Propositions on

Remote Source Data Verification and

Remote Source Data Review

A Proposition Paper from EUCROF's rSDV/rSDR Task Force

EUCROF rSDV/rSDR Proposition Paper
Version 4.0 March 2023

Table of Contents

About EUCROF

The European Contract Research Organisation Federation, EUCROF (www.eucrof.eu), is a non-profit entity founded in 2005. It consists of members from most European countries and partner members from nearby countries. EUCROF includes CROs from 25 countries as of today. The aim is to foster high-quality clinical research. EUCROF's objectives include collaboration with clinical research stakeholders as well as European Regulatory bodies such as e.g., the European Medicine Agency (EMA) and EU Commission) to improve clinical research.

rSDV/rSDR Task Force – EUCROF

The rSDV/rSDR task force consists of representatives from EUCROF member firms, including:

Annette Pimm, Bionical Emas

Antoinette van Dijk, D.O. Research

Dagmar Chase, Clinrex Munich

Martine Dehlinger-Kremer, EUCROF & ICON

Fiona Maini, Medidata a Dassault Systèmes Company

Myrte Walenberg, IQVIA Biotech

Sara Castaños, Pharm-Olam

Silke Wendler, Labcorp

Valeria Orlova, Medidata a Dassault Systèmes Company

Vivienne van de Walle, PT&R

Yoani Matsakis, AFCROs & TELEMEDICINE Technologies

Glossary of terms

EDC	Electronic Data Capture
EHR	Electronic Health Records
eISF	Electronic Investigator Site File
EFFS	Electronic File Sharing System
EMA	European Medicines Agency
GDPR	General Data Protection Regulation
ICF	Informed Consent Form
IMP	Investigational Medicinal Product
IT	Information Technology
rSDR	Remote Source Data Review
rSDV	Remote Source Data Verification
SOP	Standard Operating Procedures

Introduction

The COVID-19 pandemic has accelerated the demand to extend the conditions under which remote Source Data Verification and remote Source Data Review (rSDV and rSDR) can be used in clinical trials. Regulatory authorities have provided guidance throughout the COVID-19 pandemic that has allowed for limited use of such approaches.

It has become apparent that wider and more permanent adoption of such approaches is highly advantageous to monitoring conduct. This is multi-faceted, considering:

a) The technologies are mature and well established and leveraged more widely in other regions such as the United States.
b) The data protection regulations are providing the grounds for adapted security and confidentiality approaches and have already been applied to telemedicine and shared information systems for health.
c) It is now widely acknowledged that risk-based monitoring combining remote approaches with on-site monitoring is more efficient than 100% on-site monitoring (both from the point of view of data quality and participant safety)[1] and is becoming a gold standard[2].

Furthermore, remote monitoring would allow for continuous verification of data which would increase the safety of participants and improve data quality, monitoring effectiveness, and efficiency.

There are actual and perceived barriers to the greater adoption of rSDV/rSDR, these being technological capabilities, data protection, data privacy, and the general alignment on security and confidentiality standards between clinical systems enabling rSDV/rSDR and those applied in normal clinical practice.

This rSDV/rSDR paper aims to discuss the propositions on the use of rSDV/rSDR within clinical research. The paper outlines insights and suggestions for consideration and use of rSDV/rSDR integration for clinical trials during and post the COVID-19 pandemic, or any other force majeure, in a way that ensures consistency, preservation of participant privacy and that does not unnecessarily increase the site burden. The purpose of the document is to obtain long-term support from regulators and the wider stakeholder community for an aligned adoption of rSDV/rSDR best practices.

[1] https://link.springer.com/article/10.1007/s43441-021-00295-8
[2] https://health.ec.europa.eu/system/files/2017-08/2017_04_25_risk_proportionate_approaches_in_ct_0.pdf

Intent of the Paper - Regulatory Landscape

It is the intent to open the discussion with the European Medicines Agency and National Competent Authorities in the EU to allow for the options of a greater degree of adoption of rSDV/rSDR.

Throughout the COVID pandemic, the EMA, HMA, and European Commission issued five versions of 'Guidance for the Management of Clinical Trials'[3]. Version 3 outlines that rSDV is to only be considered in exceptional circumstances including in line with national or temporary national emergency measures, Versions 4 and 5 broaden the permitted use of rSDV. The guidance states that rSDV can be considered only during the COVID-19 pandemic as per the guidance, i.e., related to a public health crisis, and in line with EU and National Laws, possibly even temporary emergency provisions. However, strict limitations still apply as rSDV can only be considered for certain clinical trials (Figure 1). These exemptions are limited to the pandemic period only, whereas a long-term regulatory solution would be beneficial to future high-quality clinical trial monitoring. Clearly, rSDV is classified as a highly sensitive data check and although the EMA has widened the use of rSDV during the COVID-19 pandemic, it is noted that the EMA emphasises that it must be in line with EU national laws, and there may be nuances between country laws and different interpretations.

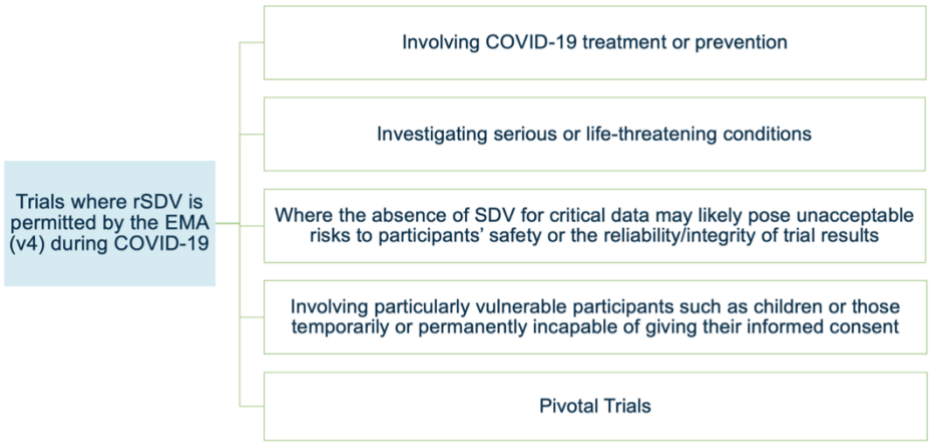

***Figure 1**: Trials where rSDV is permitted according to Versions 4 and 5 of the EMA guidance on managing clinical trials during the COVID-19 pandemic.*

The view of the rSDV/rSDR task force is that these temporary changes are considered for long-term use in the post-pandemic period and that the flexibilities are extended to all trial types to allow for a more flexible monitoring approach that would preserve some on-site monitoring and incorporate some rSDV/rSDR.

[3]https://ec.europa.eu/health/system/files/*2022*-02/*guidanceclinicaltrials*_covid19_en_1.pdf

rSDV/rSDR Task Force Propositions

rSDV/rSDR Propositions outlined by the Task Force within this document address the following topics, as seen in Figure 2.

***Figure 2**: rSDV/rSDR Task Force Propositions as outlined in this paper*.

Definitions & Key Concepts

Source Data Verification (SDV) & Source Data Review (SDR)

Traditional monitoring tasks of a clinical trial are performed physically on site. Within this context, ICH E6 R2 [4] refers to "source data", "source documents", and available for review. ICH E6 R2 does not specify the differences between source data verification (SDV) and source data review (SDR). Since SDV and SDR are different processes, it is important, in view of this paper, to define what is meant by SDV and SDR to appreciate the differences between the two.

SDV, commonly known as 'transcription checking', is defined by TransCelerate as "the process by which data within the CRF or other data collection systems are compared to the original source of information (and vice versa) to confirm that the data were transcribed

[4] https://www.ema.europa.eu/en/ich-e6-r2-good-clinical-practice

accurately (data from source matches data in the CRF or other system and vice versa)"[5]. For instance, some typical SDV tasks include checking that essential endpoints have been accurately transcribed from the medical records of the site in the corresponding CRF and completing the appropriate section of the monitoring visit report with the result of this control work.

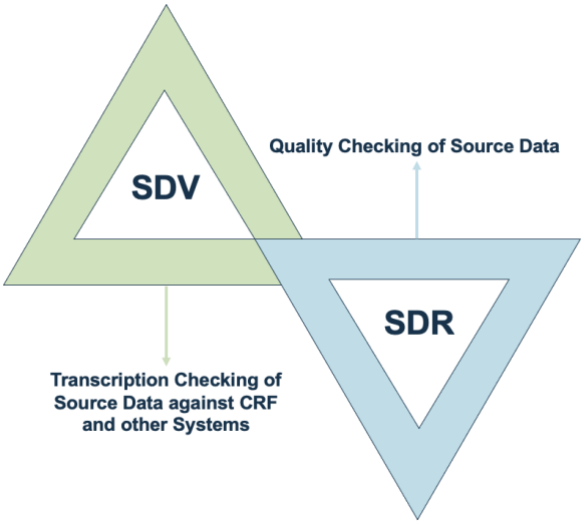

***Figure 3**: Schematic representation of the summary of the fundamental difference between SDV, source data verification, and SDR, source data review. for more information, see the definitions in this section.*

SDR, Source Data Review, is defined by Transcelerate[5] as "a review of source documentation to check the quality of the source, review protocol compliance, ensure critical processes and source documentation are adequate" e.g. ALCOA-C: Attributable, Legible, Contemporaneous, Original, Accurate, and Complete, "SDR is not a comparison of source data against CRF data", but intends to ascertain Investigator involvement and appropriate delegation, and assess compliance to other areas (e.g. SOPs, ICH GCP for pharmaceuticals, and ISO14155 GCP for medical devices clinical investigations). For instance, checking the existence of the signed informed consent of the enrolled trial participants and compliance with the trial protocol is an SDR task, the outcome of which will be included in the monitoring visit reports. Another example would be verifying that each trial procedure has been performed by a person who is qualified and who has been appropriately delegated to do so by the Principal Investigator.

Remote SDV and SDR

rSDV/rSDR opens the opportunity for an alternative model for monitoring. Thus, remote SDV/SDR does not have a fundamental difference from the on-site option in terms of efficiency

[5]http://www.transceleratebiopharmainc.com/wp-content/uploads/2016/01/TransCelerate-RBM-Position-Paper-FINAL-30MAY2013.pdf.pdf

and effectiveness. In both on-site and remote monitoring, the efficacy and effectiveness of monitoring depend on the follow-up of monitoring observations determined by the sponsor or their CRO. Hence effective follow-up determines how impactful monitoring was, irrespective of whether the monitoring was on-site or remote.

Data Protection & Health Data

Personal data which includes health data is sensitive (GDPR Rec. 10, Art. 9(1)) and access is regulated by applicable laws to ensure the protection of the rights of the data subjects. The provision of IT solutions involving the hosting of this data should therefore be carried out under data protection (security and privacy) conditions suited to their sensitivity.
In the EU, the provision of such services should comply with Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons concerning the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (also known as GDPR – General Data Protection Regulation).

Remote SDV/SDR does not have a fundamental difference from the on-site option in terms of efficiency and effectiveness. As with onsite monitoring activities, IT systems used to perform rSDV/rSDR should have appropriate data protection safeguards to ensure the privacy of participant health data. rSDV calls for additional mechanisms in place to protect participants' personal data and identity. This is an introductory section, and the propositions outlined in the document cover more detail on the topic.

Technology Enabling rSDV/rSDR

There are already established processes and technologies that are proven within the industry to support rSDV/rSDR. The wide adoption of solutions for the electronic management of clinical studies and the ongoing digital transformation of the health systems makes it possible for monitors to accomplish most SDV/SDR tasks remotely and not necessarily be physically present on site. Furthermore, ICH E6 (R3)[6] "Guideline is intended to be media neutral to enable the use of different technologies", and therefore demonstrates an industry step in the direction of the positive acceptance of clinical trial technologies.
Three key classes of existing IT tools currently already in use (Figure 5), could be envisaged for this purpose, (see Appendix 1 for more details on technology).

[6]https://database.ich.org/sites/default/files/ICH_E6-R3_GCP-Principles_Draft_2021_0419.pdf

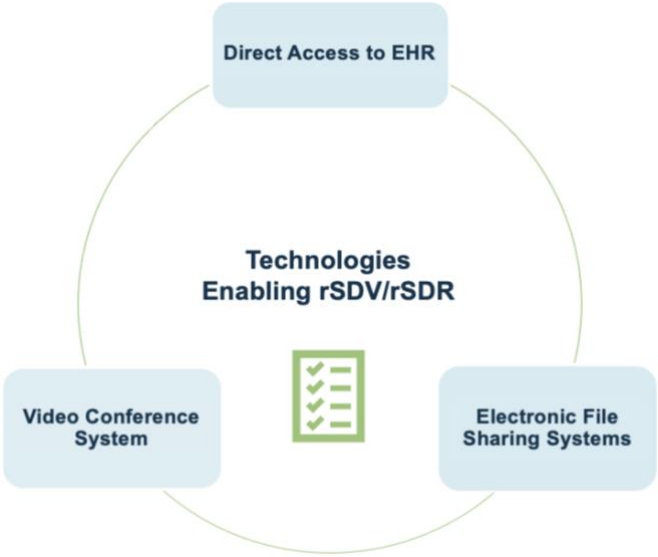

***Figure 5**: Existing technologies that enable* rSDV/rSDR*.*

Under current state-of-the-art, Electronic Health record (EHR) systems are operated under the direct responsibility of the sites, (the system is hosted on the IT facilities of the hospital/site, and assurance that the systems are compliant with national laws and health technology standards is the remit of the hospital.)

Management of the EHR system is performed by an internal IT team or a dedicated contractor, the software maintenance is performed by the software developer from which a usage licence is purchased by the site). The situation might be different when considering other technology solutions that are built specifically to enable remote data review with all required functionality, like redaction, role-based and limited time access, and security safeguards (see Figure 5). These enable rSDV/rSDR, as they are more likely to be provided as a service by specialised IT Vendors (or "Service Providers") under contractual schemes. However, it is important to mention that the responsibility for the handling of participant's personal health data (source data) remains with the site (see Proposition 3). This investigator's responsibility extends to trial participant source data that is generated by the investigator/ institution on site and outside of the investigational site. The sponsor bears the responsibility for ensuring that systems used for source data generated by the participant via ePRO or wearable devices, generated by central facilities and service providers meet the necessary requirement of privacy and security. The EMA recommends that "the investigator should have the possibility to ask for any additional information in order to perform due diligence and to require any change to the agreement or to the service when considered necessary, including the possibility to reject a certain service provider."[7]

[7] https://health.ec.europa.eu/system/files/2022-12/mp_decentralised-elements_clinical-trials_rec_en.pdf

The investigator is responsible for reviewing data that can have an impact on safety or clinical decisions and assessments of the participant, whether the data is collected on site or elsewhere. Therefore, the handling of source data responsibility also applies to source data that is generated by the participant through ePRO entries or wearable devices generated data, as well as central facilities and service providers-derived source data, such as central diagnostics and laboratories.

Going forward permission for monitor access should be a standard procedure and integral to trial planning and risk assessment. The IT system design should, in an ideal case scenario, allow for a monitor to have limited access, ideally should be restricted to only the relevant clinical trial participants and accessibility is fully auditable. In reality, not all site IT systems had already been established with the functionality that would enable remote monitoring, so adaptations would need to be catered for. Typically, a research site facility already has an established IT system design, which in the past has not been designed with remote monitor access functionality in mind. Thus, for sites with established IT systems in place, remote monitor access functionality would need to be an addition implemented downstream of the creation of the original IT system. It is important to be aware of the investigator/ institution's responsibility for ensuring data security and confidentiality of the source data at the site.

The following terms and underlying concepts will be used in the subsequent sections of this document and are important for a good understanding of the interplay between the delivery chain of technology solutions and security and confidentiality requirements.

Service Providers for Clinical Research

A Service Provider for Clinical Research is a natural or legal person (including commercial, academic, and non-profit) that provides services to sponsors or investigators on a contract basis and within the scope of clinical research (experimental or observational) as well as other activities in connected domains.

This definition is inclusive of all types of "Service Providers" in the domain of Clinical Research. It includes providers of IT solutions, such as EDC vendors and vendors of all types of information systems that are dedicated to Clinical Research and have to comply with industry-specific legal provisions.

This definition has initially been created and approved by EUCROF in 2017 to define the term "CRO – Contract Research Organisation" and was responding to the need to modernise the term CRO considering the growing importance of IT Services in Clinical Research. This definition combines three key aspects: the "delivered service", the "contractual relationship" between the involved parties, and the "domain-specific" regulatory landscape. All 3 are essential when considering security and confidentiality measures and responsibilities. Within the scope of this paper, the following 2 classes of services are of interest.

Provision of IT Managed Services

Provision of IT managed services refers to the process of delivering all administration and management services required to maintain a software solution fully operational according to the terms of the Service Contract to a client. The developer of the source code and executable code of the software solution can be a third party, as well as the provider of the IT infrastructure. In all circumstances outlined in this paper, EMA's draft guidance on computerised systems and electronic data should be taken into account for the evaluation of eligibility and compliance of IT Managed Services[8].

Examples of IT solutions that can be delivered by Service Providers for Clinical Research under Service Contracts are the following:

- EDC systems that can be accessed by investigational sites, CROs staff in charge of monitoring and/or data management as well as Sponsor's mandated staff and other involved parties;
- Shared Platforms;
- Interactive Web Response Systems (IWRS);
- Electronic Participant Reported Outcome (ePRO) solutions;
- Electronic Trial Master Files (eTMF/ISF) solutions etc.

Provision of Physical Hosting Infrastructure

Provision of physical hosting infrastructure refers to all processes required to deliver to a client the necessary physical resources to host a software solution, such as secure data centre facilities, including processing capacity, data storage space, internet connectivity, as well as possible virtualisation technologies, and/or management resources.

Such services are to a large extent 'domain agnostic', and physical infrastructure can be implemented 'on premises' by a corporation or a site. However, continuity of service, security, and confidentiality challenges are such, that the demand for the provision of Infrastructure as a Service or "virtualised data centre services" is growing and some countries throughout the EU member states have now developed standards (largely based on ISO 27001) or even certification processes for the delivery of such services when they are purchased for the delivery of IT solutions hosting health data. Service providers delivering IT Managed Services may purchase such physical hosting infrastructure from third parties.

[8]https://www.ema.europa.eu/en/documents/regulatory-procedural-guideline/draft-guideline-computerised-systems-electronic-data-clinical-trials_en.pdf

Task Force Propositions for Consideration

Proposition 1: On-site and Remote SDV/SDR

Determination of the mix of on-site and remote rSDV/rSDR on a case-by-case basis.

A risk-based approach is fully supported by ICH E6 (R2), as well as the EU guidance document on proportional approaches in clinical trials[9], and ISO 14155:2020[10], and can result in a mix of key activities targeting the individual needs of the sites and/or taking into account the specifics of a given clinical trial. A combination of on-site and remote monitoring can be tailored according to a risk-based approach, appropriate for high-risk and first-in-human trials, as well as lower-risk trials. Centralised monitoring, a key remote strategy, will support risk identification by comparing site data regarding prior identified risk factors, e.g., premature terminations or serious adverse events. Remote SDV and SDR allowing quality control independent of a physical visit will supplement or even fully replace on-site activities, depending on the trial and site risks. Finally, statistical sampling of data to be monitored should be mentioned. Such trials will show a very high number of data points and quality should be assured by applying preferably risk-based sampling strategies.

The risk-based approaches support the focus on critical-to-quality factors to ensure subject safety and data quality are protected throughout the clinical trial life cycle. The quality of the trial data can be improved by identifying, assessing, monitoring, and mitigating risks[11].

It is believed that for the majority of clinical trials, the most effective approach is to enable a mix of on-site and remote SDV/SDR techniques. On-site visits would not be fully excluded but will continue to take place as per the trial-specific monitoring plan and requirements. In many trials, rSDV/rSDR cannot fully replace certain on-site assessments and will still be needed. A combination of on-site monitoring and remote monitoring can be an advantage also for high-risk sites and trials, for example, first-in-human. Understandably, on-site monitoring is necessary for these trials, but for the data in between on-site monitoring periods, remote SDV/SDR can be an advantage as well.

A determining factor in the appropriateness of remote monitoring methodology for a specific trial would be access to the EHR system on site and the existing infrastructure. In

[9] https://www.google.com/url?q=https://www.gmp-compliance.org/guidelines/gmp-guideline/eudralex-volume-10-risk-proportionate-approaches-in-clinical-trials&sa=D&source=docs&ust=1649330520348117&usg=AOvVaw3ZcZP6xxd2nvlIEMMHnRy6

[10] https://www.iso.org/standard/71690.html

[11] https://www.ema.europa.eu/en/documents/scientific-guideline/reflection-paper-risk-based-quality-management-clinical-trials_en.pdf

circumstances where the site operates in a paper-based system, remote monitoring may not be as appropriate for circumstances outside force majeures.

Conversely, there can be trials or situations where sole rSDV/rSDR is acceptable taking the safety of the monitor, site staff, and trial participants into consideration, such as pandemics and other specific situations. Under standard conditions, not subjected to force majeures, the implementation of sole rSDV/rSDR on a clinical trial would be dependent on the extent to which identified risks to trial conduct and data quality and reliability can be appropriately controlled, as well as the assessment of the potential burden to the investigator, which should be minimised irrespective of the mode of monitoring selected, where it is on-site, remote, or centralized[12].

Proposition 2: Security & Confidentiality Standards

The provision of IT Managed Services for the purpose of rSDV/rSDR is proposed to comply with data protection security and confidentiality standards providing the same or comparable level of protection as standards applicable to telemedicine systems.

Under no circumstances should the deployment of rSDV/rSDR downgrade security and confidentiality compared to the current practice of "on-site monitoring". The identification of acknowledged standards for security and confidentiality management applicable to IT Managed Services for rSDV/rSDR is therefore of utmost importance.

As no IT Managed Service is in use for on-site monitoring, other application areas need to be considered to identify the right standard.

ISO Standards, such as ISO 27001 & ISO 27002 or, with their GDPR extension, ISO 27701 could be considered, but, in the absence of a broad harmonised approach between the Data Protection Authorities of numerous countries (see also proposition 8), this could be over-prescriptive.

This is why the proposed approach is to take as a "reference" a domain where IT Managed Services also play a central role, with an already worldwide adoption, and that shares the same requirements in terms of data protection and related security and confidentiality management. There may be different standards from one country to the other, but all countries are adopting policies and systems for a wide deployment of telemedicine solutions for example.

The main conclusion of this proposition is that, in all concerned countries, IT Managed Services for the purpose of rSDV/rSDR via videoconferencing can be delivered under data protection standards comparable to those already accepted for the telemedicine platforms

[12] RECOMMENDATION PAPER ON DECENTRALISED ELEMENTS IN CLINICAL TRIALS Version 01, 13 December 2022, EMA, European Commission, Heads of Medicines Agencies.

operated in these same countries. Therefore, data protection issues in the context of deployment of rSDV/rSDR solutions are not posing an insurmountable obstacle.

Proposition 3: Management of Access to Source Documents

Regardless of the chosen rSDV/rSDR solution, management of access rights to source documents remains under the exclusive and full control of the investigator/institution.

The IT solution for rSDV/rSDR should be implemented under the control of the investigator/institution**.** The institution's relevant IT department and data protection experts should be involved in the process. It is the responsibility of the investigator at the site to grant direct and controlled access to the monitor for the systems where the source documents and records are maintained. For example, if a file-sharing mechanism is used for image transmission or screens are shared showing source data, this happens under the responsibility of the investigator/ institution at the site. Access to source documents should be time-restricted, and, if technologically possible, also participant-restricted for monitors. If participant-restricted access is not supported by the technology used, then a 'permission to access' form has to be completed where the site grants access and the CRA confirms that only trial subjects' files will be reviewed. Access would be revoked when a CRA changes, or the session expires. The site will ultimately be responsible for granting and revoking access to data. Follow-up queries post-monitoring visits should also be considered and addressed.

Eligible solutions would include built-in audit trails enabling sites to check post-visit that the granted accesses have been used according to agreements. Such audit trails will also be used in case of audits. It is to be mentioned that on-site monitoring may not provide such traceability capabilities.

In summary, eligible rSDV/rSDR solutions should have "by design" features (user management under the control of sites, audit trail accessible to mandated site and other personnel, time restriction mechanisms) ensuring that sites can effectively exercise their full control over granting access to the monitors to the records of interest for their monitoring tasks. Various approaches could be applied to ensure that the investigator/institution is able to verify the monitor's identity at the start and during a remote monitoring session. Access should be requested in advance in a user-based manner with credentials to allow for secure identification equivalent to those standards suitable for other remote practices.

Proposition 4: Eligible Service Providers

IT Managed Services for the purpose of rSDV/rSDR can be provided by Service Providers contracted by the Sponsor of a trial, as long as the delivered service complies with the requirements resulting from propositions 2 and 3 above.

Any Service Provider of a technology that permits rSDV/rSDR is eligible to provide their system for use in a clinical trial, as long as the system would comply with the conditions outlined previously, concerning security & confidentiality standards (Proposition 2) and management of access to source documents (Proposition 3), and is appropriately validated for the intended use.

Proposition 5: Source Documents Redaction for rSDV/rSDR

Redaction of source documents does not happen during on-site visits and therefore would not be a requirement for rSDV/rSDR if the technology used guarantees security and privacy compliance.

With technology that is fit-for-purpose and is compliant with acknowledged standards to ensure privacy and security, as well as the monitor being contractually obligated to not take screenshots or photos of the source data or allow others to view the data on the screen, there is no need to additionally task the site with the redaction requirement, which does not exist for on-site monitoring visits. If the right security and quality management systems are installed, the concern for privacy breaches is further mitigated, making redaction redundant and not consistent with ALCOA-C principles, as attributability cannot be assured.

Ultimately, the technology used for monitoring will be the determining factor in the decision for redaction. In the case where source documents leave site technology, they would need to be redacted, and thus re-monitoring might be advisable later. In the instance where the source documents are not leaving the site technology, redaction would not be necessary, and furthermore, re-monitoring would also not be needed afterward.

Proposition 6: Acceptance and Adherence by Investigator/Institution

When the IT Solutions are proposed under the Sponsor's responsibility, mechanisms would be envisaged to ensure that the investigator/ institution can accept the corresponding technical and organisational measures in a fully informed, transparent, and independent manner.

rSDV/rSDR cannot be implemented without the prior agreement of the investigator/institution. The institution’s relevant IT department and data protection experts should be involved in the process. When the IT tools that are intended to be used in a clinical trial are proposed by the Sponsor and are delivered in the context of IT Managed Services, as this can be expected in a significant proportion of cases, the question of how Sites can accept and sign the agreements with sufficient knowledge of the included technical and organisational measures arises.

The suggestion is that adherence to the proposed IT services & solutions to appropriate and acknowledged standards are transparent and publicly acknowledgeable, providing sufficient trust and contractually binding safeguards to all involved parties, in particular for the Site

institution. This would be of ultimate importance to enable a wider and quicker acceptance of rSDV/rSDR for Sites that are involved in a large number of clinical studies with multiple Sponsors. In this respect, see Proposition 9 hereafter.

Investigators are medical professionals and not IT or data protection experts. Therefore, the required involvement of IT and data protection experts should be addressed in this section. See also Proposition 6 below.

Proposition 7: Complete Re-monitoring of rSDV/rSDR

Complete re-monitoring following the completion of rSDV/rSDR would only be needed subject to risk analysis based on data criticality.

The EMA COVID-19 Guidance for Clinical Trials mentions that data that is monitored using rSDV, "in particular if it was based on pseudonymised documents", and the EMA suggests "that remote monitoring is expected to only have focused on the most critical information", and is likely to require re-monitoring.[13] The need for re-monitoring if rSDV and rSDR have been performed with the necessary safeguards when performed on unredacted source documents does not seem necessary. Complete re-monitoring would be quite inefficient and involve additional work for Sites and CRAs. When using rSDV/rSDR procedures, sponsors should ensure that they are fit for their particular purpose and thus can be considered equivalent to on-site SDV/SDR.

There are some scenarios when the remote monitoring infrastructure involved source documents leaving the site systems, and hence requires redaction, where re-monitoring may be applicable according to a risk-based approach on the criticality of the data.

After risk analysis as well as analysis of the technical capabilities of the sites involved, the sponsor should ensure that the selected rSDV/rSDR procedures quality is equivalent to on-site SDV/SDR

Proposition 8: Towards a Harmonised Approach in the EU & Beyond

The adoption of rSDV/rSDR would be highly facilitated by a harmonised approach throughout the EU Member States Data Protection Authorities and beyond about the security and confidentiality standards applicable to the provision of IT Managed Services for that purpose.

Regulatory requirements in the context of rSDV/rSDR can differ widely from country to country. For example, some national health authorities require rSDV/rSDR procedures to be explicitly

[13] https://ec.europa.eu/health/sites/default/files/files/eudralex/vol-10/guidanceclinicaltrials_covid19_en.pdf

outlined in the Informed Consent Form (ICF), while others state that this is not necessary. For global studies to be successful, a level of harmonisation of the rSDV/rSDR requirements would be highly beneficial. Some countries, like the USA, take a more general approach, where monitoring and SDR/SDV are included in the ICF, but the method of access of the documents, remote or on-site, is not specified, allowing for greater flexibility and adaptation for global trials.

In order to increase the adoption of rSDV/rSDR use in clinical trials in the EU region, as well as globally, a harmonised regulatory approach for the protection of personal data but also IT security (see Proposition 2) would be greatly beneficial. In particular, a collaborative approach agreed by EU Member State Data Protection Authorities on the requirements for security and confidentiality standards for rSDV/rSDR technologies would be highly effective (see Proposition 2). In addition, to also cover global clinical trials, the Task Force is of the opinion that the topic of rSDV/rSDR should also be addressed on an ICH level, e.g., within the project of GCP Renovation, which is underway.

Taking the GDPR as the highest guiding principle, it becomes clear that it is well-suited to enable rSDV/rSDR. Indeed, Article 5(1)(d) of the GDPR includes 'accuracy' as a principle for lawful personal data processing, which rSDV/rSDR directly facilitates[14] . The European Data Protection Board (EDPB) has planned for further guidance later this year on how to comply with GDPR in the context of scientific research[15]. In anticipation of that guidance, several existing mechanisms in the GDPR would facilitate harmonisation between EU Member State Data Protection Authorities in how to apply the GDPR's requirements to rSDV/rSDR.

The provisions under Article 35 call for formal data protection impact assessments "in particular using new technologies" that may present a risk to the rights and freedoms of data subjects. The development of a Data Protection Impact Assessment (DPIA) template based upon best industry practice, for example, can enable Member State Data Protection Authorities to align on the risk assessment and mitigation for new rSDV/rSDR technologies.

In a similar fashion, the use of Prior Consultation under Article 36 of the GDPR provides an opportunity for clinical trial sponsors to attain certainty around the data protection controls undertaken while using rSDV/rSDR. Articles 60, 63, and 70 of the GDPR encourage Member State Data Protection Authorities to cooperate with one another and with the EDPB in order to provide consistent advice to controller sponsors who are implementing rSDV/rSDR in their trials.

Finally, the provisions under Articles 40 and 41 of the GDPR in respect of codes of conduct ("codes") provide another such framework for a cooperation mechanism between all Data Protection Authorities throughout the 27 EU Member States Data Protection Authorities.

[14] "Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay" GDPR Article 5(1)(d).
[15] *See* Para. 3, "EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research." Adopted on 2 February 2021. Available at: https://edpb.europa.eu/our-work-tools/our-documents/other-guidance/edpb-document-response-request-european-commission_en

Details can be found in the EDPB Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, Version 2.0, 4 June 2019.[16] In section 8.3, the EDPB Guideline defines the cooperation mechanism between the DPAs for the approval of codes.

In summary, the Task Force can only encourage the stakeholders to activate these various existing mechanisms to achieve harmonisation within the EU and beyond, and provide a practical, transparent, and cost-effective framework enabling wider adoption of IT Tools for rSDV/rSDR.

Additional Considerations

A Staggered Implementation of rSDV/rSDR

As per ICH GCP 5.8.13, the sponsor should determine the appropriate extent and nature of monitoring. Many aspects that determine the extent and nature of rSDV/SDR should be performed considering the impact on sites with care to reduce/limit site burden as much as possible while maintaining participant safety, data integrity, and confidentiality of personal data. In particular, direct access to EHR is the preferred option for mitigating site burden due to the minimal impact on normal site activities. The Sponsor should clearly define what needs to be monitored during the trial, identification, and assessment of critical trial processes and data to be flagged as causing a potential risk, identify the expected, acceptable values and parameters, and what RBM approaches are appropriate for the trial. This can be a combination of risk-based monitoring approaches such as on-site monitoring, targeted SDV/SDR, centralised statistical/data monitoring, rSDV/rSDR as examples. It is important to assess the SDV and SDR that needs to be performed on data, furthermore, the data quality would also need to be assessed. A risk-based approach may, in certain trials, leverage various tools, platforms, and dashboards to identify signals, which indicate potential issues with trial conduct, participant safety, data integrity, and protocol compliance. This allows the trial team to concentrate on high-value tasks and focuses resources on specific trial-related matters.

Site-specific Feasibility of rSDV/rSDR

It is important to consider what method or methods the site can use to make its source data available to the monitor. The site will use different options, this may vary by country, and some potential considerations may include:

- Direct controlled access to the restricted / relevant part of the electronic medical records of the participants involved in the trial.
- Upload certified copies via a secure portal or a location hosted by the site.
- Ability to upload a scan of their source records certified copies into a secure location owned/hosted by the Sponsor / CRO / Vendor. In the cases where there is a requirement for the documents to be redacted, they should be identified only with the

[16] "[Codes] can help to bridge the harmonisation gaps that may exist between Member States in their application of data protection law."

trial participant trial number (ICF exemption outlined below). This could be performed using normal query management and would deliver an audit trail.

- Video review /Video conference capability. This would need to be used sparingly, as it is a burden to Sites, but would allow verification that participants really exist and remotely perform SDV & SDR on the ICFs. It would also be suitable for use of verification of Investigational Product accountability.
- The burden of the introduction of alternative measures on the site staff and facilities should also be considered, including the potential burden of uploading source documents in a secure site-controlled platform, and a proportionate approach should be taken, balancing appropriate oversight with the capacity of the site[12].

Site Staff and Monitor Training

This section on training is not exhaustive and will vary depending on country requirements, organisation, and trial.

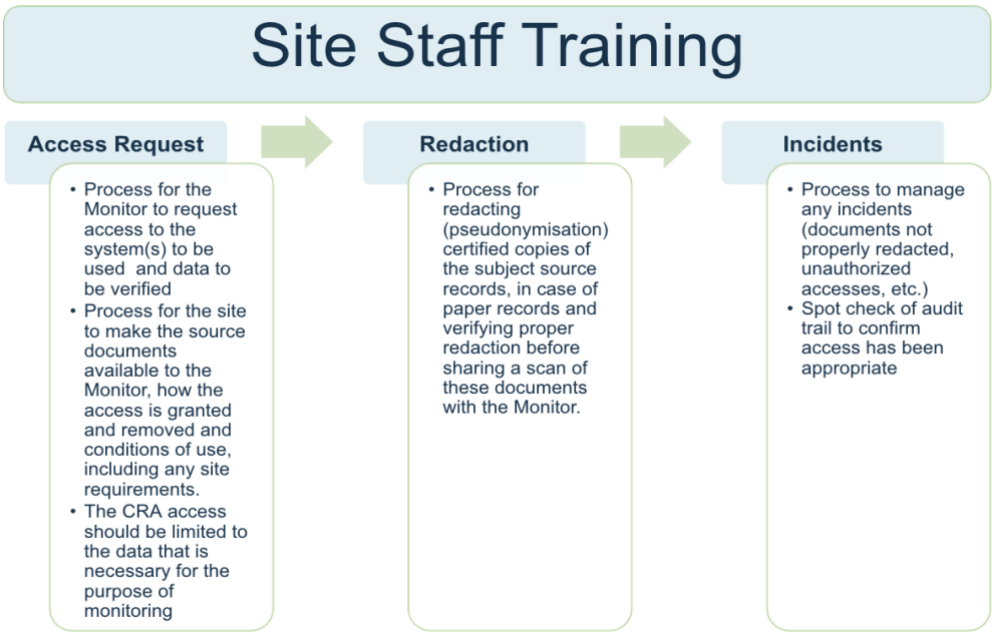

***Figure 6**: Site Staff training aspects for rSDV/rSDR*

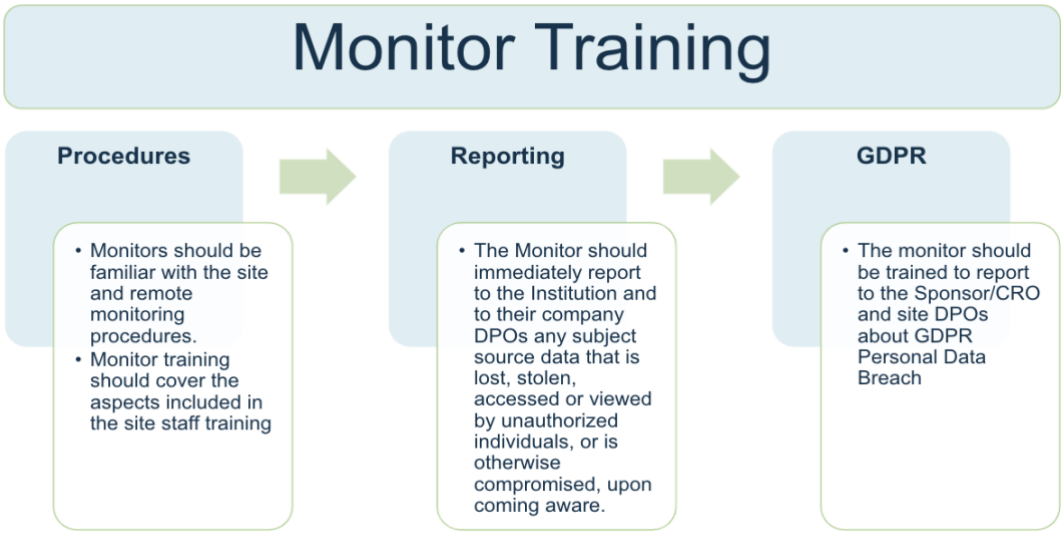

***Figure 7**: Monitor aspects for rSDV/rSDR*

Documentation Submission of rSDV/rSDR

The monitoring strategy would be documented within a required document for regulatory submission depending on the local requirements.

Information on Audits

Whereas the risk-based approach to monitoring was only promoted in ICH GCP [R2], audits have been guided by risk factors from the very beginning. Quality Assurance (QA) activities are targeted, for example, at important trials for submissions (e.g., pivotal trials), high-impact investigator sites (e.g., high recruiters), critical data points (e.g., primary endpoints, SAEs), etc., and are as well driven by risks inherent to the investigational medicinal product (IMP), trial procedures and condition of trial participants. QA resources (auditors, inspectors) are more limited than Quality Control (QC) resources (e.g., monitors, data managers) - therefore a risk-based approach is the only way to cope with the giant task to review the protection of trial participants and the reliability and robustness of trial data. With time, we have learned that the targeted risk-based approach is also applicable to QC activities like monitoring and might even result in better quality than the very cost-intensive 100% approach (well respecting that in early phases and certain complex situations (e.g., use of ATMPs) a 100 % approach might be the right strategy).

Based on the above, monitoring and auditing are following similar risk-based approaches, however, the number of human resources and site contacts will still differ. In terms of methods used, for example switching from on-site to remote activities, we sense reluctance with respect to Investigator Site audits This is understandable, given the fact that often there is only a one-time chance for audits We think that remote rSDV/rSDR is not fully replacing the need for on-

site visits, therefore auditors and inspectors will want to get the full picture of on-site conditions by visiting the sites. In monitoring, usually offering multiple chances for site contacts, the mixture of on-site and remote activities is highly suited to reach both, high quality and cost efficiency. Additionally, the monitoring strategy is adaptable (e.g., in the case that significant flags of concern are raised, the frequency of on-site monitoring /extent of rSDR/SDV may be increased).

Conclusion

A trend for risk-based monitoring has been outlined and the concepts of rSDV/rSDR were explained. An optimal solution for certain trials could be a custom mix of on-site and remote monitoring including rSDV/rSDR, which would be made possible by existing technologies for clinical trials, such as direct access to EHR, video conference systems, or electronic file sharing systems. The support from Regulatory Authorities for rSDV/rSDR to become best practice would be paramount. There is potential for future incorporation of rSDV/rSDR into the 'Guideline on computerised systems and electronic data in clinical trials'[17] being published by the EMA, as well as into ICH GCP E6 (R3) with its significant update to monitoring approach. Furthermore, a risk proportionate approach to monitoring is outlined by the EU CTR, allowing for a combination of remote and on-site monitoring[18].

[17]https://www.ema.europa.eu/en/documents/regulatory-procedural-guideline/draft-guideline-computerised-systems-electronic-data-clinical-trials_en.pdf
[18]https://ec.europa.eu/health/sites/default/files/files/eudralex/vol-10/2017_04_25_risk_proportionate_approaches_in_ct.pdf (See section 4.4)

Appendix 1- Additional Information

Technology enabling rSDV/rSDR

Remote access to electronic health records (EHR)

A site equipped with an EHR system has the capability to make health records (i.e., source data) accessible to the clinical research monitors through "electronic" and "remote" means. In fact, this is already current practice with on-site monitoring: monitors are granted access to the EHR, from a workstation of the site, as long as they are performing their monitoring visit. This should be the preferred standard for rSDV/rSDR.

When the site is equipped with an EHR system, there is no other way than granting the monitors electronic access to the system, from a workstation of the site, even if EHR systems are, to our knowledge, only rarely designed to allow such access limited to the records of interest. However, contractual conditions to which monitors are bonded include confidentiality clauses, and there is the availability of an audit trail, both of which safeguard the system.

Access to the EHR, is only one part of the solution to perform a full rSDV/rSDR protocol. In addition, there are strong regional differences: the deployment status of EHR significantly varies from one EU country to the other, or even between sites within one country. However, the digital transformation of health systems is a fundamental and irreversible trend, and this trend is a favourable mid-term driver to the widest adoption of rSDV approaches with EHRs.

Electronic File Sharing Systems (EFSS) for rSDV/rSDR

Site documents can be uploaded on an IT Platform that can be accessed by representatives of the sponsor in charge of monitoring, on a need-to-know basis, and with the appropriate audit trailing as well as access rights management functionalities, including time-restricted access.

In the view of the task force, such systems can hardly be "general purpose" file-sharing systems and require the implementation of clinical research-specific functionalities, in relation to SDV and SDR. It might be necessary to use such general-purpose systems as an alternative to rSDV/rSDR IT solutions when Medical Records are still managed on a paper basis. Also, for ICF where wet-ink signature is still required; or when Medical Records and other documents (for example, medication accountability records) are electronic but it is not possible to grant remote access to the CRA. In this case, a scanned certified copy of these records needs to be generated by the site, and current requirements necessitate the documents to be redacted in order to hide the full names or other directly identifiable data (e.g., telephone number, social security number, email, etc.) and there should be appropriate operational procedures for this purpose. Re-monitoring on-site would then be necessary.

Clinical trial-specific technology solutions specific to rSDV & rSDR are available on the market today which were purpose-built as a result of the COVID-19 pandemic. These fit-for-purpose systems facilitate rSDV and rSDR workflows with capabilities to upload source documents.

Video Conference Systems

The video review of documents may include site staff sharing the screen of their computer with the monitor using a secure video conference application hosted on their device or sharing paper documents showing them through the camera. Some important aspects to fulfil when performing rSDR/rSDV through a videoconference include:

- Video review and/or screen sharing of medical records of trial subjects are granted only with authorised site team support, without sending any copies to the monitor and without the monitor recording images or taking screenshots during the video review.
- The monitor should not request the site to upload documents to the video conference chat.
- The quality of the video should be adequate to enable reading, without the risk of confusion between similar characters, and to avoid a negative impact on the visual health of the monitors.
- The transmission of the data should be adequately protected against unauthorised third-party access. The technology solution should store the videoconference data within the EU for EU countries (this refers to the actual details of participants, time, etc. of the conference). There should also be end-to-end encryption included.
- For videoconferencing when there is the possibility for the Monitor to see site personnel, their consent may be necessary prior to enabling the camera.
- The site team, or at least some mandated representatives, should be present throughout the whole duration of the videoconferencing session.
- Source data is not leaving the site location during a videoconference-facilitated rSDR/rSDV
- Showing source documents to the camera during a videoconference can be very time-consuming for the site and should be minimised only to very essential documents such as ICF and critical data and processes based on the protocol and trial design.

Video conferencing systems could be combined with EFSS systems, but in this case, the EFSS should implement all required features for such systems, as outlined in the previous section, and the video conference system should not be used as a workaround of an EFSS.

The point of view of The Task Force is that videoconferencing systems that will be embedded in IT solutions dedicated to monitoring purposes are the only viable solution for the regular use of videoconferencing systems in the context of remote SDV & SDR.