chaucer...

LIFE SCIENCES

iMATCH Work Package 4

Data Stewardship Scope Document

Prepared for : iMATCH stakeholders

Written by : Stephanie Roberts

Date/Version : 22nd May 2018/Draft v1.4

chaucer...
LIFE SCIENCES

Contents

1. Introduction

iMATCH (Innovate Manchester Advanced Therapies Centre Hub) is an Innovate UK funded collaborative project focused on scaling up the production and availability of Advanced Therapy Medicinal Products (ATMPs), a novel T-cell therapy for cancer treatment. This therapy is currently too costly to be able to deliver on the NHS at scale but offers unprecedented promise.

The project is a collaboration of 12 partners connecting the supply chain sector, manufacturers, academic sector, clinical sites and specialist data sector to build up technical infrastructure and solutions so that a treatment capability can be developed. The project will be run over 3 years with a start date of 1st March 2018.

The project is organised into seven work packages, each work package is focused on delivering a particular aspect of the strategy which is crucial to achieving the overall objective. Chaucer Life Sciences will be supporting Work Package 4 which is concerned with supporting the development of a scalable, cost-effective data collection and visualisation solution. Chaucer's responsibility will be as a 'Data Steward', ensuring that the solution is a secure, compliant and governed system that will deliver robust processes for managing the data during its lifecycle from collection through to archiving.

This scoping document outlines the work that Chaucer Life Sciences will deliver as part of work package 4. It will contain detailed information around activities that Chaucer will conduct to ensure that all technology and organisational components of the data hub are in place to deliver the work package 4 data stewardship objective.

The intended audience of this document are industry partners involved in work package 4 and additionally other stakeholders that require oversight of the scope of the WP4 data stewardship delivery.

2. Project Objectives

iMATCH is organised into seven work packages, each work package focused on delivering an aspect of the strategy which is crucial to achieving the overall objective. Each work package is made up of a team of industry and/or public-sector contributions each with its own deliverables. Some cross-work package working will be required for some aspects of project delivery (see below) but mostly work packages will work within their own teams.

Chaucer Life Sciences will be supporting Work Package 4 (WP4) which is concerned with supporting the design, build and delivery of an Open Innovation Hub that will provide a platform to share data and content in a single 'end-to-end' solution that is compliant with Good Clinical Practice (GCP) and all relevant regulations.

WP4 will need to also gather the complex requirements for later phase ATMP study databases, and use these requirements to build a library of data collection and data analysis standards that are applicable across different types of ATMP studies. WP4 will also work with the partners in WP 2, 3.1 and 4.2 to develop systems that will integrate patient data with sample tracking systems.

2.1: Work package 4

The majority of this scope document will concern work package 4.1 which is aligned to the core deliverables for the data hub infrastructure.

2.1.1: Work Package 4.2

This is focused on the development of systems to safely manage patients receiving ATMP therapies through the development of early-warning systems to flag evolving toxicities. This work package is jointly owned by Donal Landers and Elaine Kilgour from the digital ECMT group. Elaine will be developing a cytokine ELISA on a set of cytokines that will be predictive of the early signs of cytokine storm which is one of the severe toxicity syndromes that may occur for some patients. Donal will support the development of an early warning system through algorithm development and corresponding visualisation tools.

Work package 4.1 and 4.2 will collaborate to ensure the data required for algorithm development is included in CRF design (4.1) and that the visualisation solution that may support the warning system is also encompassed in the data hub infrastructure.

A web-based application called REACT will be used in order to visualise data generated from work package 4.2. The data for REACT will need to flow through the data hub that will be built in WP4.1. A review of data stewardship for REACT will be included in the scope of this data stewardship activity. It will be important to ensure that the data that is consumed by the algorithm engine and visualisation software reaches the destination in a secure and compliant state.

2.1.2: Work Package 4.1

Work Package 4.1 is made up of 4 industry partners from the CRO and technology sectors with defined objectives aligned against the delivery of the data hub;

Partner	**High Level Deliverable for Work Package 4.1**
Aptus Clinical	Develop a compliant clinical conduct solution to support CTL in delivering 2 patients under a specials exemption and 'rolling-over' into the 55-patient clinical study
Chaucer Life Sciences	Deliver the required oversight of how the data and content will be managed throughout its life cycle. The governance structure will also allow for continued oversight throughout the years as regulations change and systems are matured throughout their life cycle
Data Trial	Provide the content repository (Nucleus) for all transformed data and documents (eTMF) including connectors with Formedix and enabling visualisation of data in the repository
Formedix	Provide the software platform (Formedix On) which will enable (a) the design of CRFs, CDISC compliant datasets and mappings between multiple study data sources (b) the build of case report forms for data capture (c) data transformations for the integration of multiple data sources and (d) metadata management of all study components so they can be versioned and re-used in subsequent trials

Chaucer Life Sciences will work closely with each of the industry partners to confirm that they have the required technical and organisational measures that are needed so that the core components of the data hub are aligned to the principles of data stewardship.

Chaucer Life Sciences will also work closely with partners to build a governance structure so that the data hub is able to have all the procedures and policies in place to maintain high data integrity and GCP standards when the data hub goes live. The governance structure will also enable work with different study sponsors, vendors and third parties in the future and is be able to respond to the 'scale up' and 'scale down' of the system.

3. Data Stewardship and Governance is critical to delivery of WP4.1

3.1: Data Stewardship Definition

Within the scope of iMATCH work package 4.1, the role of the data steward is defined as;

The person responsible for the identification of and management of data risks to integrity, quality, trial conduct and patient protection that will arise through the build of the 'data hub infrastructure'.

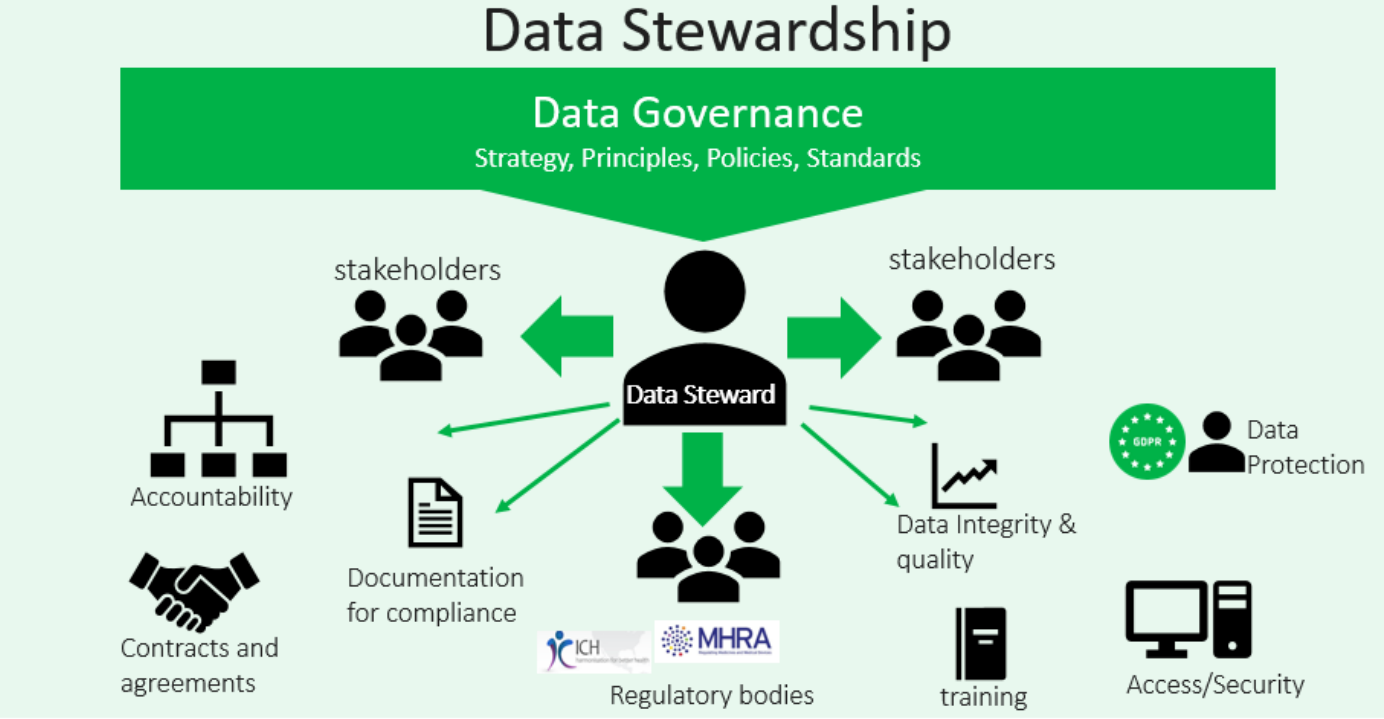

Figure 1: The data steward will need to review all aspects of the data flow, and technical and organisational measures that are either already established or need to be set up to ensure the data hub is a secure, compliant platform.

The data steward will understand all the necessary measures that are required to build a secure and compliant data hub including many of the aspects highlighted in figure 1. The data steward will also ensure that a data governance framework is put in place to manage and monitor ongoing risks.

3.2: Data Steward Objectives

1. Assume responsibility for monitoring the flow of clinical and operational study data from acquisition to consumption in order to help identify data quality/integrity/security issues and facilitate their resolution.
2. Ensure there is an executable governance strategy and architecture to manage the quality, consistency, usability, security, and availability of the data through its life cycle in the data hub.

3.3: High Level Data Stewardship Deliverables

No	Year	Delivery Date	Deliverable Description
1	1	31/05/18	Planning and Scoping: Scope Data Integrity and Data Stewardship requirements. Scope and understanding of functionality, policy and procedures for underlying technical solution.
2	1	31/08/18	Review and assess draft data flows. Assessment of underlying technology system gaps. First draft data Integrity and stewardship plan
3	1	30/11/18	Advice and guidance to technology providers and process owners. Further development of Data Integrity and Stewardship plan.
4	1	28/02/19	Finalized Data Integrity and stewardship plans.
5	2 & 3	Continual up until project end 28/02/21	Management of Data Integrity and Stewardship Plans

3.4: High Level Scope for Data Stewardship Activities

3.4.1: Data Integrity Scope

This refers to the degree to which data are complete, consistent, accurate, trustworthy and reliable through the data lifecycle. Data should be collected and maintained in a secure manner, so that they are attributable, legible, contemporaneously recorded, original (or a true copy) and accurate (ALCOA). Regulatory recommendations for meeting standards for data integrity exist from the MHRA[1], FDA[2] and ICH[3,4].

The scope of this project will include a set of health checks/gap analysis for each of WP4 vendors against the data integrity requirements. Integrity risks in the source data collection procedure at the clinical trial site will also be recorded. A risk-based approach such as that used in ICH Q9[3] will be employed for classification of any risks for remediation. This will be covered in more detail in later sections of this document.

3.4.2: Data Quality Scope

This is not the same as data integrity, which mainly refers to the 'preservation' of the data as it flows from data collection or 'source' through to its destination so that it is an identical representation of the original data. Data that has had its integrity maintained does not necessarily guarantee that the data is of high quality. If the data recorded at the source is erroneous, missing or incorrect then it will not be suitable for decision making and may impact trial quality.

Defining the thresholds for data quality requires domain knowledge and expertise to understand which data are critical to decision-making. Risk classification can be assigned to data variables so that an assessment of quality can be performed.

Within the scope of this project Chaucer will try and gain an understanding of data quality measures so that a risk classification can assigned. Any areas of quality concern will be identified and a risk-based approach for remediation as defined in ICH Q9 will be recommended by Chaucer.

3.4.3: Data Protection/Security Scope

The data hub will be involved in the collection, transfer and storage of clinical data. The data that is processed by the data hub should be pseudonymised in line with EU/UK data protection principles and requirements. Following Pseudonymisation, the clinical data is still classed as sensitive and must be kept secure to protect patient rights.

A new version of data protection law will apply from 25th May 2018 in the form of the General Data Protection Regulation (GDPR). Organisations are in scope for GDPR if they control or process EU citizens personal data, this is irrespective of whether they have a physical presence in the EU. GDPR introduces more accountability for organisations controlling or processing data and a requirement for increased transparency of processing activities.

As the data hub will be processing EU citizen data, the GDPR regulation will need to be complied with. Chaucer will conduct a health check/gap analysis ahead of any data processing in the data hub and make recommendations to meet the obligations of the new GDPR regulation. Chaucer will not act in the role of the Data Protection Officer for the Data Hub.

3.4.4: Data Governance Scope

Data governance refers to the policies. procedures and rules that govern the data and minimise risk to quality, trial conduct and ensure patient data is securely protected. As part of WP4, policies, procedures and documentation will need to be in place to ensure that data integrity, quality and security are maintained.

Within the scope of the data stewardship role, Chaucer will conduct a health check of existing policies and procedures and highlight any gaps that exist for the vendors involved in WP4. Additionally, Chaucer will consider additional policies and procedures that need to be implemented as a consequence of the data hub build.

The scope will include a proposed governance structure so that any aspect of data risks can be reviewed, monitored and escalated if necessary. The governance structure it will allow for other aspects of the data hub to be monitored/reviewed including new sponsors/studies/vendors/visualisations/regulatory changes.

4. Data Stewardship Plan

The data stewardship plan is one of the key deliverables for delivery at the end of year 1 of the project. The plan will consist of information on data integrity and quality risk, security and governance controls that will be used for the data hub. The information on key data risks for the ATMP trials will come as a direct result of some of the activities that are conducted early on in the project. This section of the scope document will therefore cover more details around each activity listed in section 3 that will help build the data stewardship plan.

For more information on the content of the Data Stewardship Plan please refer to the Appendix as this will not be covered here. The Appendix lists a proposed content for the data stewardship plan but this could change over the course of the project as it is developed further.

4.1: Year 1 Activities

A large amount of the data stewardship activities will be completed in year 1, after year 1 the data stewardship role will move to a maintenance phase. The activities that will occur in year 1 are shown in figure 2.

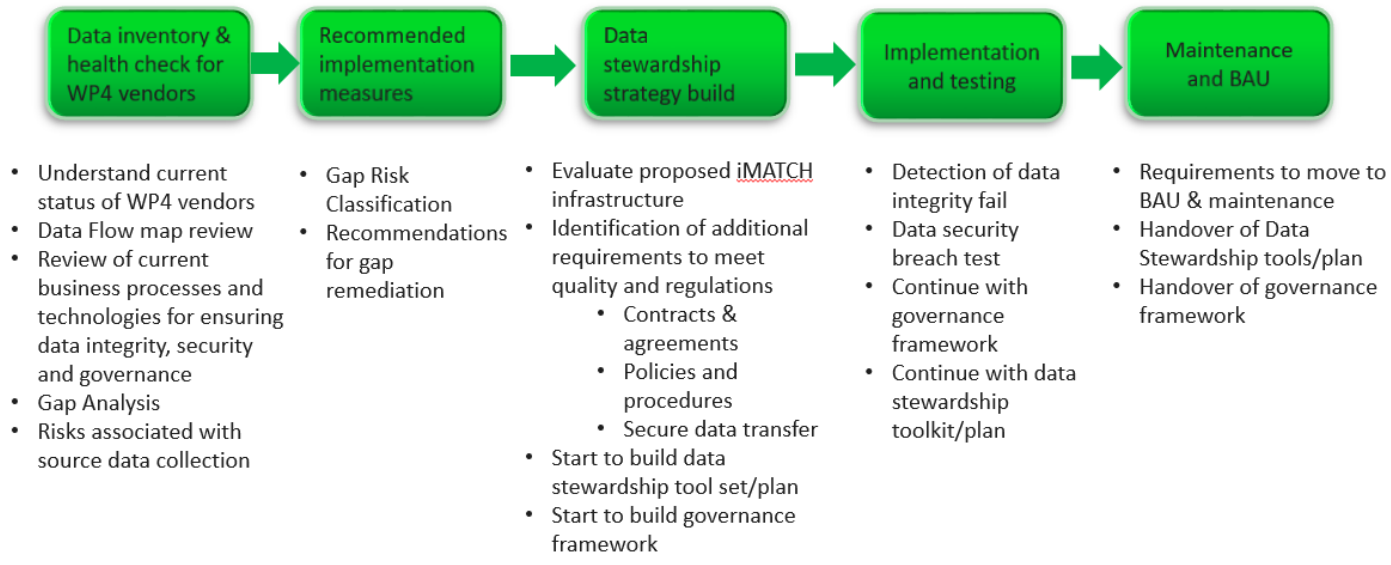

Figure 2. Shows the activities that will be conducted in year 1 in order to build the data stewardship plan. These activities are roughly in time order (left to right) however there will be some activities that will happen in parallel.

4.2: Fixed and Non-Fixed Vendors in scope for data stewardship

The iMATCH data hub infrastructure will consist of some known or recommended vendors and additionally it will also require some additional technology components that may change from one study to another.

Without all components of the infrastructure being fixed, the data stewardship work will involve delivering a strategy that can allow for a rapid comprehensive assessment of a new vendor.

Within WP4 known vendors that are likely to be involved in delivering the data hub infrastructure will be Formedix, Data Trial, Aptus Clinical and the REACT visualisation platform. For these four vendors a thorough data stewardship health check will be conducted to identify any upfront risks for utilising the vendors as part of the data hub solution. Should any data stewardship gaps emerge as a result of the health checks, remediation plans can be put in place.

For the non-fixed vendors a set of tools will need to be delivered in order to evaluate aspects of their technical and organisational infrastructure. Tools such as procedures, training, governance framework and risk assessment kits will be in place to enable comprehensive and efficient evaluation.

Non-fixed vendors might include; EDC vendor, Data Management Solution, e-Traceability solution, LIMS, Wearable devices.

Risks will also be associated with source data collection at the Clinical Trial Site. Patients attending the Clinical Trials Unit at the Christie for an ATMP trial or receiving treatment at the Christie will have measurements and vitals taken which will form part of source data collection. Risks to data stewardship generated through this process will be logged and risk classified, risk reduction measures will be noted if they are in existence.

4.3: Vendors not in scope

The scope of this project does not include the trial sponsor. The trial sponsor is the data controller and they are responsible for determining how decisions are made on the data. WP2 describes the work that Cellular Therapeutics will conduct to set up an ATMP trial so start at the end of year 1. It is proposed that CTL will use the data hub infrastructure for this trial as a POC.

It is not within the scope of WP4 to review the sponsor in terms of its compliance for data protection and standards for data integrity and quality, it will be up to CTL to conduct this review and ensure they are working to regulatory standards. Chaucer can advise if requested but if additional services are requested such as GDPR health check this will not occur within the iMATCH collaboration and will need to proposed as an additional service offering.

4.4: Health Checks for Fixed Vendors

4.4.1: Data Flow Maps

To able to perform a thorough evaluation of each of the fixed vendors it will be necessary to have oversight of the technical architecture of the system or database they will provide. The first requirement for analysis will be to review a data flow map for each vendor to understand characteristics of data flow and storage including physical location, file structure, any data processing including transformation and aggregation, data transfer to third party vendors/systems.

The data flows will form the basis for subsequent risk assessment for both data integrity/quality, these risk assessment strategies are covered in more detail in later sections of this document.

An analysis of the source data collection data flow at the Clinical Trials Unit will also be reviewed in order to identify any risks to data prior to data hub collection.

4.4.2: Data Integrity Health Check

A data integrity health check will be conducted for the fixed vendors in the proposed data hub infrastructure to highlight any areas for concern that need technical or organisational measures put place. The first part of the health check is to map the data flow for each of the vendor systems and assess any associated data integrity risks, this will form the basis of a risk assessment. The risk assessment process that will be followed corresponds to standards set out by the MHRA[1], FDA[2] and ICH[3].

The MHRA suggest *"a data integrity risk assessment is conducted where the processes that produce data or where data is obtained is mapped out and each of the formats and their controls are identified and data criticality and inherent risks are documented*. *Where data integrity weaknesses are identified, companies should ensure that appropriate corrective and preventative actions are implemented across all relevant activities and systems and not in isolation"*.

4.4.2.1: Data Integrity Risk Assessment

The first part of the risk assessment process is to define risk. This includes defining the following[3];

- What might go wrong?
- What is the likelihood it will go wrong?

- What are the consequences?

The method that will be used to establish the risk is to define 'data criticality' and 'integrity risk', this is currently part of the guidance set out by the MHRA[1].

Data Criticality: Determine how the data is used for decision making *(in terms of ICHQ9, this helps to understand the consequences of a Data Integrity fail)*

Integrity Risk: The potential to be deleted, amended or excluded without authorisation and the opportunity for detection of the events *(this helps to establish the likelihood of a data integrity fail*).

The combination of the data flow maps and risk assessment process will allow for a description/classification of the risks for each of the fixed vendors in the data hub. The risk assessment strategy can also be employed for new vendor engagements.

A template similar to that set out in Appendix 10.3 will be used as a data integrity risk assessment tool.

A template similar to that set out in Appendix 10.4 will be used for risk classification and management.

4.4.2.2: Data Integrity Gap Analysis

The next part of the health check will be to establish what processes, procedures and technologies are already used by the vendors to manage data integrity/quality risk and identify if any gaps exist. Not all activities will be relevant to every vendor system.

The following activities/checks will be conducted for the fixed vendors and clinical trial unit if applicable;

- A review of how systems and processes are designed to facilitate data integrity
    - Training, environment (including accuracy of time stamps), access to source data, user access rights
- Current procedures used to assess data integrity processes of external vendors (vendor assessment SOP)
- Management of data integrity during data transfer and/or migration
- Audit trail review; defining which systems should have audit trails
- Review of completeness of meta data
- Review of data retention, archiving and backup strategy
- Review of system URS (Are the critical steps for Data Integrity and quality called out?)
- Computerised system user and system admin access control

- Computer system validation status: which systems are in scope, evidence of last CSV check, compliance with 21CFR part 11
- Review of access and export function of electronic versions of records from Document Management System
- Review of record retention policy for systems
- Data review and approval procedures
- Review of Data Integrity aspects of 3rd party contracts

A review of the current procedures used will be documented. Gaps for remediation will be identified and prioritised according to risk.

4.4.3: Data Protection Health Check

A data protection health check will be conducted for the fixed vendors in the proposed data hub infrastructure to highlight any areas for concern that need technical or organisational measures put in place. It will be the responsibility of the fixed vendors to rectify any and all areas of concern in relation to ensuring data protection under EU and UK applicable legislation.

4.4.3.1: Data Flow Inventory and Article 30 review

The first part of the health check involves a comprehensive review of the data flows that involve personal data, this will include all clinical and health data. It is expected that each vendor would have conducted such a data flow inventory in preparation for GDPR which goes live on 25th May 2018. The data flow inventory and documentation of data processing activities is a requirement of GDPR as set out in Article 30[6]. The work Chaucer will conduct in reviewing the GDPR compliance is listed here;

- Review of data flow inventory
    - Inclusion of data origin, path, storage location.
    - Inclusion of all aspects of network infrastructure e.g. servers, backup media, devices
- Review of Article 30 compliance documentation for processing corresponding to data flows e.g.
    - lawful basis and purpose of processing, special category processing condition, information around data transfers and security measures that will be used to safeguard personal data and more.

Any gaps that emerge will be documented and prioritised for remediation according to risk.

4.4.3.2: Other GDPR Health Check Activities in Scope

- Review processor contracts for compliance
- Review the list of stakeholders and accountable persons for Data Protection within each vendor

- Review a list of policies, processes and procedures that were modified due to GDPR
- Review breach notification process
- Review of vendor Data Protection governance procedures
- Review ISO27001 Certification Status if applicable
- Review GDPR training for organisation
- Privacy Notice review
- Review privacy by design and default measures
- EU representation if applicable

Responses to the checklist will be summarised in a report with any gaps in compliance highlighted.

4.4.3.3: Data Protection Impact Assessment (DPIA)

When a new processing activity is planned or a new data processing technology is introduced, GDPR encourages a risk assessment known as a Data Protection Risk Assessment (DPIA) to be performed in advance of the processing. This assists the controller of the processing operation to look in detail at each aspect of processing and identify any areas of risk so that the appropriate measures can be put in place.

The data hub will be introducing a set of new technologies and highly sensitive health data will be processed within the data hub. The responsible owner of the data hub will therefore have a role of a joint controller along with the trial sponsor and will have obligations to carry out a risk assessment of data protection ahead of processing. It is recommended by Chaucer that the owner of the Data Hub perform a DPIA and Chaucer can guide this process. The DPIA will be facilitated by ICO's recommended template (Appendix 10.2). The completion of the DPIA will be carried out ahead of any sensitive personal data being processed by the technology components and should be done in consultation with the controllers DPO.

4.4.4: Out of Scope Health Check Activities

Chaucer will review all listed artefacts for data integrity/quality and data protection as outlined in section 4.4. Chaucer will conduct an inventory of data flows and make recommendations to bridge any gaps in compliance.

Chaucer will help assist vendors in reducing any Data integrity/protection risks by recommending solutions however if the solutions are not implemented Chaucer cannot be held responsible. Chaucer indemnifies itself from any and all responsibility in the event of a data breach or non-compliance under the appropriate EU and UK data protection legislation. Additionally, although Chaucer will look at ways that data protection risk can be reduced they will not act in the role of the data protection officer for the data hub. The DPO is a role that will be recommended by Chaucer to be in place ahead of data processing so that the risk of incurring a personal data breach can be significantly reduced. The DPO role is not in scope in the data stewardship activity but can be discussed as an additional service that Chaucer could provide if requested.

Chaucer will recommend solutions for gap remediation and will help guide the process of SOP review and update, it will be the vendor's responsibility to write and own any legal contracts and to implement any technical measures that are needed to be compliant.

5. Data Stewardship Strategy Build

5.1: Risk Assessment for iMATCH Infrastructure

Following the health check and risk assessment activities for each vendor, a review of additional risks to data integrity, quality and security needs to be conducted for the proposed iMATCH infrastructure.

The followed activities will be conducted upon finalisation of the infrastructure by Chaucer;

- Identification of new data integrity/quality risks introduced as part of the innovation hub
- Risks associated with data transfer between vendors
- Risks of technology changes, updates
- Risks introduced at source data collection at the Clinical Trials Unit in Manchester

The following activities will be assisted with if necessary but responsibility will be for the data hub owner to initiate the activity in collaboration with the data hub DPO (not yet assigned).

- Data Protection Impact Assessment- to be conducted in collaboration with the DPO by the Data Hub owner

The risk assessment will be documented and strategies for reducing risk or managing risk will be recommended if they are not already in place. If risks are acceptable they will be called out at this stage. Chaucer will not own the risk register, instead accountability will need to be owned by data hub owner/ governance group.

The DPIA is the responsibility of the data hub controller or owner, Chaucer will help to guide this process if needed but it should be driven by the data controller and done in consultation with the Data Protection Officer.

5.2: Governance Strategy for iMATCH Infrastructure

One part of the risk management strategy for the iMATCH data hub will to be to ensure that a comprehensive and fit for purpose governance framework is built.

Chaucer will review existing governance procedures and policies for fixed vendors and look for areas of synergy. The governance framework will encompass not only policies and procedures but additionally any review boards or committees that need to be established to ensure the data hub operates in a way that ensures any risk to patient safety or to product quality are minimised.

Chaucer will not be responsible for management of risk during the project but will instead recommend the tools, processes and systems that will enable the data hub to own and manage risk.

The following activities are in scope for the governance framework build;

1. Ensure that ownership and accountability for the Data Hub is clearly defined.
2. Ensure there is a comprehensive set of systems and procedures (technology and organisational measures) that minimise the risk to data integrity, quality and data protection.
    - ICHE6(R2) sets out expectations in terms of procedures for assurance of data quality and integrity
    - Procedures should be located within the Nucleus document management system so can be located easily by the relevant stakeholders
    - An outline and index of the procedures (SOPs) and other relevant documents to the governance framework will be in the Data Stewardship Plan delivered by Chaucer.
3. Ensure that trial-related responsibilities are specified clearly in writing for each data hub vendor as defined in ICHE6R2
4. Ensure there is adequate staff training on data integrity/quality and data protection
    - Training should also encourage a culture of transparency and a working environment that actively encourages reporting of errors, breaches and issues that create data integrity risks
5. Ensure there is a plan for a periodic audit of systems within the open innovation hub to ensure that technological and organisational measures are operating as expected.
6. Ensure that the open innovation hub has a management structure in place with accountability for data protection and data integrity/quality.
7. Ensure that access to data within the data hub is managed in an effective way so that access is restricted only to the appropriate job roles.
    - A list of Data Hub access permissions including system administrator access should be stored in Nucleus and should be kept up to date
    - A list of access permissions relevant to job role will be included within the data stewardship plan
    - Security of systems should prevent unauthorised access
8. Ensure that a set of groups are established so that the innovation hub can be developed effectively and can respond to a changing environment and new technology components. Examples of such groups or committees include;
    - **Steering committee**; responsible for reviewing collaborations, new studies, risk review, overall steering of the data hub.
    - **Visualisation committee**; responsible for review of new visualisation proposals
    - **Technology committee**; responsible for review of new technology components

9. Ensure there is a robust set of procedures in place to enable detection and a quick response to any issues that arise concerning data integrity, quality and security breaches.
    - This should include a clear method for reporting the breach to the relevant internal management group and external authorities if required
    - This should include a clear instruction to initiate a Corrective And Preventative Action (CAPA) if required
10. Ensure there are a set of procedures for system set up as well as use of all technology components of the data hub.
11. Ensure a set of procedures are in place to ensure trial conduct is not impacted e.g. safeguarding of blinding if required.
12. Ensure a set of procedures and tools are in place for new vendor assessment and engagement
    - For any new vendors that will be used as part of the data hub, a strategy for assessing the vendor for data integrity and data protection compliance will need to exist.
    - Chaucer will ensure that a set of procedures are in place to guide this activity
    - Chaucer will deliver risk assessment templates to allow for data integrity and data protection risk assessments to be completed
    - Ensure that compliant contract templates are available
13. Ensure there is guidance around storage length of documents corresponding to regulatory requirements for ATMP trials

Chaucer will work with the vendors within the data hub to recommend the elements described above are included as part of the governance framework.

6. Implementation and Testing

At the end of year 1 a test of the data hub will be performed by Chaucer to ensure that components are working as expected for maintenance of data integrity, quality and protection as set out in the data stewardship plan. The test will look at technology components but additionally the governance framework to ensure that policies and procedures are in place and are being used.

6.1: Data Integrity Test

Follow a data trail from source to archiving and ensure its data integrity is maintained including availability of meta data that is necessary to reconstruct events

6.2: Audit Trail review

Review audit trails for each technology component including document management system and data standards conversion tool.

6.3: Data Quality Test

Review key data quality metrics including how low quality data is flagged and detected within the hub, review if procedures are in place to respond to poor quality issues.

6.4: Data Access/Security Test

Review data access rights, test system to see if issues such as multiple log-ons are flagged, system admin access is restricted to appropriate members, source data can be accessed.

6.5: Governance Framework

- Review if all policies and procedures are accessible and are organised in a structured manner to enable easy navigation.
- Review minutes of steering committees and other relevant governance groups

- Review system and organisation training

7. Maintenance and BAU

During year 2 and 3 of the iMATCH project, Chaucer will support work package 4 in an advisory capacity and to maintain an awareness of any change to the data hub or regulations that could impact data stewardship.

Activities that Chaucer will undertake will include;

- A system test of the data hub once it is operational (as set out in section 6).
- A review of the risk register at regular timepoints (once a month).
- Consultation with steering committee to understand if any data stewardship issues have arisen.
- Consult on any data stewardship issues that should arise during years 2 and 3.
- Notify the data hub stakeholders and management group of any regulatory changes that arise during years 2 and 3 that could impact data integrity, quality and data protection.

8. Dependencies and Risks to Data Stewardship Delivery

8.1: Dependencies

Data flows are provided to enable risk assessments

Information is provided by qualified persons around ATMP trial data criticality for risk assessments

Procedures, policies and contracts are provided by vendors for gap analysis review

Fixed vendors are in place and technology components developed to enable system test

Information provided at all stages are accurate and complete

8.2: Risks

Chaucer will make recommendations to ensure that the Data Hub operates compliantly will minimal risks to data integrity, quality and data protection. If the recommendations are not followed Chaucer Life Sciences cannot be held accountable for failures due to poor data stewardship.

Chaucer will not manage risks to the data hub, risk should be managed by a management group within the data hub, who owns and reviews the risk will form part of the governance strategy.

9. References

1. MHRA 'GXP' Data Integrity Guidance and Definitions March 2018
2. **Code of Federal Regulations**, Title 21, Food and Drugs (Government Printing Office, Washington, DC), Part 11 (2003)
3. ICH, Q9, **Quality Risk Management**, step 4 version (2005).
4. ICH, E6 R2, INTEGRATED ADDENDUM TO ICH E6(R1): **GUIDELINE FOR GOOD CLINICAL PRACTICE** (2015)
5. **ISPE GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems**, International Society of Pharmaceutical Engineering, 2008.
6. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (General Data Protection Regulation).http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
7. EMU, **Draft Detailed guidelines on good clinical practice specific to advanced therapy medicinal products,** 2009. https://ec.europa.eu/health//sites/health/files/files/eudralex/vol-10/2009_11_03_guideline.pdf

10. Appendix

10.1: Data Stewardship Plan (Suggested Content)

Section 1: Overview of data hub infrastructure

- Data flow map of data hub, including fixed and non-fixed vendors
- High level overview of technical and organisational measures in place for hub

Section 2: Key data risks and methods for reducing risk in the data hub infrastructure

- Data Integrity Evaluation of Data Hub Infrastructure
    - ATMP Clinical Trial Data Integrity Risks
    - ATMP Therapy Data Risks
    - Data Integrity Risk Assessment toolkit for new vendors
    - Measures for reducing risk
- Data Quality Evaluation for ATMP trials using Data Hub
    - ATMP data risk classification by data variable
    - ATMP quality risks for clinical trials
    - ATMP quality risks for therapy
    - Data Quality Risk Assessment toolkit for new vendors
    - Measures for reducing risk
- Data Protection Evaluation of Data Hub Infrastructure
    - Data protection risks for infrastructure
    - Measures for reducing risk
    - Data Protection Impact Assessment

Section 3: Governance Framework

- Overview of Data Hub Governance Organisational Structure
    - To make decisions around new trials
    - To make decisions around new vendors/technologies
    - To escalate issues around operational/compliance aspects of data hub
    - To communicate with regulators/auditors
    - List of roles, responsibilities and accountabilities
- Overview of Quality Management System for Data Hub

    - Data Integrity Policies and procedures
    - Data Protection Policies and procedures
    - Data Quality Policies and procedures
    - Training and Utilisation
- Data Stewardship Tools
    - Data Protection Impact Assessment
    - Data Integrity Risk Assessment
    - Technology assessment SOP?
    - Vendor selection SOP?
    - Contract requirement checklist

10.2: DPIA Template

https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf

10.3: DIRA Template

10.4: Risk Classification Template