wherever possible, objective data should be used but it may be necessary to include subjective judgments as part of the overall assessment.

4.2.1 Findings to be escalated

The following findings may be escalated:

- Critical Findings designated for escalation by a quality management document or SOP.

  In the case of critical findings observed during audits, the critical findings are reported to upper management by the usual process, according to the company quality management process.
- Suspected fraud/misconduct/significant GCP non-compliance

  When fraud/misconduct/significant GCP non-compliance is suspected, this issue should be reported to upper management.
- Organizations may also define other categories of audit findings to be escalated.

4.2.2 Escalation Process

Escalation should be to a sufficiently senior level in the organization so that the problem can be addressed or issues resolved in compliance with the organizations policies and expectations. It is also an idea to have some kind of Issue Advisory Committee to discuss the issues to be addressed by management.

.

Suspected fraud/misconduct/significant GCP non-compliance is escalated to higher management (often involving legal counsel) and also usually escalated to QA management, where investigation of fraud/misconduct/significant GCP non-compliance may be conducted. After the investigation, upper management begins the work for problem solving in cooperation with QA.

4.2.3 Responsibilities of Escalation

Outcomes from the escalation process are the responsibility of the company/organization management. QA only has the responsibility to inform the management of problems or issues to be solved, and to cooperate with any escalation or investigation required.

4.3 Procedure for Grading Audit Findings

4.3.1 Grader

Normally the auditor who prepares the audit report should grade the audit findings but organizations may have different processes detailed in their SOPs.

4.3.2 Timing of Grading

The audit findings grade is first proposed as information supplementary to the audit findings and subsequently determined by the time the audit report is finalized. With regard to critical audit findings that require immediate and prompt actions, the audit findings grade should be determined promptly, and the auditee is required to take immediate and prompt actions.

4.4 Maintaining Consistency in the Grading Audit Findings

The results of grading need to be consistent with other results of grading obtained within the same time period or within the same project, which helps accountability and consistency in the assessment by the audit department.
In order to maintain consistency in the results of grading, the followings may be considered.

4.4.1 Training

Each auditor should be familiar with the rationale for grading of audit findings. As part of auditor training, auditors could be provided with examples of typical audit findings for each grade so that they are able to grade their actual audit findings accordingly. Even if the typical examples contain many elements, including background information, that

makes the grading task complicated, it is still important to share more or less the same policy on grading of the audit findings. It is always useful to discuss actual audit findings between individual auditors.

4.4.2 Peer Review

When an audit report is prepared by the auditor who conducted the audit (and who visited the site of the audit) there is the possibility that they may not have included enough information to explain the audit findings to those who do not know the audit. Moreover, the grading result may be influenced by the auditor's misconception or misinterpretation. Thus, sometimes such audits are restructured in an objective manner using only the information extracted from the audit report, and as peer review, other auditors who have not participated in that particular audit are sometimes asked for their opinion in order to confirm whether or not the audit findings are understandable from the information included in the audit report. More understandable audit findings can be obtained by standardized evaluation of grading results and peer review. One method used to maintain consistency in grading results is to allow audit findings to be graded by selected personnel who have sufficient experiences in the grading of audit findings. Moreover, an improved consistency in grading results can be obtained by sharing between the auditors, the results of grading of audit findings reported by individual auditors. Also it is preferable that there be a QA management review of all audit reports to improve consistency.

4.4.3 Database

Accumulating audit findings, grading results and the classification used for audit findings* in a database could be shared between auditors and used as a reference at the time of grading of other audit findings, or used as training materials for the auditors. Such a database is useful for trend analysis of audit findings and detection of risks.

*Classification of audit findings can form part of the metrics reported to the sponsor management, , e.g. protocol non-compliance, contracts and agreements.

4.4.4 Algorism

Conflicts in grading results between auditors or between different audit type (e.g. investigator site audit, Pharmacovigilance audit or system audit) can be minimized by establishing an algorithm for the grading of audit findings. This helps maintain consistency in the results of grading of audit findings.

Appendix 03
Grading of Audit Findings

5.0 References

Grading of Inspection Findings of **PROCEDURE FOR REPORTING OF GCP INSPECTIONS REQUESTED BY THE COMMITEE FOR MEDICINAL PRODUCTS FOR HUMAN USE (CHMP)**

GCP INSPECTION FINDINGS CLASSIFICATION at MHRA Website http://www.mhra.gov.uk/home/groups/is-insp/documents/websiteresources/con2033551.pdf

Guideline on good pharmacovigilance practices (GVP) Module IV – Pharmacovigilance audits http://www.ema.europa.eu/docs/en_GB/document_library/Scientific_guideline/2012/12/WC500136233.pdf#search='module+IV+Audit'

Grading of inspection findings at Good Pharmacovigilance Practice: The inspection process of MHRA Website http://www.mhra.gov.uk/Howweregulate/Medicines/Inspectionandstandards/GoodPharmacovigilancePractice/Theinspectionprocess/index.htm

6.0 Recommended Readings

ISO 9001 Quality management Systems -Requirements

ISO 9000 Quality management systems –Fundamentals and

Vocabulary ICH Guideline Quality Risk Management Q9

ICH Guideline Pharmaceutical Quality System Q10

Appendix 04
Clinical Investigator Site Audit

1.0 Introduction/Background

Clinical investigator site audits are conducted in order to fulfill sponsor obligations under ICH 5.1.1, to review study conduct for compliance with national and international GCP guidances, national legislation and the study protocol, paying particular attention to subject rights, safety and well-being, and to provide verification of data integrity.

The objectives of clinical investigator site audits are:

- To determine the research site's adherence to the study protocol, SOPs, GCP guidelines, International Conference on Harmonization (ICH) guidelines for Good Clinical Practice and applicable national, regional and local regulations;
- To ensure scientific data is reliable, accurate and verifiable;
- To determine that the rights, privacy, safety and welfare of human research subjects are being adequately protected; and
- To ensure that the study sponsor and designated site monitors are monitoring the study in accordance with GCPs, ICH guidelines, and applicable national, regional and local regulations.

Additional attention may be placed upon ensuring that clinical investigator sites are "inspection-ready" in the event of a regulatory agency inspection.

2.0 Scope

Clinical investigator site audits may be conducted at any medical facility or institution where clinical trials are conducted on human volunteers or subjects. Typically, the following clinical investigator sites are audited:

- Clinical investigator sites conducting Phase II – Phase III studies
- Clinical investigator sites conducting Phase IV studies upon requirement of regulatory authorities
- Clinical investigator sites, CROs, or Phase 1 Units

3.0 Definitions

NA

4.0 Contents

4.1 Audit Planning

According to ICH GCP, audit plan needs to be prepared. An audit plan can be prepared at a study level or for each audit. If the sponsor has engaged a CRO for the monitoring of clinical investigator sites, the audit plans of the sponsor and CRO should be coordinated.

Appendix 04
Clinical Investigator Site Audit

A study level audit plan typically describes all study related audit activities, such as clinical investigator site audits, CRO audits, and other study-specific audits. The actual selection of the clinical investigator sites to be audited may be included in the plan, or alternatively the plan may describe only the sampling plan for site selection, and such considerations as timing of audit in relation to recruitment, etc. The requirements for site selection and audit timing are also described in Standard Operating Procedures (SOP).

The number of auditors and the days of audit can be determined according to the project complexity, the number of patients screened/enrolled, the size of CRF, and/or geographic location and budget. The audit plan should also describe sampling plans, e.g. for selection of subjects for review, review of consent documents, source data verification, drug accountability and any study-specific requirements.

4.2 Selection of Clinical Investigator Sites to be audited

The selection of the sample of clinical investigator sites may be achieved by a risk-based algorithm, by following a pre-determined set of selection criteria, or according to the auditor's own judgment. In all of these approaches, the factors that affect site selection typically include some or all of the following criteria:

- Number of subjects recruited or enrolled at the clinical investigator site;
- Concern that the Investigator is not fulfilling his/her obligations or is non-compliant with GCP, protocol, or regulatory requirements;
- Information relating to concern for subject safety;
- Information relating to consistent CRF discrepancies or high query rates;
- At request of the study operational team (if accepted by Quality Assurance unit);
- Past audit experience;
- Past inspection experience;
- Geographical and logistical considerations.

The sample of investigator sites allows assurance that systems and procedures for running clinical studies are effective.

4.3 Selection and Training of Auditors

Auditors should be selected according to education, training, experience, and language skills to conduct the audit. Audit team members need to have adequate knowledge of the project, protocol, GCP and relevant SOPs to fulfill their responsibilities.

4.4 Scheduling

Depending on the organization of the study, auditors or CRAs can contact the sites selected for audit to determine mutually-acceptable dates for the audits. CRA attendance at a site audit is recommended for the following purposes:

1) the CRA will be familiar with the investigator, site staff, site facilities and source documents, which can greatly assist the auditor's job.
2) as a learning opportunity for the CRA.
3) to assist with translation, if the language of the clinical investigator site is not understood by auditors;

A confirmation letter should be sent to each investigative site confirming the audit date and schedule for the audit, and providing details of any documents or personnel required to be present during the audit.

Monitoring visit schedules will be taken into consideration when audits are scheduled, to ensure an adequate amount of data have been monitored prior to audit, and to ensure that the audit visits do not conflict with monitoring visits.

4.5 Preparation

In preparation for the audit, auditors will review key regulatory and essential documents from the trial master file and investigator file at the sponsor or CRO. Documents to be reviewed include, as appropriate:

- Protocol and amendments
- Investigator Brochure
- Regulatory/IRB/Ethics Committee approval documentation
- Protocol agreement and other study contracts
- Case Report Forms (CRF) and site-specific consent forms
- Investigational Medicinal Product Documents (e.g. accountability, shipment)
- Monitoring Plan, Monitoring Visit Reports, project plans and manuals
- Safety plans and safety reports (e.g. CIOMS)
- Important correspondence (pertaining to safety, protocol deviation or key decisions)
- Investigator qualification documentation (e.g. CV, medical licenses, Financial Disclosure Forms (if necessary)

It is important to consider how the auditors will access any of the above documents that are not paper-based, for example, electronically-managed CRFs (eCRF) or trial master files (eTMF). The auditors may request their own access to the eCRF or eTMF, or they may rely on paper printouts of these documents for reference and review. The auditors may review a sample of completed eCRFs and associated data queries prior to the site visit.

Another important consideration for the scheduling of site audits includes defining responsibilities between sponsor and audit contractor, when using an

audit vendor. Considerations include communication responsibilities, audit SOPs to be followed, management of preparation and review of audit reports, and responsibility for audit follow-up.

4.6 Onsite Audit Activities

Audit activities conducted at the investigator site include, but are not limited to:

- Introductory Meeting: meeting with the Principal Investigator, Sub-Investigator and/or Study Coordinator to review the objectives of the audit and to obtain preliminary information regarding site practices and conduct of the study at the site
- Informed Consent: review of informed consent source documentation and signed Informed Consent Forms at the site
- Regulatory/Ethics/Essential Study Documentation in the Site File: regulatory/IRB/IEC communication and approval of protocol, amendment, consent form, and advertisements and reporting of protocol deviations, serious adverse events, and safety reports for regulatory submission, site personnel qualification and training documentation, protocol and protocol amendment signature pages, delegation documentation, financial disclosure documentation, monitoring documentation
- Investigational Medicinal Product (IMP): receipt, storage, security, and accountability processes and documentation
- Source Data Verification (SDV): CRF sampling ratio and Study criteria to verify is determined prior to audit
- Safety: identification, documentation and reporting of AEs and SAEs. Medical management of adverse events
- Study Conduct: adherence to protocol and Good Clinical Practice
- Monitoring: review of monitoring practice, SDV and adherence to the Monitoring Plan
- Facility tour (e.g. pharmacy, laboratory, archive or other relevant departments). Any laboratory and/or equipment used for generation of key efficacy/safety data, and associated records, will be inspected during the tour. Any freezers used to store biological sample that will be analyzed for key data should also be checked during the tour.=
- Debriefing or Closing Meeting: meeting with relevant site personnel to discuss audit observations, explain audit reporting process, and answer any questions

It is advisable to have a process for the expedited escalation and reporting of serious non-compliance issues that may be discovered during the course of the audit. This process may include the opportunity for the auditors to discuss the issues directly with the study sponsor during the audit, if considered appropriate.

4.7 Audit Reporting

Following the completion of each site audit, a comprehensive audit report will be generated, using the current report template, which describes the scope of the audit activities and key findings and observations, within a determined business days of return to the office, according to the relevant audit SOP. It is usual for the audit report to be completed no later than one month of audit.

Once the audit report is issued, the monitor, study coordinator and any other key investigator site staff should discuss the audit findings and decide how to respond to each finding. The response should contain both corrective and preventative actions, as appropriate to the findings of the audit. The audit response is therefore often referred to as a Corrective Action and Preventative Action plan (CAPA). The processes for preparing, reviewing, approving, follow-up and closure of a CAPA are usually described in the sponsor company's audit SOPs.

It is customary for a post-audit courtesy or thank-you letter to be sent to the investigator site following the audit. Audit findings are not normally included in this letter. An Audit Certificate is usually generated upon completion of the audit as a record that the audit has taken place.

5.0 References

NA

6.0 Recommended Reading

NA

Appendix 05
Electronic Medical Records (EMR)

1.0 Introduction/Background

Electronic Medical Records (EMR) are a collection of a patient's medical information in a digital (electronic) form that can be viewed on a computer or other electronic reader (e.g. Tablet or smartphone etc) and easily shared by people taking care of the patient. When an EMR is used in clinical research, the specific focus of data integrity and subject safety may not necessarily involve the full and comprehensive medical information; the context is specific to the requirements of the Investigational Plan (Study Protocol) and the manner in which the system is used to comply with the applicable requirements of Good Clinical Practice (GCP). As such, a site may have data maintained in EMR that is not part of the clinical trial.

The terms EMR and EHR (Electronic Health Record) have been used interchangeably in healthcare regarding electronic systems; however, these systems have different meanings in medical informatics. The term EHR is being engendered by the 2009 HITECH Act in the US with increasing familiarity; however, the term EMR is more relevant in the context of technical informatics and within the international GCP community. Definitions are provided in section 3.0.

3.0 Definitions

3.1 Electronic Medical Record (EMR – National Cancer Institute, 2009)

A collection of a patient's medical information in a digital (electronic) form that can be viewed on a computer and easily shared by people taking care of the patient.

3.2 Electronic Health Record (EHR)

A longitudinal electronic record of patient health information generated by one or more encounters in any care delivery setting; including information on patient demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data, and radiology reports.

3.3 Validation (US FDA Glossary of Computerized Terms, 1995)

Establishing documented evidence that provides a high degree of assurance that a specific process will consistently produce a product meeting its predetermined specifications and quality characteristics.

3.4 Software Validation (GAMP, version 5)

Confirmation by examination and provision of objective evidence that software specifications conform to user needs and intended uses and that the particular requirements implemented through the software can be consistently fulfilled.

3.5 System Life Cycle (SLC - FDA Glossary of Computerized Terms, 1995)

The course of developmental changes through which a system passes from its conception to the termination of its use.

3.6 Installation Qualification (IQ - USP General Chapter 1058)

Documented collection of activities necessary to establish that an instrument is delivered as designed and specified; properly installed in the selected environment and the environment is suitable for the instrument.

3.7 Operational Qualification (OQ - USP General Chapter 1058)

Documented collection of activities necessary to demonstrate that an instrument will function according to its operational specification in the selected environment.

3.8 Performance Qualification (PQ – USP General Chapter 1058)

Documented collection of activities necessary to demonstrate that an instrument consistently performs according to the specifications defined by the user and is appropriate for its intended use.

3.9 Raw data (Based on GLP definition)

Any worksheets, records, memoranda, notes or exact copies thereof that are the result of original observations, and activities and are necessary for the reconstruction and evaluation of that trial.

3.10 Source data

All information in original records and certified copies of original records of clinical findings, observations, or other activities in a clinical trial necessary for the reconstruction and evaluation of the trial. Source data are contained in source documents (original records or certified copies).

4.0 Content

4.1 Introduction

The use of EMR systems has rapidly evolved in patient medical care over the last decade improving the limitations imposed by paper records, including but not limited to unavailability (must be centrally located), inconsistent legibility, duplication of information, storage and maintenance of the record, and inconsistency of information. EMR has brought its own challenges such as control and access to patient information, back-up, traceability and retrievability of data from decommissioned systems, back up/disaster recovery and protection of personal patient information. As a result a number of guidances/position papers and legislation has evolved such as Annex 11, Computerized Systems, GAMP, PEACH, CDISC and 21CFRPart 11 to ensure data is managed in a controlled environment.

As Clinical Research moves into increased automation, the use of an institution's EMR system has become more prominent, replacing traditional paradigms for subject/patient recruitment (improved cost effectiveness), medical screening and inclusion/exclusion data capture (reduction in simple data entry errors) and rapidly identifying adverse events (data mining). The regulatory expectations of GCP, whether a paper-based system is used or electronic, remain unchanged. The

data must be **A**ccurate, **L**egible, **C**ontemporaneous (timely), **O**riginal and **A**ttributable – often referred to as ALCOA or standard Good Documentation Practice (GDP).

The EMA Reflection paper (effective 01-Aug-2010), "Expectations for electronic source data and data transcribed to electronic data collection tools in clinical trials", an additional four (4) data standards were added to the traditional ALCOA GDP acronym: Complete, Consistent, Enduring, and Available when needed. This is often referred to as ALCOA +.

The standards for the documentation providing objective evidence to support conduct of the clinical trial and compliance with the protocol are the foundation for any assessment (audit and/or inspection) of the use of an EMR system as well as the manner in which the system has been validated. An instrument used to capture source data should ensure that the data are captured as specified within the protocol.

The qualification of an investigator site differs from the audit of a site after first patient in (FPI). This appendix focuses on the audit of the investigator; specifically, approaches to assessing fitness of EMR usage in the context of the investigational plan (protocol). Site qualification of investigators employing EMR or any electronic system should be properly assessed prior to initiating patient recruitment; primary focus on the validation or fitness testing employed within the organization's computing environment.

4.2 Audit Planning and Preparation

In determining the suitability of an EMR for managing Clinical Trial data, an assessment needs to be carried out to determine its suitability. This should be carried out at site selection stage (feasibility) when a site/private practice services and systems will be assessed.

A risk-based approach is a recommended best practice for auditors in selecting which investigator sites should undergo an audit. It is not feasible, for every site enrolling patients to be audited. Typical risk factors or information that should be considered by the QA professional in selecting sites for audit are as follows (not an exhaustive list):

- Systems used by the Site (off the shelf/hybrid/bespoke/medical applications used in the clinical practice and potentially supplying data to the clinical trial)
- Number of IT systems used by the site and interfaces between systems versus paper based source data
- Risk Based approach for audit planning (covered in an additional appendix)

As the prominence of automation in clinical trials continues to evolve, an investigator site using electronic systems presents an additional risk factor that

must be considered. A key aspect of any electronic system implementation in the GCP environment is the operation of the system and the documentation of its operation. An investigator site that purchases an EMR system (Configurable off the shelf software (COTS), applies to systems that can be self configurable not requiring hard coding) or implements their own system that claims compliance to a regulatory standard simply uses it "out-of-the-box" presents a significant regulatory risk to a Sponsor/CRO.

It is recommended that investigator site audits be conducted using a basic checklist as an aide memoire to assess minimum requirements of data access, security, storage, backup and archive procedures. When an investigator site employs EMR, it is recommended that the site audit checklist include information for assessing the use of the system. In preparation for an investigator site audit that employs an EMR system, the following (in no particular order of importance) should be considered – this can be built into a checklist (recommended):

1. EMR System access and privacy rules
    a. Monitors and QA auditors must have access to original source data
    b. Privacy/data protection rules may not allow the monitor/QA to access original data within the EMR system; for patients who have consented to such data access in which case the site should have a documented process to provide certified copies of source data from the system.
        i. The auditor should familiarize themselves with applicable privacy/data protection regulations in the country/region in which the site is located
        ii. Privacy rules may cause issues regarding auditor access to original data – appropriate, documented process should be in place to ensure access either through training & access rights to the auditor for Read Only access to the files of those subjects who have consented; or through the process of providing adequate certified copies that a sample can be QC checked "over the shoulder" of an authorized user to ensure authenticity.
    c. The system should have unique identifiers (i.e., username) and passwords to access the system
        i. Passwords should never be shared
    d. The EMR system should have automated log-off or suspend functionality after a period of inactivity, including forced password expiry e.g. 90days.EMR end-user roles should be defined; specifically, access to certain functionalities controlled.
        i. A list of individuals authorized to access each function should be maintained by the site
        ii. Note: During the audit, it is recommended that the list in 1.d.i be made available along with the delegation of duty log to facilitate assessments of data attribution and if that individual is qualified for their role and system use
2. EMR System End-User Application

a. How is the EMR used?
    i. Direct data entry – the original data is electronic
        1. Auditor should have direct access to the e-record within the system or a process as identified above 1bii.
    ii. Hybrid – combination of direct data entry and transcription from paper
        1. Process for certifying a copy of the original data should be in place. Paper should also be maintained and at a minimum a sample monitored/audited where appropriate.
    iii. Do subjects/patients enter data directly?
        1. Process should be defined, training provided
b. How is source data defined – is raw data differentiated from source data?
    i. The investigator should maintain the original source document or a certified copy.
c. Training
    i. Are staff trained on system use?
    ii. Are monitors trained on system use? (Read Only access to the files of those subjects who have consented and rescinding of access rights after study closeout)
    iii. Data Correction/Audit Trail
    iv. Changes to original entries are captured in an independent audit system trail
        1. Original and changed information should be available for review
        2. Changes are time and date stamped
        3. Audit trail indicates who made the change and reason for change should be captured
        4. Audit trail cannot be modified
        5. Audit trail cannot be turned off and should be available in a readable format
    v. Source data should only be modified with the knowledge or approval of the investigator
d. Electronic Signatures
    i. Electronic signatures should be protected from intentional and unintentional misuse
    ii. Electronic signature applied to a record cannot be "cut and pasted" into another record
    iii. Electronic signatures should display the name of the signer and meaning of the signature defined
e. The location of source documents and the associated source data should be clearly identified at all points within the capture process.

3. EMR System Validation, Maintenance and Control
    a. Validation
        i. Organization should have documented processes for validation of the system

.

1. Best practice for validation is a SDLC (defined) approach
2. In lieu of a standard SDLC approach, at a minimum, IQ/OQ/PQ should be documented detailing the install and set-up of the system for use at the site
3. End-user requirements of the system should be tested and shown to be fit for purpose within the organization

ii. Vendor verification of System fitness without at least User Acceptance testing (UAT) at the organization is not sufficient for the purposes of GCP compliance

b. Change Control
   i. Documented procedures should be in place for system maintenance and upgrades
   ii. Changes to the system should be documented and tracked and as applicable re-validated/UAT for fitness
c. Back-up and Recovery
   i. The institution should have an effective Disaster Recovery Plan which is periodically tested with objective evidence of the testing
   ii. System data should be backed-up (remotely and/or protected storage)
   iii. Testing of restoration should be executed at adequate intervals
   iv. Procedures in place per applicable regulations for compliance with record retention requirements.
      1. The storage of source documents should provide for their ready retrieval.
      2. Source documents and data should be protected from destruction.

The preceding list highlights key aspects for consideration in preparation for an investigator site audit. Sites using EMR should be vetted to ensure the EMR system is fit for use. Once screening/randomized has occurred and data captured, a non-compliant (to GCP standards and expectations) EMR system presents a significant risk to the validity of data used to support a marketing application and may present a risk to the safety and well being of the subject.

Appendix 05
Electronic Medical Records (EMR)

5.0 References

Computerized Systems in Clinical Research: Current Data Quality and Data Integrity Concepts (Peach - 2011)

EMEA Reflection Paper: Expectations for electronic source data and data transcribed to electronic data collection tools in clinical trials; June 2010, Carl Anderson

Applied Clinical Trials (ACT), "The Ins and Outs of Electronic Medical Records: Shedding light on common EMR concerns about privacy, government regulations and data integrity." September 2008

FDA Guidance: Computerized Systems Used in Clinical Trials; May 2007

FDA Guidance: Part 11, Electronic Records; Electronic Signatures – Scope and Application; August 2003

Clinical Research Systems and Integration with Medical Systems, Joyce C. Niland and Layla Rouse; April 2011

ICH GCP E6: Good Clinical Practice: 1996

6.0 Recommended Reading

Journal of the American Medical Association (JAMA), "Should Sensitive Information from Clinical Trials be included in Electronic Medical Records?" August 2010, Boadie W. Dunlop

Electronic Medical Records Utility in Clinical Trial Conduct; January 2009

FDA Guidance: Electronic Source Data in Clinical Investigations; September 2013

Electronic Medical Records in Australia and Clinical Trials; ARCS Australia Ltd., March 2008

FasterCures, White Paper – Think Reseach: Using Electronic Medical Records to Bridge Patient Care and Research; Fall 2005, Kathi E. Hanna

Clinical Data Interchange Standards Consortium (CDISC)

Good Automated Manufacturing Practices (GAMP)

.

Appendix 06
Conducting an IRT (IVRS/IWRS) Vendor Audit

1.0 Introduction/Background

Interactive Response Technology (IRT) is the generic term that can be applied to the use of Interactive Voice Response Systems (IVRS) and Interactive Web-based Response Systems (IWRS) and is one of many different types of systems/vendor audits that may be conducted. IVRS employs the use of computer based technology, via the telephone, to randomize subjects and/or manage investigational medicinal product (IMP) distribution during a clinical trial. The advancement of technology has meant that companies now employ the use of IWRS over traditional IVRS. This appendix will use the generic term IRT to describe assessment of the electronic systems.

2.0 Scope

This guidance will focus on conducting an IRT system audit. This guidance will only focus on the unique items to consider when assessing the suitability of vendor for performing IRT services. General items that are performed in common vendor/system audits will not be covered in this document.

3.0 Definitions

NA

4.0 Content

4.1 Preparing for the Audit

The first thing you will need to do is get a clear understanding regarding what the IRT will be used for. Will it be used for recruitment/randomization only? Will it be used for IMP management only? Will the system be used for both?

Secondly, it is important to determine how the IRT (and the subsequent data collected) will interact with the clinical trial systems in place. For example, will randomization data be uploaded directly into the eCRF? How will the system interact with any current processes that are in place for clinical supply management?

It is very important that you identify all IT systems early on that will be or are affected by IRT. Speak with the systems owners early.

4.2 Audit Conduct

Some key items to focus on when conducting an IRT audit include:

.

- Quality Management System including Computerized System Validation policy/standard
- Validation Plans and Reports
- User Acceptance Testing and Report
- Change Control
- Security Measures
- Management of Issues
- Training, qualification of key personnel
- Customer Support Services (e.g. Helpdesk)
- System Down Time (Both for routine maintenance and unexpected)
- Disaster Recovery and Business Continuity
- Data Storage and Backups
- Server Room

To conduct computerized system validation activity, it is necessary to have Swapnil Mahapure (non-Celgene) a documented procedure for computerized system validation as policy or standard. The IRT Vendor should have a suitable Quality Management System including QA/QC activities. According to authority regulatory requirement, quality management system including QA should be established in the vendor.

Data generated by IRT is electronic data. The items referenced above will need to be reviewed in detail during the audit. For electronic data, it is imperative that data integrity remain intact at all stages: from data creation, transfer and reporting, archiving. Review the validation plans and change control to ensure the system was designed and continues to perform as expected. Issue management and system down time are key elements that can make or break electronic systems. Does the IRT vendor have adequate procedures in place to manage issues? Can the IRT vendor provide any evidence that they followed these procedures? What type of system uptime/downtime metrics can the vendor provide? There should be proper security measures in place such as setting up user accounts and restricted access. This includes ensuring that only trained and authorized individuals are granted access and that access rights are revoked in a timely manner. Finally, the vendor should be able to provide training based on the role of the individual with respect to system use.

It is also important to visit server room, where access security, fire protection, disaster protection, power supply and data back-up and general review of Disaster recovery/Business Continuity controls can be ensured.

4.3 Study Specific Example of IRT Audit Scope

This type of audit assesses the documented process for study specific set up of an individual study. The audit should take into account randomization requirements, regional and country set up requirements including any specific reports that may

be required. For example, some countries require periodic reports for controlled drugs. If CDs are used, the system needs to be configured to allow for reporting requirements, validation and change control processes for IRT and will focus on the following core areas:

- Study Requirements – User Requirement Specification, documentation of Initial kick off meeting with vendor
- Personnel involved – Level and nature of oversight and review/sign off process by the Sponsor
- Current Vendor Process used for setup/management/training
- Documentation
  - URS (User requirement specification)
  - PRS (Project requirement specification)
  - UAT (User acceptance testing)
    - Critical Items
    - Non critical items
  - Responsibilities
  - User Manual
- Trigger levels
- Randomisation process
  - Who is responsible for randomisation – how is that communicated to the Vendor and monitored
- Oversight of CRO – changes to work order/who is responsible for sign off and authorisation of payment for changes to the scope of work
- Use of IRT for monitoring recruitment, patient compliance, returns
- Translation process (Web, Phone, User Guide)
- Communication Process/Issue management process between vendor and sponsor
- Data Query Handling (e.g. data corrections, manual changes, and evidence of PI confirmation)
- Risk-management Process
- A review of a sample of documents at the site/CRO
- Access to source data (if IRT holds source data)

5.0 References

- ICH E6 Good Clinical Practice 1996
- Directive 2001/20/EC "Clinical Trials Directive"
- Directive 2005/28/EC "GCP Directive"
- Orange Guide, Annex 13
- PI 011-3 25 September 2007 - PICs (PHARMACEUTICAL INSPECTION CONVENTION)
- 09 June 2010 EMA/INS/GCP/454280/2010 GCP Inspectors Working Group (GCP IWG) - Reflection paper on expectations for electronic source data and data transcribed to electronic data collection tools in clinical trials
- EMEA/505620/2007 - REFLECTION PAPER ON EXPECTATIONS FOR ELECTRONIC SOURCE DOCUMENTS USED IN CLINICAL TRIALS
- Current GAMP Thinking on Quality Risk Management: Mapping of the GAMP QRM Concept to ICH Q9 and ISO 14971

6.0 Recommended Reading

NA

.

Appendix 07
Conducting Audits of Data Management or Electronic Data Capture Systems

1.0 Introduction

Systems and procedures relating to Data Management activities are key to ensuring that data for a clinical trial are collected, verified and stored in a secure way, not only to provide assurance of data quality and reliability, but also to protect the privacy of subjects participating in clinical trials (ref: ICH GCP section 5.5).

Key tools used within data management processes are an electronic clinical trials database and, very often, an electronic data capture (EDC) system. Typically these are either 'off the shelf' packages or in-house developed systems used by data management groups. Special consideration should therefore be made to assess aspects of design, building and validation of these databases during data management audits.

2.0 Scope

This document provides guidance on the key considerations when performing audits of Clinical Trials Data Management functions and EDC systems. It does not cover statistical analyses, clinical study reports or the more general aspects of auditing any type of vendor.

3.0 Definitions

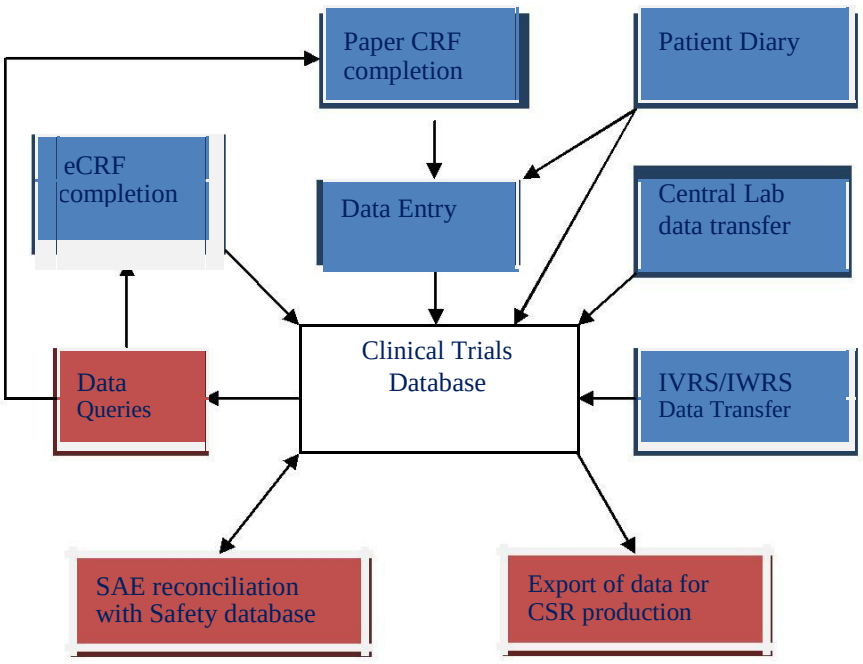
N/A.

4.0 Content

4.1 Preparing for the Audit

Knowing what data management systems are being used helps to determine the scope and timing of the audit. For example, if the purpose of the audit is to look at systems supporting a specific study, then the scope could be limited to those areas of particular interest and may include more data checking (e.g. if only using paper case report form (CRF) then there is no need to assess EDC systems). Awareness of the overall database structure and associated interfaces will also help to prepare (e.g. whether data are being transferred into the database from external sources such as central laboratories). Discussing the systems of interest with the relevant system owners will develop the auditor's understanding of what needs to be included in the scope and the timing of the audit in the data management process (e.g. prior to database lock, for example). Using simple process mapping or simple schematics as tools helps to visualize the whole system and to recognise critical steps and interfaces (inputs and outputs). An example simple schematic is given below. It is important to note that this is just one possible example and that each data management system may have different interfaces and processes. The auditor can request support from subject matter experts on some of the technical aspects of data management.

Appendix 07
Conducting Audits of Data Management or Electronic Data Capture Systems



4.2 Audit Conduct

Key items to focus on when conducting data management or EDC system audits typically include:

	DM Audit	EDC Audit
Maintenance of written procedures for all aspects of the process	X	X
Appropriate and clear delegation by Sponsor	X	X
Roles and responsibilities of data management team	X	X
Data management plans	X	X
Data management study files	X	X
Database set up (specifications /build /validation / user acceptance testing)	X	X
Programming activities (e.g. data exchange)	X	X
Design of CRFs and other data collection tools (e.g. patient diaries or questionnaires)	X	X
Qualification and training, including of temporary/contract staff	X	X including investigator sites
Qualification, contracting and oversight of any	X	X

Appendix 07
Conducting Audits of Data Management or Electronic Data Capture Systems

	DM Audit	EDC Audit
sub-contractors		
Receipt and tracking of completed and uploaded CRFs or CRF sections	X	X
Data entry / data transfer from eCRFs and e-diaries to database	X	X
Subject disposition (i.e. correct management of screening and randomisation numbers according to the protocol)	X	X
Manual and automated validation checks of CRF data with focus on critical efficacy and safety parameters in the study protocol	X	X
Data queries and resolution	X	X
Coding (e.g. MedDRA, WHO-DDE or WHO-ART)	X	X
QC processes including e.g. double data entry and error rate monitoring with acceptance/rejection criteria	X	X
Implementing protocol amendment-driven changes	X	X
Import and export of data (e.g. import from central laboratories, export for statistical analysis)	X	X
Database lock (including process for interim analyses)	X	X
Controlled unblinding (e.g. for Independent Data Monitoring Committee or after database lock)	X	
SAE/AE Reconciliation (between clinical trials database and safety database)	X	
Data privacy protection	X	X
User support	X	X
System security, including maintenance of list of authorised users from activation to deactivation of access, ID/password management	X	X
Computer System Validation documentation	X	X
Change control procedures	X	X
Back-up and recovery systems/ Business Continuity	X	X
Physical security of electronic systems, data servers and paper records, including equipment at investigator sites	X	X
Arrangements for archiving of electronic and paper media	Electronic & paper data	Electronic data only

.

Appendix 07
Conducting Audits of Data Management or Electronic Data Capture Systems

	DM Audit	EDC Audit
Quality assurance	X	X
Any other obligations according to contract or functional procedures	X	X

Appendix 07
Conducting Audits of Data Management or Electronic Data Capture Systems

4.2.1 Considerations for Data Management Audits

In general terms, the assessment of data management systems during audit can be divided into four main activities:

a) General functional processes, clearly assigned between client and vendor in the case of outsourced tasks – roles and responsibilities, procedural documents, training, general physical security of systems and paper records.

b) Study set up activities – this will typically include CRF design and database set up and validation (specifications /build /validation /user acceptance testing) .

Tools used to capture clinical trials data (e.g. CRFs/eCRFs, patient diaries, quality of life questionnaires) should be designed to capture all data required by the study protocol. A level of checking must therefore have been performed to ensure that these requirements have been met as well as demonstrating that the overall database is performing as intended (i.e. validation). A comparison of the CRF with protocol requirements could be made to ensure that all critical data fields required fulfil the needs of the protocol.

c) On-going study activities – these will typically include system access maintenance, data entry, management of data queries, QC processes, importing of data into the clinical trials database (e.g. from central laboratories or IVRS/IWRS providers), coding activities production of metrics reports (number of queries, error rates, missing pages/data, number of outstanding queries and time outstanding), production of data for interim analyses, implementation of database changes based on protocol amendments, SAE reconciliation of clinical trials database and safety database. Involvement of the medical monitor in this process could also be explored.

Data query management processes should be designed to ensure that changes made to data are performed by authorized personnel only and that any data changes are evident (with no permanent deletion of previous entries) through the use of adequate data traceability (e.g. data clarification forms and audit trails, including self-evident corrections and corrections approved by investigators). Consider selecting a sample of data from the database and comparing with CRF and query documentation to assess this process.

Changes to an EDC system resulting from substantial protocol amendments pose a particular risk because it is possible technically to implement them quickly but should generally not be available to an investigator until relevant regulatory and ethics approvals are confirmed.

.

This might require the EDC changes to be implemented in a phased way (e.g. country by country) as approvals are received.

Interfaces with other data systems should also be considered as part of the data management audit (e.g. transfer of laboratory data from central laboratories into the clinical trials database or export to a clinical trial management system). Assessment of procedures to ensure that data integrity is not compromised during data transfer should therefore be included (e.g. format specifications, test transfers and/or post-transfer QC).

d) End of study activities – this will include data cleaning, database lock, unblinding, export for statistical analysis, archiving process (including ongoing availability of eCRF data at the investigator site), revocation of access/privileges to electronic systems and transfer of the database to the sponsor.

Additional Scope Items

In additional to core activities covered above, audits may also cover CRF completion guidelines, reports by Data Management used to implement adaptive monitoring strategies, EDC system, managing data entries and corrections depending on whether source document verification has been done by a site monitor

4.2.2 Considerations for EDC System Audits

The same general principles for preparation of a Data Management Vendor Audit will also apply for an EDC system audit. The main difference being that the scope of an EDC audit will generally be more limited (e.g. it is not possible to perform a standard database audit comparing paper CRF with the clinical trials database), or may focus more on computer system aspects (e.g. validation, user acceptance testing, backup and security).

Some additional high level aspects of eCRF audits could be taken into consideration during investigator site audits, i.e. whether:

- study-specific user acceptance testing has been performed at the site level
- installation and access levels have been tested and are being followed
- continued access to the data for the investigator is available after the end of the study
- the system has robust procedures for capturing valid electronic signatures
- procedures include a check of audit trail for overuse or under use of accounts (indicator of account sharing by site staff)

5.0 References

E6 Good Clinical Practice - Section 5.5 (International Conferences on Harmonisation, 1997)
http://www.ich.org/fileadmin/Public_Web_Site/ICH_Products/Guidelines/Efficacy/E6_R1/Step4/E6_R1__Guideline.pdf

European Commission Directive 2001/20/EC Article 3, Section 2 (c)
http://ec.europa.eu/health/documents/eudralex/vol-10/index_en.htm

US Code of Federal Regulations, Title 21:

Part 11 – Electronic Records; Electronic Signatures
http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfCFR/CFRSearch.cfm?CFRPart=11
Part 312 – Investigational New Drug Application
http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRsearch.cfm?CFRPart=312

Guidance for Industry - Computerized Systems Used in Clinical Investigations (US Food and Drug Administration (FDA, May 2007)
http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM070266.pdf

Reflection paper on expectations for electronic source data and data transcribed to electronic data collection tools in clinical trials (European Medicines Agency, 2010)
http://www.ema.europa.eu/docs/en_GB/document_library/Regulatory_and_procedural_guideline/2010/08/WC500095754.pdf

6.0 Recommended Reading

Guidelines to Facilitate the Production of a Data Handling Protocol (Association for Clinical Data Management)
http://www.acdm.org.uk/assets/DHP_Guidelines.pdf

Clinical Data Interchange Standards Consortium (CDISC) – Operational Data Model http://www.cdisc.org/odm

Guidance for Industry - Electronic Source Data in Clinical Investigations (FDA, 2013)
http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM328691.pdf

Good Clinical Data Management Practices (Society for Clinical Data Management, 2009)
http://www.scdm.org/sitecore/content/be-bruga/scdm/Publications/gcdmp.aspx

Appendix 08
CRO Audit

1.0 Introduction/Background

Sponsors may transfer any or all clinical study-related duties and functions to Contract Research Organizations (CROs). In recent years CRO usage has been increasing among sponsors for effective utilization of in-house human resources, reduction of fixed expenses and supporting sponsor's increasing business operations.

2.0 Scope

This Supplement describes CRO audits when study-related duties and functions are contracted out to CROs. For audits of other external vendors such as clinical laboratories and Interactive Response Technology (IVT) vendor audits, refer to other appendices.

3.0 Definitions

3.1 Contract Research Organization (CRO)

A person or an organisation (commercial, academic, or other) contracted by the sponsor to perform one or more of a sponsor's trial related duties and functions. (ICH GCP)

4.0 Content

4.1 Purpose of CRO audit

The sponsor, who has ultimate responsibility for the quality and integrity of clinical study data, must ensure that the services which are provided by the CRO fulfill the quality requirements of the sponsor.

While a CRO usually carries out quality assurance (QA) and quality control (QC) for the delegated tasks, the sponsor also needs to ensure those QA/QC activities, as well as the reliability of all clinical study related data and its adequate processing, are conducted according to contracted agreements.

The sponsor's QA department, independently audits the activities of the CRO as well as the CRO management activities of the sponsor's department who are responsible for delegating the tasks, and makes objective evaluations on whether the transferred duties and functions meet the quality requirements of the sponsor, in order to contribute to the reliability of the clinical data.

4.2 Timing and types of CRO audits

Appendix 08
CRO Audit

The necessity of conducting CRO audit, timing of audit, audit frequency, audit types should be determined based on sponsor's predefined audit strategies including the importance and complexity of the tasks entrusted to CRO, and risk assessments which are made in consideration of the audit and outsourcing experience. Moreover, a CRO audit does not necessarily have to be conducted onsite. Other adequate means may be used to confirm the appropriateness of CRO, e.g. audit questionnaires. Types of CRO audits include the following;

4.2.1 Pre-contract system audit (CRO selection investigation or audit)

When a sponsor conducts a Qualification Audit for selecting a new CRO prior to the final contract being signed, the candidate CRO's capability and the robustness of systems/procedures should be evaluated, in compliance with Good Clinical Practice (GCP), applicable regulations and the sponsor's standards, through a pre-contract system audit.

In general, an investigation or audit should be implemented for the system with which transferred duties and responsibilities are conducted, after closing the confidentiality agreement.

Since documents on outsourced tasks are yet to be generated, the audit should focus on the organization for transferred duties and responsibilities, facilities/equipment, Standard Operating Procedure (SOP) system, QC/QA system, and qualification and training of personnel. Furthermore, if possible, a tour of the facilities and interviews with the personnel in charge should be performed in some cases.

If the CRO has been previously used, the current evaluation of the CRO (including updates to systems and processes since the last audit) can be achieved remotely with the use of an audit questionnaire. The audit questionnaire must be completed by the CRO and responses agreed with the sponsor QA function prior to the final contract being signed.

4.2.2 Project audit during/after the implementation of outsourced tasks (Project compliance and evaluation audit)

Project audits should be conducted, during or after the implementation of outsourced tasks, to verify and assess whether the outsourced tasks executed by the CRO meet GCP, applicable regulations and the quality requirements of the sponsor.

The auditor reviews documented records of agreed outsourced tasks and confirms that an operational plan of the outsourced task is documented, operations are conducted according to the operational plan, and the outcome of the activities are recorded and reported to the sponsor. In particular, in the case of any deviations from the operational plan, it is

important for auditors to check that the reason for the deviation, narratives of influence of deviation on study results, and improvement status are reported to the sponsor. In other words, the sponsor should audit whether a cycle of "PLAN – DO – CHECK – IMPROVE" is functioning by focusing on the outsourced tasks.

Note: The sponsor should also negotiate agreement with the CRO (e.g., contract) in advance so that the sponsor can smoothly perform audits even after the completion of outsourced task.

4.2.3 Periodic system audit (Continuous CRO audit)

The sponsor should periodically carry out system audits at a frequency that may be a fixed period (e.g. once every 2 or 3 years) or based on a risk assessment approach using performance and quality metrics, on continuously used preferred CRO (e.g., CRO having Master Service Agreement with sponsor). Typically this audit includes a sample of projects of various statuses (e.g. from ongoing or completed outsourced projects), to verify whether the quality management system of the CRO is adequately operated and whether delegated tasks meet the sponsor's quality requirements. The selection of newly recruiting clinical trials is beneficial, as it allows Corrective and Preventative Actions (CAPAs) to be implemented that directly help improve the efficiency and completion of that particular clinical trial.

Periodic system audit is beneficial for efficient selection of candidates for the next outsourcing project and for efficient CRO management after delegation of tasks.

The periodic system audit is routinely conducted on site at the CRO, however if the responsibilities are deemed low risk by the Sponsor QA function, the current evaluation of the CRO (including updates to systems and processes since the last audit) can be achieved remotely with the use of an audit questionnaire.

4.3 CRO Audit Plan/Scope

4.3.1 CRO systems, facilities and equipment

An audit should be performed for all systems, facilities and equipments necessary for executing outsourced tasks. See Appendix for details of audit areas.

The contents of delegated tasks and risks should be taken into consideration when determining the audit scope.

4.3.2 CRO Project Tasks

The sponsor should assess whether the outsourced project tasks were implemented according to GCP, applicable regulations, agreed SOPs and contract terms.

The following areas may be included:

- Project Management (e.g. plans, organization, meetings, communication)
- Monitoring activities (e.g. staff training and operational processes)
- Data management and statistical analyses (e.g. staff training and electronic data processing system)
- Audit activities (e.g. audit process and the efficacy of audit)
- Clinical laboratory test activities
- Pharmacovigilance (PV) activities
- IRT(IVRS/IWRS)
- Manufacturing, storage/control and distribution of an investigational product(s)
- Medical writing (clinical study report, protocol and investigator's brochure), and others

In order to conduct an efficient audit, the sponsor should specify audit areas (scope) by taking account of the contracted responsibilities, risks identified through past audit, any risks specific to the clinical study, and presumable significant risks based on past experiences.

4.4 Preparation and distribution of audit plan, audit report and audit certificate

4.4.1 Audit plan

An auditor should prepare an audit plan according to the type of the audit. (See section 5 of "The Global Guideline for GCP Audit.")

4.4.2 Audit report

The auditor (either contracted or employed by the sponsor) reports the audit results to the responsible person of the sponsor. The responsible person of the sponsor, based on the audit results, requests the CRO and the CRO management function of the sponsor (e.g., CRO Manager) to take necessary actions such as implementation of a CAPA plan. The auditor provides necessary support to the responsible person of the sponsor such as notification of audit results to CRO, and requests action/ response, confirmation of actions, etc., in accordance with the applicable audit SOP.

Audit reports should be submitted to the responsible person of the sponsor who can actually execute corrective and preventive actions or instruct others to take corrective and preventive actions.

The auditor should receive responses to audit findings from the sponsor's auditee or the CRO in accordance with the applicable audit SOP.

When CAPA plan is executed, the auditor should follow CAPA completion based on applicable audit procedures. In the case of critical findings (classified as such based on applicable grading criteria), or when CAPA completion is not confirmed, further investigation (including a possible follow-up audit), should be implemented.

4.4.3 Audit certificate

For the preparation of an audit certificate, see section 10 of "The Global Guideline for GCP Audit."

4.4.4 In the case where the sponsor contracts out audit activities

The following documents should preferably be obtained by the sponsor's QA department in advance for review and approval, i.e., check consistency with sponsor's audit policy/procedures, adequacy of audit report contents against sponsor's standards, and appropriate resolution of CAPAs.

- Audit plan(s)prepared by the CRO
- Audit report(s)prepared by the CRO
- CAPAs prepared by the CRO

4.4.5 Audit Closure

For the audit to be completed smoothly, follow-up and audit closure should be performed in interacting with the CRO QA where applicable.

Appendix 08
CRO Audit

Table CRO Audit areas regarding Systems and/or facilities/Equipment

1. Organization and Responsibilities
1) Company Organization Structure and Related Organizations for Implementing Contracted Activities
Current Organization Chart
Current Job Descriptions
2) Job Description and Curriculum Vitae or other documents which specify qualifications of selected CRO staff member
3) Past Experience of Inspections by Regulatory Authorities and/or Audits by Clients
2. Training
1) Training System and Training Process
2) Training Records and Status of selected CRO staff member
3) Staff Qualification and Assignment System
3. SOP Management System
1) SOP Approval, Version Control Process
2) Version Control of Obsolete SOP and Records on Revision
3) SOP Deviation Management
4) SOP Training and Records
Mandatory SOP Training List and Training Records
4. Facility Tour
1) Work Place
2) Investigational Product Storage and Accountability
3) Document Storage
4) Server Room
Lock and Access Control Temperature and Humidity Management Risks of Fire and Fire-Protection/Resistance System Authorization of Server Room and Access Control (approval, inactivation of authorization and list of authorized personnel) Cleaning of facility, Management of Pest Control and Records
5. Regulatory Affairs Authorities Experience
6. Project Management
7. Monitoring
8. Pharmacovigilance/Medical Safety services
9. Data Management
10. Statistical Analysis

.

11. Investigational Product Management
12. Document Management and Archive
13. Translation
14. CSV (Computerized System Validation)
1) CSV Policy and SOP
2) Target Regulatory Requirements to be compliant
3) CSV plan, CSV report and CSV documents
4) Authorization Management and List of Authorized Users
5) ID and Password Management
6) Back up
7) IT Vendor Evaluation and Management
15. Quality Management System
1) Quality Control System and Process
2) Quality Assurance System and Process
3) Certification/Accreditation of Public Agencies
16. Information Security and Privacy Protection
Information Security Management based on confidentiality of the information
Encryption of Documents and Data for External data transfers
Training on Information Security
17. BCP (Business Continuity Plan), DRP(Disaster Recovery Plan)
Preparation for Supposed Unexpected Accidents, Mitigation Plan and /or, Contingency Plans
Drills and its Records for Supposed Unexpected Accident, and/or Actual Actions for taken for actions in accordance with the above mentioned plan
18. Management and Assessments of Sub-contracted Vendors of the CRO
19. Development of project specific document
20. Issue escalation process
21. Management oversight
22. Contracts, if applicable
23. Legal/ Insurance, if applicable

5.0 References

- International Conference on harmonization of Technical Requirements for Registration of Pharmaceuticals for Human Use (ICH). Note for Guidance on Good Clinical Practice (CPMP/ICH/135/95) 1 May 1996.

- ISO 9000:2000 Quality Management Systems - Fundamentals and Vocabulary. ISO December 2000
- ISO 19011:2002 Guidelines for Quality and /or Environmental Management Systems Auditing. ISO 2002
- Food and Drug Administration (FDA). 21 Code of Federal Regulations Part 11, 50, 54, 56, 312 and 314
- ICH Guideline – Quality Risk Management Q9
- ICH Guideline – Pharmaceutical Quality System Q10
- European laws and regulation contained in EudraLex, Volume 1-4, 9A and 10
- UK law, Statutory Instruments 2004/1031 and amendments 2006/1928

6.1 Recommended Reading

- GCP Auditing: Methods and Experience - Edited by the German Society for Good Research Practice (DGGF) 2nd edition
- COMPLIANCE PROGRAM GUIDANCE MANUAL: CHAPTER 48 - Bioresearch Monitoring, SPONSORS, CONTRACT ORGANIZATIONS AND MONITORS by FDA
- Good Clinical Practice Guide, Medicines and Healthcare products Regulatory Agency
- Reflection paper on risk based quality management in clinical trials, EMA/INS/GCP/394194/2011 Compliance and Inspection, 4 August 2011.
- GLOBAL COMPLIANCE & OVERSIGHT: A Primer on Vendor Oversight for Clinical Project Managers, FEBRUARY 2012
- GCP Quality Audit Manual: Second Edition, - Edited by James E. Sayre, Jr. Published 1990, 1994 by Interpharm Press, Inc.

Appendix 09
Audit for IRB/IEC

1.0 Introduction/Background

Auditing IRB/IEC may be somewhat challenging. The function of IRB/IEC are essentially the same, as specified in ICH-GCP principle; however, the rules on its establishment, legal status, composition, function, operations and regulatory requirements are governed by national and/or local regulations and differ on a country basis.
An auditor must be fully aware of regional requirements.

An IRB/IEC is established as various forms, i.e., in hospitals, local community, independent organization or government entity. While some countries in the EU have government run IRB/IECs, others countries such as Japan and the US do not.
Audit for IRB/IEC which is commercial, academic, or associated with hospitals, are currently frequently carried out by sponsor auditors or their designated partners (e.g., CRO).
Although auditing IRB/IEC is not always conducted, depending on geographical region, contract status or acceptance of IRB/IEC, this appendix can be applied when needed.

According to inspection outcomes by regulatory authorities like FDA, observations related to the IRB/IEC have constantly been pointed out, and in some cases, reviews conducted by the IRB/IEC have been judged to be invalid. So there is an increasing need for a sponsor to review IRB operational procedure and/or IRB operation as qualification audit or study audit.

An effective IRB/IEC plays an active, important role throughout the clinical trial by reviewing the rationale for implementing the clinical trial at the start of the study, followed by timely reviews of changes such as protocol and informed consent amendments, and continuing review of safety information. Deficiencies in IRB/IEC reviews have a significant impact on the validity of clinical trials; notably, ensuring research volunteer safety. Therefore, the sponsor should confirm compliance of IRB/IEC with the ICH-GCP and/or applicable regulatory requirements of each country. Auditing IRB/IEC is also conducted from the viewpoint of subject safety which will be reviewed by IRB/IEC. Disclosure or transparency of IRB/IEC operation will also prepare the opportunity for the improvement of IRB/IEC operation.

2.0 Scope

This Appendix describes audits for the IRB/IEC, if applicable within their geographical region.

3.0 Definitions

The following terms are to be used in this appendix to ensure that it is understood and interpreted consistently across QA groups and other functions involved.

1) Review meeting: A meeting of the IRB/IEC in which handling of the clinical trial is reviewed. The meeting is valid when a pre-specified number of members attend.

2) Expedited review: An expedited review is a procedure through which administrative matters that do not affect the conduct of a clinical trial may be reviewed and approved without convening a review meeting.
3) IRB/IEC acknowledgement: An acknowledgment of receipt issued by an IRB/IEC administrator when the principal investigator or the institution requests the review of IRB/IEC. This IRB/IEC acknowledgment ensures the submission from the principal investigator or the institution for IRB/IEC review.
4) Vote: A vote is carried out to ascertain the opinions of the IRB/IEC members after the review by the IRB/IEC. The procedures for determination of the voting method (majority or full agreement) and handling when majority is not obtained in voting are also considered as a part of the voting procedures.

4.0 Content

4.1 Audit for IRB/IEC

An audit for the IRB/IEC confirms the appropriate establishment of the IRB/IEC system and its proper operation.

The majority of objective evidence available to an auditor or audit team at assessing the IRB/IEC system is captured in formal meeting minutes or analogous form of documentation.

However, for a qualification audit of IRB/IEC, it is unlikely that an IRB/IEC would allow access to minutes or other objective evidence attesting to execution of meeting procedures. It is important to ensure a detailed assessment of meeting procedures for qualification audits of IRB/IEC.

4.1.1 Determining Conduct of IRB/IEC Audit

While audits for the IRB/IEC are standard practice in some countries and regions, they are not routinely done or accepted in other countries and regions.

Given this background, the necessity of auditing the IRB/IEC, selection of the IRB/IEC to be audited, and objectives of IRB/IEC audits (e.g. systems audit prior to study start, operation of IRB/IEC reviews on a specific study, for-cause audit) need to be considered.

It is important to emphasize the operational independence of the audit team. Subject matter experts (SME) are often recruited by QA to support an IRB/IEC audit. SME must be independent from IRB/EC process to enable the audit team to complete the audit without bias.

4.1.2 Request for Visiting IRB/IEC or Interview with IRB/IEC staff

Onsite visits to the IRB/IEC office are generally not regarded as a part of the audit scope of investigator site audits. Therefore, when auditors' plan to visit the IRB/IEC, the schedule for visiting the IRB/IEC at the time of an investigator site audit, or for an independent visit needs to be notified to the IRB/IEC in advance. In some cases, visits made for auditing purposes may be rejected by the IRB/IEC. However, it may still be possible to interview IRB secretary or staff and ask how the IRB functions. This information will help auditors in understanding the communication/process and documents exchanged between the investigator site and IRB/IEC during the clinical study.

4.1.3 Handling of Multiple IRB/IEC Review

Some clinical trials will be reviewed not only by a local IRB/IEC (e.g. hospital IRB/IEC) but also by a Central, Joint or Lead IRB/IEC. In some cases, only the Central, Joint or Lead IRB/IEC review the clinical trials. In these cases, the apportioned responsibilities of Central/Joint/Lead IRB/IEC need to be confirmed (i.e., the meaning or positioning of the Central, Joint, or Lead IRB/IEC, whether reviews will be done by affiliated hospital IRB/IEC of the PI or not).

Moreover, in case of overlap in review items by various parties, the priority of the review results (i.e., which IRB review results will take precedence), will need to be determined beforehand, and applicable procedures for this process should be in place, and adhered to. Especially, in the case of conflicting IRB review results, situations where investigator or sponsor can intentionally choose to follow preferable IRB/IEC outcomes must be avoided.

4.2 Audit Area

The sections below indicate the points that auditors should pay attention to when auditing the IRB/IEC, if applicable within their geographical region.

4.2.1 System of IRB/IEC

The system of IRB/IEC includes the responsibilities of the IRB/IEC to qualify investigators/research sites, member composition of the IRB/IEC, IRB/IEC functions/operation and retention of records (paper or electronic). The Standard Operating Procedures (SOPs) of the IRB/IEC need to include at least information required by ICH-GCP, and applicable regulatory requirement(s) of each country and region. Items described in

.

Appendix 09
Audit for IRB/IEC

Sections 4.2.1.1 to 4.2.1.8 below should be confirmed in the IRB/IEC SOPs, or in other documents, or through interviews with IRB/IEC staff.

4.2.1.1 Qualification of Investigators/Research Sites

- How the IRB/IEC ensures the participating investigators including principal investigators, and research sites are qualified to run the clinical study
  (e.g., review curriculum vitae of investigator and other necessary study staff, verify professional associations and medical licensure, or review relevant publications and training in good clinical practice)

4.2.1.2 IRB/IEC Membership

- Requirements regarding member composition (e.g. number of IRB/IEC members, areas of expertise, gender, presence of at least an independent member and a non-scientific member)
- Minimum number of attendees who must be present for the review meeting to be valid.

If information on occupations of the respective members above cannot be confirmed in documents (e.g. IRB/IEC membership list), the category of membership of independent and non-science members should be confirmed through an interview with IRB/IEC staff. The expertise of IRB/IEC scientific members should be wide ranging to cover the various types of clinical trials reviewed, e.g. Pediatrician member for Pediatric clinical trials.

4.2.1.3 Review Methods and their Criteria

- The types of review methods (e.g., convened review meeting, expedited review, no reviews but report only (at review meeting), or IRB/IEC acknowledgement only)
- The criteria and procedures to handle the items submitted by investigator or research site (e.g. initial submission of clinical trial, annual review, safety report, deviation report, administrative changes of the trials, GCP noncompliance, fraud/misconduct) to the applicable review methods

4.2.1.4 Procedures for Convened IRB/IEC Review Meeting

- Procedures for sending invitations to the IRB/IEC members and materials for the IRB/IEC review meeting

- Procedures for prior review/opinion collection
- Confirmation method of attendees on the day of the review meeting
- How to proceed the agenda
- Handling of trial staff members in the IRB/IEC attendees
- Determination of the voting method (e.g., majority or full agreement)
- Handling when majority is not obtained in voting when a majority voting method is used
- Reporting the results of the IRB/IEC review

4.2.1.5 Procedures for Expedited Review by IRB/IEC

- How to select items to be dealt as expedited reviews
- Procedures for expedited reviews (who and how)
- Procedures to notify results of an expedited review
- Reporting results of expedited reviews in next convened review meeting (if applicable)

4.2.1.6 Procedures for Handling of Safety Information in IRB/IEC

- How safety information from the sponsor or from the principal investigator is handled
- Procedures to notify the result of IRB/IEC review to the investigator

4.2.1.7 Procedures for GCP Non-Compliance, Fraud, Misconduct or Protocol Deviation

- How GCP Non-Compliance, Fraud, Misconduct, or Protocol Deviation is handled
- Procedures to issue the result of IRB/IEC review to the principal investigator

4.2.1.8 Role and Procedures of IRB/IEC Office

- Roles of the IRB/IEC Office
- Procedures on SOP management, SOP preparation and amendments
- Procedures for preparation of review materials, how to proceed the agenda in the review meeting, preparation and finalization of review meeting minutes, finalization of approval
- Procedures to record attendees of the IRB/IEC review meeting
- Retention of Records

Appendix 09
Audit for IRB/IEC

4.2.2 Operation of IRB/IEC

For IRB/IEC audits of a specific study, the IRB/IEC meeting procedures and minutes evidencing the execution of deliberations are critical to compliant GCP ensuring subject/patient safety. To this end, a review of meeting procedures and documented evidence of IRB/IEC meetings attesting to execution of procedures must be a primary focus of the audit/inspection.

The meeting minutes or documented evidence sometimes contain confidential information regarding other pharmaceutical companies. Information regarding the relevant studies should be disclosed and verified.

In addition, the followings should be verified.

- Communications between the principal investigator (and research site) and IRB/IEC from the beginning of the clinical trial are documented and retained.
- Whether a clear conclusion on approval/disapproval/suspension/conditional approval was obtained
- Whether IRB/IEC queries were sufficiently resolved
- Whether the fulfillment of condition(s) for conditional approval was achieved

4.2.2.1 List of Attendees of IRB/IEC Review Meetings

- Consistency between the attendees and the membership list (e.g., number of attendees, their areas of expertise, Gender, and presence of independent members and non-scientific members).
- Handling of clinical trial members when these persons including the principle investigator attend the review meeting
- Whether quorum is obtained or not

4.2.2.2 IRB/IEC Review and Reporting of Results

- IRB/IEC acknowledgment and reporting of results (including the completeness and accuracy of essential documents reviewed including version numbers/dates) as per the SOP
- Compliance with SOP on the administrative procedures for requesting an IRB/IEC review, communications with each member, procedures for provision of materials (internal and external members), review/discussion time at review meeting, procedures for reporting results in writing after the IRB/IEC review, and procedures for development and finalization of meeting minutes.

4.2.2.3 Handling of Expedited Review

- Compliance with SOP on appropriate conduct of expedited reviews and notifying results of expedited reviews

4.2.3 Records

Archive of documentation including IRB/IEC SOP and operational documentation, from submission documentation including materials provided to the approval documents, is important to verify proper operation of IRB/IEC. The archive should be secured and fire protection and pest control in place. Management of archive documents and storage period should be verified. If the IRB/IEC uses an electronic system, then the validation of the system also needs to be confirmed.

5.0 References

- 21 CFR Part 56
- Directive 2001/20/EC of the European Parliament and of the Council of 4 April 2001 on the approximation of the laws, regulations and administrative provisions of the Member states relating to the implementation of good clinical practice in the conduct of clinical trials on medical products for human use
- Detailed guidance on the application format and documentation to be submitted in an application for an Ethics Committee opinion on the clinical trial on medical products for human use
- MHLW Ordinance number 28 issued on 27-Mar-1997 (only Japanese)
- Bioresearch Monitoring Metrics by FDA http://www.fda.gov/downloads/ScienceResearch/SpecialTopics/RunningClinicalTrials/UCM341516.pdf
- Guidance for IRBs, Clinical Investigators, and Sponsors - IRB Responsibilities for Reviewing the Qualifications of Investigators, Adequacy of Research Sites, and the Determination of Whether an IND/IDE is Needed - http://www.fda.gov/downloads/RegulatoryInformation/Guidances/UCM328855.pdf

6.0 Recommended Reading

- GCP Auditing. Methods and Experience – Edited by the German Society for Good Research Practice (DGGF) 2nd edition
- Clinical Trials Audit Preparation: a guide for good clinical practice (GCP) inspections. – Edited by Mihajlovic-Madzarevic , Published 2010 by John Wiley & Sons, Inc.
- 2011 Good Clinical Practice: A Question & Answer Reference Guide – Edited by Mark P. Mathieu, published BARNETT EDUCATIONAL SERVICES

Appendix 09
Audit for IRB/IEC

- Guidance for Auditing Quality Systems of Independent Ethics Committees in Europe –by Nicky Dodsworth, Mary O'Flaherty,Colin Wilsher, Published 2008 by The European Forum for Good Clinical Practice