

	GPSoC Data Migration Specification			
	Programme	NPFIT	Document Record ID Key	
	Sub-Prog / Project	GPSoC	NPFIT-PC-PMG-DEL-0020.07	
	Prog. Director	Kemi Adenubi	Status	Approved
	Owner	Kees van Ek	Version	2.0
	Author	Rory Davidson	Version Date	23/07/2008

GPSoC Data Migration Specification

GPSoC Data Migration Specification

NPFIT-PC-PMG-DEL-0020.07

23/07/2008 APPROVED V2.0

Amendment History:

Version	Date	Amendment History
1.0	12/03/07	Final version for approval and publishing. Approved.
1.1	01/08/07	Draft incorporating comments from Suppliers
1.6	27/02/08	Updated following clinical review
1.7	12/05/08	Updated to incorporate comments from JGPITC and suppliers
2.0	23/07/08	Approved

Forecast Changes:

Anticipated Change	When

Reviewers:

This document must be reviewed by the following:<author to indicate reviewers>

Name	Signature	Title / Responsibility	Date	Version
Kees van Ek		GPSoC		1.2
Ian Harrison		ITB		1.3
Nicci Wilson		IQAP		1.3
Brian Morrissey		TAG		1.2
Gillian Braunold		NCL		1.3
Clinical Safety Group		Various		1.3
Ian Lowry		ETP		1.3
Sandy Scales		GP2GP		1.3
Steve Bentley		Summary Care Record		1.3
Geri Oakley		PDS		1.3
Beth Gildersleve		Technical Deployment		1.3
John Williams Alan Hassey		Joint GP IT Committee		1.7
GPSoC Framework Suppliers		Various		1.6

Approvals:

This document must be approved by the following: <author to indicate approvers>

Name	Signature	Title / Responsibility	Date	Version
Michael Thick		Chief Medical Officer		
Paul Jones		Chief Technology Officer		
Kemi Adenubi		Commercial Director		

GPSoC Data Migration Specification

NPFIT-PC-PMG-DEL-0020.07

23/07/2008 APPROVED V2.0

Distribution:

GPSoC Suppliers

PCT's

Joint GP IT Committee

Document Status:

This is a controlled document.

Whilst this document may be printed, the electronic version maintained in FileCM is the controlled copy. Any printed copies of the document are not controlled.

Related Documents:

These documents will provide additional information.

Ref no	Doc Reference Number	Title	Version
1	NPFIT-SHR-QMS-PRP-0015	Glossary of Terms Consolidated.doc	

Glossary of Terms:

List any new terms created in this document. Mail the NPO Quality Manager to have these included in the master glossary above [1].

Term	Definition
"Authority"	means the Department of Health agency NHS Connecting for Health
"Call Off Agreement"	means an agreement between a PCT and the Supplier on behalf of Practices for the provision of GPSoC Services entered into pursuant to the GPSoC Framework Agreement
"Clinical Hazard"	means the potential to cause or fail to prevent harm to a patient.
"Clinical Risk"	means the likelihood, probability, impact, or severity of hazard resulting in harm to a patient
"Clinical Safety"	means the process of reviewing and dealing appropriately with Clinical Hazards and Clinical Risks in order to ensure patient safety, including anything which has the potential to cause harm to a patient, but excluding health and safety considerations in terms of operating clinical IT systems
"Data & Audit Trail Retrieval Service"	means the provision of access to the medical records contained in the Source System together with the associated audit trail following migration to the Target System
"Data Extract"	an extract of the Practice's clinical data produced in accordance with the requirements of section 7.
"Data Extract Supplier"	the Supplier of the Data Extract from the Source GP IT Clinical System.
"Data Load"	the loading of Transformed Data into the Target System
"Data Migration Approach"	has the meaning given to it in section 3 3
"Data Transformation"	the mapping of data from the Source System to a format which can be loaded onto the Target System;
"Deployment Verification"	means the process by which the Supplier shall verify the operation and performance of its system, in accordance with the Deployment Verification

GPSoC Data Migration Specification

NPFIT-PC-PMG-DEL-0020.07

23/07/2008 APPROVED V2.0

	Criteria.
"Deployment Verification Criteria"	means those measurable and quantifiable criteria measuring the Supplier's responsibilities and which are the criteria to demonstrate Deployment Verification
"Deployment Verification Report"	means the report produced by the Supplier setting out evidence that it has met the Deployment Verification Criteria
Compliance	means a process by which a Supplier's Data Migration Service, including its procedures, tools and algorithms, is assured and approved as set out in section 4 of this document.
"Issue Log"	the log described in section 4.5 of this document
"Migration risk"	Means risks to e.g. schedule or migration activities that does not necessarily have a clinical risk to patient safety.
"Patient Safety Assessment"	an assessment of the specific Clinical Risks associated with a data migration (also known as the Clinical Risk Assessment)
"Practice"	means all partners, employees and other persons at all locations that constitute a GP practice including all branch sites of such GP practice and all locations where a clinical IT system is used and where more than one GP practice operates from a location, each separate GP practice shall be treated as a Practice.
"Source System"	the GP clinical IT system from which data is being migrated
"Supplier"	means each GP IT supplier providing Data Migration Services to Practices. The Supplier could be acting as a Target or Source System Supplier.
"Target System"	the GP clinical IT system to which data is being migrated
"Target System Supplier"	the Supplier of the GP clinical IT system to which data is being migrated
"Transformed Data"	clinical data which has been through a process of Data Transformation

Contents

1 PURPOSE.....6

2 DATA MIGRATION PROCESSES6

3 SUPPLIER’S DATA MIGRATION APPROACH.....8

4 OVERARCHING REQUIREMENTS.....9

5 PROJECT PLANNING AND PATIENT SAFETY ASSESSMENT14

6 DATA CLEANSING IN SOURCE SYSTEM.....17

7 DATA EXTRACTION FROM THE SOURCE SYSTEM.....19

8 DATA TRANSFORMATION22

9 DATA LOAD INTO THE TARGET SYSTEM.....26

10 RETENTION OF THE SOURCE SYSTEM.....28

11 DATA AND AUDIT TRAIL RETRIEVAL30

12 POST GO-LIVE DATA QUALITY32

APPENDIX A – SOURCE DATA CHECKS.....33

APPENDIX B – PRODUCT DESCRIPTIONS34

APPENDIX C – DATA MIGRATION DELIVERABLES.....35

1 Purpose

1.1 The purpose of this document is to set out a description of the Data Migration Services in relation to GP clinical IT systems and the associated requirements, roles and responsibilities required to support the migration of GP clinical IT system data. In response to the requirements set out in this document, the Supplier shall produce a document detailing the Supplier's Data Migration Approach.

2 Data Migration Processes

- 2.1 The requirement to migrate data from an existing GP clinical IT system may be triggered by any of the following circumstances, alone or in combination:
- i. a change from one data code set to another e.g. Read 2 to SNOMED. This may be instigated by a change of GP clinical IT system or by a change in the data code set implemented in a Practice's existing GP clinical IT system;
 - ii. physical migration of the data e.g. from a local server based system to a hosted system or from one Supplier's system to another Supplier's system;
 - iii. a change to the data model/structures or database product on which a Practice's system is based e.g. changes to such structures from one Supplier's system to another Supplier's system or from one Supplier's existing system to an upgraded system from the same Supplier.
 - iv. any merging or de-merging of one or more Practices involving the replacement or consolidation of existing GP clinical IT systems.
- 2.2 Figure 1 below sets out the separate Data Migration Services that will be required at each stage of the Data Migration Process.

Stage	Service	Trigger for Requirement	Responsible	Optional Delivery Agent
1	Project Planning and Patient Safety Assessment	Data migration due to either of i)-iv) above	Target System Supplier	N/A
2	Data Cleansing in Source System	Prior to production of each Data Extract or for ongoing data maintenance	Practice	N/A
2	Data Cleansing tools (e.g. reporting and audit tools)	Practice undertaking Data Cleansing activity	Any Supplier offering Data Cleansing services that is selected by a Practice or by a Target System Supplier with the Practice's approval	Any Supplier

GPSoC Data Migration Specification

NPFIT-PC-PMG-DEL-0020.07

23/07/2008 APPROVED V2.0

Stage	Service	Trigger for Requirement	Responsible	Optional Delivery Agent
3	Data Extraction from the Source System	Migration from a local server based system	Target System Supplier	Source System Supplier/Data Extract Supplier
		Migration from a hosted system	Source System Supplier	Target System Supplier/Data Extract Supplier
4	Data Transformation	Following production of each Data Extract	Target System Supplier	Source System Supplier / Other Supplier
5	Data Load into Target System	Once Data Extract and Data Transformation has been verified by the Practice	Target System Supplier	N/A
6	Retention of Source System	Migration to another System	Source System Supplier	N/A
7	Data & Audit Trail Retrieval from the Source System	Migration to another System where audit trail has not been migrated	Any Supplier contracted to provide this service	N/A
8	Post Go-Live Data Quality	A Practice undertaking Data Cleansing activity	Any Supplier selected by the Practice or by the Target System Supplier with the Practice's approval	Any Supplier

2.3 Appendix C contains a list of the deliverables which make up the Data Migration Process. Each of these deliverables is described in this document.

3 Supplier's Data Migration Approach

3.1 Supplier's Data Migration Approach

- 3.1.1 The Supplier shall produce a document setting out its Data Migration Approach in response to the requirements set out in this document. The Supplier's Data Migration Approach shall describe as a minimum:
- 3.1.2 the Supplier's Data Migration Process, setting out how each of the Data Migration Services will be delivered, including details of the Supplier's equivalent to the development and deployment products set out in Appendix C;
- 3.1.3 the Supplier's detailed procedures for each stage of the Data Migration Process including details of how interfaces with other parties will be managed:
- a plan for how the key issues and risks associated with each stage of the Data Migration Process will be mitigated;
 - details of subcontract arrangements where applicable including details of contractual arrangements relating to migration risk transfer; and
 - a template plan for a Practice migration which will form the basis of future Practice specific plans.
- 3.1.4 The Supplier shall provide the Data Migration Services as part of the Deployment Services and associated products as set out in the GPSoC Framework Agreement, including the products such as a Practice specific PID and Deployment Verification Report for the practice being migrated.

3.2 Authority approval of the Supplier's Data Migration Approach

- 3.2.1 The Authority reserves the right to approve or reject the Supplier's Data Migration.
- 3.2.2 No migrations to the Supplier's system(s) can be undertaken unless the Authority has approved the Supplier's Data Migration Approach or the Supplier is compliant with the Data Migration requirements.

3.3 Assessment and evaluation of the Data Migration Approach

- 3.3.1 Upon receipt of the Supplier's Data Migration Approach the Authority shall undertake an assessment and evaluation of the Supplier's Data Migration Approach.
- 3.3.2 Where a Clinical Hazard and/or a Clinical Risk is identified by the Authority in the course of the assessment and evaluation, then the Supplier shall change its proposed processes and procedures so as to reduce the Clinical Hazard and/or Clinical Risk, and the Supplier shall amend the Supplier's Data Migration Approach accordingly and target system as necessary.

4 Overarching Requirements

4.1 Scope of Data to be migrated

4.1.1 The Supplier shall migrate all data required to replicate in the Target System each patient's record as it was recorded in the Source System at the time of migration. The data to be migrated shall include but not be limited to:

- all electronic medical records including free text data and patient registration status;
- the relevant structural and coding information;
- all clinical record attachments (e.g. scanned letters, image files, etc) and associated links to the relevant patient records; and;
- records for all patients with data in the Source System.

Other data that may be migrated at the discretion of the Supplier shall include:

- GP's details;
- system users (Clinical & Administrative) and privileges; and calendars and activities.

Two specific exceptions to the above requirements may be agreed with the Supplier subject to the existence of an approved method for the archiving and subsequent retrieval of any data which is not migrated to the Target System (see section 11 of this document for the relevant service). The two types of excepted data which need not be migrated to the Target System, subject to the existence of a suitable archive, are:

- data relating to deducted patients;
- the audit trail for the migrated data (usually when migrating from one Supplier's system to another).

In addition other potential exceptions concern Source System specific non-clinical data, e.g. templates and past appointments.

4.1.2 During the Project Planning and Patient Safety Assessment stage, the Supplier shall clearly identify any data which will not be migrated, gain the agreement of the PCT and the Practice and confirm how access to non-migrated data will be maintained in line with Department of Health policy.

4.2 Business Continuity

4.2.1 The Supplier shall minimise the impact of data migration on the day to day activity on the Practice:

- agree with the Practice suitable business continuity and technical data recovery procedures to ensure the Practice is able to continue operating during (but not limited to) situations where for example:
 - the timescales for data migration slips considerably;

- source data is damaged as part of the data migration process and necessitates restoration from backup;
- there is a serious data error discovered with the Target System following Data Load;
- the loss of a system necessitates the temporary use of manual records until the system is restored;
- confirm that the Practice has adequate data backup and data archive regimes in place prior to commencing any activity with the Practice data. The Practice/PCT having the responsibility to ensure that there are adequate data backup and archive regimes in place;
- agree with the Practice and Source Supplier that any software or terminology updates to their existing source clinical system between the last 'sample' and 'live' stages of the migration process need to be agreed with the Supplier carrying out the data migration;
- maintain all existing interfaces with other Practice IT systems and equipment unless the Practice has chosen to replace or remove such existing systems or equipment as part of the migration to the Target System;
- demonstrate to the Practice that QOF points on the Target System match, subject to agreed exceptions, those on the Source System for the same Data Extract.

4.2.2 The Supplier shall ensure that:

- the Practice's involvement is streamlined, automated where practical, and makes efficient use of Practice staff;
- it avoids onerous and unnecessarily technical activity by the Practice;
- it utilises best practice techniques to make the transformation largely self-checking; and
- the Practice may simply and efficiently perform end-to-end sampling of transformed records without onerous procedures

4.3 Clinical Safety

4.3.1 The objective of NHS CFH Assurance is to provide an independent appraisal of the potential for technical and clinical risk in the migration of data. The detail of how technical and clinical safety assurance of Supplier's Data Migration services will be conducted by NHS CFH is set out in the CAP-GP Procedure for Data Migration Services (NPFIT-PC-PMG-DEL-0045).

4.3.2 The Supplier shall comply with the NHS CFH Clinical Safety Requirements, taking into account specific Clinical Risks associated with data migration. For the avoidance of doubt, the NHS CFH Clinical Safety Requirements (NPFIT-FNT-TO-TOCLNSA-0059) shall apply to any work performed by the Supplier.

4.3.3 The NHS CFH Clinical Safety Group has produced a set of product descriptions (Appendix B) to cover the Clinical Safety Products required to support data migration. The Supplier shall use these product descriptions as a minimum baseline of the contents required in order to meet Clinical Safety requirements set out herein:

- Patient Safety Assessment: At the outset of the planning of the data migration the Supplier shall facilitate a Patient Safety Assessment with the Practice involved. The PSA shall identify specific Clinical Hazards and associated clinical risks with the data migration.
- Clinical Safety Case: The Supplier shall present a mitigation for each Clinical Risk involved in the data migration, in a Clinical Safety Case.
- Clinical Safety Closure Report: The Supplier shall present a closure report containing evidence of successful implementation of the Clinical Safety Case.

4.3.4 The Supplier shall adhere to the NHS CFH Clinical Safety Incident reporting procedure, (NPFIT-FNT-TO-TOCLNSA-0057).

4.3.5 Once a Supplier has achieved Compliance, the Supplier shall only be required to undertake Patient Safety Assessments for subsequent migrations where additional clinical risks have been identified for any given Practice that is migrating. Approvals will be given by PCTs once the Supplier has achieved Compliance.

4.4 Information Governance

4.4.1 The Supplier shall be required to be compliant with the following standards in respect of information governance where applicable:

- Access to Medical Reports Act (1988)
- Access to Health Records Act (1990)
- Records Management - NHS Code of Practice
- Health & Social Services Act (Section 60) (2001)
- NHS Data Dictionary
- Data Protection Act (1998)
- Good Practice Guidelines for General Practice Electronic Patient Records
- NHS (Venereal Diseases) Regulations (1974)
- Confidentiality and security requirements set out in the document "Information Governance v2 - baseline index Foundation Module" (NPFIT-FNT-TO-TIN-1031).

4.5 Data Migration Tools

4.5.1 The Supplier shall set out how it will provide and/or use the following tools as part of its Data Migration Process. Any software or tools employed during the Data Migration Process must be maintained along with

configuration data and data mapping documentation under formal version control.

4.5.2 Data Quality Reports

The Supplier will prepare data quality reports to highlight possible irregularities in Source System data. Such reports shall include standard checks on data and any bespoke requirements that the Practice may have.

4.5.3 Supplier Mapping tables

The Supplier will provide the mapping tables that are being used during migrations. The Supplier should also provide specific mapping tables which map Supplier defined codes to the codes in use in the Target System. Local Practice defined codes will, however, need to be mapped by the Practice and not the Supplier.

4.5.4 Data reports and checklists

The Supplier should provide data reports and checklists for the Practice and for the Supplier for use in verifying the completeness and accuracy of the Transformed Data. Checks may be undertaken manually or be automated as appropriate. The Supplier is required to provide template reports and checklists, for inclusion in Appendix A, which the Supplier and the Practice will use as part of the assurance of the data migration activity. As a minimum, the Supplier must provide comprehensive aggregate reports listing counts of all coded data items from both source and target systems, with a facility to drill down to individual records. These would support reconciliation and quality assurance of code translations, verifying the correct application of the authorised mapping tables. These reports must be available on request on the Target system, in both trial and live environments during the Data Migration Process.

4.5.5 No other practice should be able to view these reports. The reports will be available at all times from the moment the trial environment is released to the Practice for data checking. The reports must be refreshed every time a Practice's data is re-loaded in the dummy environment.

4.5.6 The reports shall include comparisons of the data in the source system with the data in the target system (for example number of current active patients, active medications, results of standard QOF searches) and report any variances.

4.5.7 Issue Log

The Target System Supplier shall maintain a consolidated log of exceptions and issues encountered in each Practice and how each exception or issue was resolved.

4.6 Audits of the Data Migration Process

4.6.1 The Supplier shall undertake a comprehensive risk assessment in respect of the planned data migration for each Practice in accordance with section 5.4 . The Authority will select individual Practices at which to undertake a detailed audit of the application of the processes and procedures set out in

the Supplier's Data Migration Approach and of the quality and accuracy of output from the Data Migration Process.

4.6.2 The Supplier shall:

- maintain a comprehensive audit trail to evidence each relevant stage in the agreed Data Migration Process and shall provide access to these detailed records relating to the Practice's migration on the request of the Authority;
- provide the Authority with access and technical support to any interim files including, but not limited to, suspense files, or temporary files;
- respond to the Authority regarding any clarification points raised as a result of any audit within 5 days of receipt;
- evidence the correctness and completeness of any algorithms used to transform the data as part of the Data Migration Process;
- undertake any corrective actions identified as a result of any audit, within timescales agreed with the Authority; and
- provide evidence of completion of corrective actions.

4.6.3 The Authority shall identify those representatives responsible for auditing the Data Migration process and any associated governance arrangements for dealing with issues arising during migrations.

4.6.4 The Supplier shall ensure that Data sign-off and subsequent migration to the live environment is to a stated version of the approved Compliant Data Migration Approach.

4.7 Process Improvement

4.7.1 The Authority requires continuous improvement of the processes and procedures employed by the Supplier in supplying the Data Migration Services.

4.7.2 The Supplier shall consent to the sharing of information from the Supplier's Issue Log, the output of data migration audits and amendments to data mapping tables with the Authority. This is to ensure that where appropriate any common lessons learned, process improvements and changes to mapping tables can be made available to all suppliers by the Authority.

4.7.3 The Supplier shall demonstrate how it will review its processes, procedures and tools in order to introduce improvements to take account of issues identified in the Supplier's Issue Log, the output of data migration audits and amendments to data mapping tables.

5 Project Planning and Patient Safety Assessment

5.1 Project Planning and Patient Safety Assessment - Applicability

Stage 1 of the Data Migration Process shall be undertaken prior to the commencement of any data migration activity in a Practice. This applies equally to data migration undertaken between different Suppliers' systems and between systems provided by the same Supplier. The circumstances in which data migration activity may be required are set out in section 2 of this document.

5.2 Project Planning and Patient Safety Assessment - Service Description

- 5.2.1 The Supplier is required to deliver a Data Migration Plan which reflects the scope of the data migration activity in the Practice and identifies the responsibilities of the Practice and the PCT in the migration of data to the Target System. A Patient Safety Assessment shall be conducted in accordance with sections 4.3 and 5.4 of this document and appropriate mitigation action taken in respect of the clinical risks identified.
- 5.2.2 The outcome of the Patient Safety Assessment will identify the scale of the Clinical Risk associated with each migration and may indicate a requirement for an Authority led audit to confirm the efficacy of the processes, procedures and tools used by the Supplier in respect of higher risk migrations.

5.3 Authority/PCT Roles and Responsibilities

- 5.3.1 The PCT shall ensure that a robust set of contractual arrangements are in place for the delivery of the Data Migration Services as required for a particular Practice's migration. This shall include a review of any subcontract arrangements entered into by the Supplier for the delivery of the Data Migration Plan.
- 5.3.2 The PCT shall prioritise Practices for migration based on minimising the Clinical Risks in the migration activity. The Patient Safety Assessment undertaken by the Supplier shall be reviewed by the PCT and used to inform priorities.
- 5.3.3 The PCT shall ensure that it has access to both clinical and technical expertise in evaluating the Patient Safety Assessment.
- 5.3.4 The NHS CFH Clinical Safety Group reserves the right to review the Patient Safety Assessment and question the Supplier's proposals if it so wishes.
- 5.3.5 The PCT shall approve or reject the Supplier's proposed Data Migration Plan for the Practice. The PCT shall consult both the Practice and the Authority.
- 5.3.6 Where the Data Migration Plan has been rejected, the Supplier shall present a revised Data Migration Plan for approval within 7 days of

receiving notice of the rejection of the Data Migration Plan together with the reason for such rejection.

5.3.7 The PCT shall confirm the lines of communication, escalation and the key contacts in the Authority, PCT and Practice.

5.4 Supplier Roles and Responsibilities

5.4.1 The Supplier shall prepare a Project Initiation Document which will include a Practice specific Data Migration Plan which will set out the activities and timeline for implementing its Data Migration Process at the Practice.

5.4.2 The Supplier shall set out the procedures for data checking and how the Supplier, in conjunction with the Practice, will address situations which may be specific to the Practice, such as poor quality source data, migrating data from systems that use a different clinical code set and Practice specific codes.

5.4.3 The Supplier shall set out a bespoke Data Migration Plan for the Practice which shall clearly take account of the following:

- the size of the Practice and the amount of data to be migrated;
- the quality of existing data;
- the Source System data structures;
- the file format required for the Target System;
- the resources available to the Supplier and the Practice.

Both the Practice and the PCT should be involved, with the Supplier, in the creation of the Data Migration Plan and provide adequate resources for the migration or take the decision to delay the migration until the resources are available or issues with poor quality data have been addressed.

5.4.4 The Supplier shall undertake, in conjunction with the PCT and the Practice, a Patient Safety Assessment for the data migration activity in the Practice using the product description provided in Appendix B. The Patient Safety Assessment shall take account of the following:

- the Supplier's experience of migrations from and to the particular combination of Source and Target Systems;
- data coding related risks including:
 - different data code sets in use in the Source and Target Systems e.g. Read 2 to CTV3;
 - extensive use of Supplier specific codes in the Source system;
 - extensive use of Practice specific codes or free text in the Source System;
 - the potential for a change in the presentation or interpretation of the Source System data when it is imported into the Target System;

- changes to data structures in use between the Source and the Target Systems e.g. due to a change in system architecture;
- the size of the Practice;
- the availability of resource in the PCT and the Practice to adequately support the migration activity;
- the availability of Supplier resource;
- the complexity of the migration activity e.g. if a number of Practices are merging at the same time as migrating systems;
- the level of IT expertise and use within the Practice;
- the extent of change between the two systems and the level of training required for competent usage of the Target System;
- the quality of data in the Source System;
- the appropriateness of the overall timescales and whether they are realistic.

5.5 Practice Roles and Responsibilities

5.5.1 The Practice shall review the Supplier's Practice specific Data Migration Plan and advise the PCT as to whether it should approve or reject this Plan on behalf of the Practice.

5.5.2 The Practice shall identify key resources who will be involved in each stage of the Data Migration Process. As a minimum each Practice will require a Practice Data Migration Lead Clinician who will take responsibility for supporting the completion of the Patient Safety Assessment, data verification and for recommending sign off of the transferred data.

5.5.3 Where the Practice requires specific advice on Clinical Safety issues they shall contact the NHS CFH National Clinical Lead for Safety via the NHS CFH National Integration Centre help desk or direct to clinical.safety@nhs.net.

5.6 Project Planning and Patient Safety Assessment - Output

- Details of the contractual arrangements including the scope of the services, each party's responsibilities and risk transfer;
- Project Initiation Document
- A Data Migration Plan for the Practice. This shall be kept up to date and revisions circulated to all parties involved in the data migration for the Practice;
- A Patient Safety Assessment;
- A Clinical Safety Case: mitigation of specific clinical risks identified during the Patient Safety Assessment;
- Key resources identified – Supplier, Practice and PCT.

6 Data Cleansing in Source System

6.1 Data Cleansing in Source System - Applicability

For Stage 2 of the Data Migration Process, the Practice should undertake data cleansing, as per the basic Data Quality requirements document, NPFIT-FNT-TO-DQM-0157, prior to the extraction of data from the Source System as well as a reconciliation exercise with NHAIS - New Health Authorities Information Systems (better known as the Exeter system).

The Practice shall undertake data cleansing as an ongoing activity during the Data Migration Process to address irregularities that are found as data is mapped from the Source System to the Target System.

6.2 Data Cleansing in Source System - Service Description

Each Practice shall be required to review the quality of the data in its existing Source System and to improve data quality to a minimum standard in accordance with the Data Quality requirements document, NPFIT-FNT-TO-DQM-0157. The Practice may seek assistance to do so from PCT IM&T facilitators, the Source System Supplier or a third party supplier.

6.3 Authority/PCT Roles and Responsibilities

- 6.3.1 The PCT shall provide IM&T facilitators to assist the Practice in the data cleansing activity. Alternatively, PCTs may supply funding for specialist third parties to perform data cleansing.
- 6.3.2 The PCT shall ensure that the necessary contractual arrangements are in place to cover any supplier activity related to data cleansing.

6.4 Supplier Roles and Responsibilities

- 6.4.1 The Supplier or third party supplier shall, upon the Practice's request, prepare reports, using the tools referenced in section 4.5, that highlight possible irregularities in data entry to the Practice. Such reports shall include standard checks on data and any bespoke requirements that the Practice and Supplier agree on.

6.5 Practice Roles and Responsibilities

- 6.5.1 The Practice shall amend data entries in the Source System where data has not been entered in accordance with the Source System data structures and applicable code set.
- 6.5.2 The Practice must ensure they are using up to date codes and highlight any local configuration of codes in their legacy systems, as per the basic Data Quality requirements document, NPFIT-FNT-TO-DQM-0157. For example, the Practice will be required to identify and correct any retired codes and any changes that they have made to the descriptions associated with codes prior to migration.

6.5.3 The Practice shall develop data improvement plans which it shall work to during and after the Data Migration Process as applicable. Before Data Migration can take place, the PCT shall review these plans and agree with the Practice any elements of the plan which may be rejected during the migration.

6.6 Data Cleansing in Source System - Output

- A data set on the Source System which has been cleansed in accordance with the Data Quality requirements document, NPFIT-FNT-TO-DQM-0157;
- A Data Quality Report highlighting the quality of Practice data and irregularities.

7 Data Extraction from the Source System

7.1 Data Extraction from the Source System - Applicability

Stage 3 of the Data Migration Process requires an extract of the Practice's data and will be required where the Practice currently uses an electronic GP clinical IT system.

- 7.1.1 The Supplier of the Source System or the Data Extract Supplier shall provide a fully documented Data Extract. Otherwise the Data Extract can either be provided by the Source or Target System Supplier where the Source System Supplier is not covered under GPSoC.

7.2 Data Extraction from the Source System - Service Description

The Data Extraction service shall include the provision of all medical records to be transferred, as defined in section 4.1 , in a format documented by the Source Supplier or Data Extract Supplier to the Target Supplier or the PCT at the instruction of the PCT.

- 7.2.1 Source Supplier or the Data Extract Supplier shall provide a minimum of 2 separate extracts of the Practice's data, including an initial sample set of data and a final Data Extract for Data Load, taken in accordance with the Supplier's Data Migration Approach and the timeline set out in the Practice's Data Migration Plan.
- 7.2.2 The Source Supplier or the Data Extract Supplier, in providing the Documented Data Extract, shall document in the Issues Log any irregularities that it is aware of which relate to how the particular Practice has entered data into its GP clinical IT system.
- 7.2.3 Where a Source Supplier is required to provide assistance, the Source Supplier shall provide the Data Extract to the Target Supplier in accordance with the Target Supplier's Data Migration plan, agreed in accordance with 5.3.5 . Any variation to the agreed Data Migration Plan shall not prevent the Source Supplier from providing the Data Extract given that at least 48 hours notice is provided.

7.3 Authority/PCT Roles and Responsibilities

- 7.3.1 The Authority shall adjudicate in the event of disputes between the Suppliers of the Source and Target Systems.
- 7.3.2 The PCT, based on the Practice's Patient Safety Assessment, shall confirm the choice of Supplier to provide the Data Extract.
- 7.3.3 PCTs shall provide at least 48 hours notice to the Source Supplier for a Data Extract.

7.4 Suppliers Roles and Responsibilities

7.4.1 Target System Supplier

7.4.2 Where the Source System Supplier is providing the Data Extract, the Target System Supplier shall provide specific instructions to the Source System Supplier as to when Data Extracts are to be taken.

7.4.3 The Target System Supplier shall make formal requests for engineering support from the Source System Supplier when required.

7.4.4 Data Extract Supplier

7.4.5 The Data Extract Supplier may be the Source System Supplier, Target System Supplier or a sub contractor to the Source or Target System Supplier

7.4.6 The Source System Supplier should provide an automated mechanism to allow any Supplier to extract the Data where the Source Supplier is not providing the Data Extract, as set out in section 4.1 , from the Source System. This can either take the form of the existing methods of the production of backup media, or the provision of a mechanism to extract the relevant practice data from a hosted system. The existing mechanism for the provision of a back up tape in the Practice, augmented by the provision of the necessary documentation, will meet this requirement.

7.4.7 The Data Extract Supplier shall undertake the data extraction from the Source System on a minimum of 2 separate occasions in accordance with the Practice Data Migration Plan.

7.4.8 The Source System Supplier shall provide documentation which clearly sets out the Data Extract data structures. The Data Extract Supplier shall document any irregularities which relate to how the particular Practice has entered data into the Source System.

7.4.9 The Data Extract Supplier shall provide the extracted data in an electronic format, encrypted employing cryptographic techniques which conform to NHS cryptographic standards (as issued by the Authority from time to time, NPFIT-ELIBR-AREL-DST-0025). Any encryption keys necessary to access the extracted data must be provided to the Practice.

7.4.10 Any extracted data must be managed as defined "Information Governance - baseline index Foundation Module" (NPFIT-FNT-TO-TIN-1031).

7.4.11 The Source System Supplier shall ensure that the Practice has unrestricted access, as required to their Source System data.

7.5 Practice Roles and Responsibilities

7.5.1 The Practice shall ensure that a verified and encrypted Source System data back up is produced at the same time as the final data extract from the Source System.

7.6 Data Extraction from the Source System - Output

- A fully documented Data Extract supplied encrypted in an electronic format by the Source System Supplier.
- Confirmation from the Data Extract Supplier that the Data Extract contains the full set of patient records including document attachments, scanned images, etc.
- Confirmation from the Practice that the last system back up prior to Business Go-Live of the Target system has been verified to include the full set of patient records and audit trail for the Source System, see section 11.5 .

8 Data Transformation

8.1 Data Transformation Service - Applicability

Stage 4 of the Data Migration Process requires the Data to be transformed and can proceed once a Data Extract has been obtained by the Target System Supplier.

8.2 Data Transformation - Service Description

- 8.2.1 The Supplier shall be required to map data from the Source System to a format which can be loaded onto the Target System. Where non-standard codes have been identified, the Practice will be required to map these codes as part of stage 2, Data Cleansing.
- 8.2.2 The Supplier shall provide the Practice with access to the Transformed Data and a trial environment in order that it may check the integrity of the Transformed Data.
- 8.2.3 The Supplier shall undertake as many iterations of Data Extraction and Data Transformation as are required to assure the Practice that all omissions, errors and irregularities are addressed prior to system Go-Live.

8.3 Authority/PCT Roles and Responsibilities

- 8.3.1 The Authority shall consider requests for changes or additions to code sets where the Data Transformation process identifies a genuine deficiency.

8.4 Supplier Roles and Responsibilities

- 8.4.1 The Target System Supplier shall ensure that the transformation process is controlled by adherence to the compliant Data Migration approach.
- 8.4.2 The Supplier shall produce a detailed Patient Data Mapping document showing relationships between Source and Target System fields and clearly illustrating any limitations, assumptions and work rounds which will relate to the migrated patient data. This document may be subject to review by the Authority. This document also needs to be subject to formal change control and configuration management as changes are likely to be made almost on a per Practice basis so they will need to be formally tracked.
- 8.4.3 The Supplier shall conduct rigorous and comprehensive testing of all proposed Data Transformation processes both manual and automated, using appropriate samples of real and test data.
- 8.4.4 Suppliers shall provide a set of mapping tables from their specific Supplier defined codes to the standard data code sets where applicable.
- 8.4.5 Where clinical information coded under one coding system is translated to codes in another coding system meaning may be altered in a way that could affect patient safety. This should be considered both for human and for machine reading of the record. Change of meaning is a clinical safety hazard with the potential to cause harm and may affect either in isolation or both together -

- automated translations should only occur where there is a clear 1:1 map between the coding systems for the concept represented on the source system;
- where there is no exact 1:1 map the entry should be degraded to human readable text and no machine readable code should be added to the target system;
- the original text of the concept on the source system must always be preserved;
- consideration should be given to the handling of the *term + code + termID* triad as there may be implications for future interoperability (e.g. refer to GP2GP clinical safety assurance documentation for details).

8.4.6 Prior to commencement of the Data Transformation stage, the Supplier shall present a test report covering the work conducted to prove the transformation approach, as part of achieving Compliance. This report shall form part of the future Go/No-Go criteria at the end of this stage, before the launch of the Data Load Stage of the project. The report shall be provided to NHS CFH, the Practice and the PCT for review as part of achieving Compliance.

8.4.7 The Supplier shall propose and agree with the Practice a combination of checks, balances and reconciliations sufficient to automate a large majority of key clinical Data Transformations. Consideration shall be given to the use of batch controls during Data Transformation including hash totals, batch totals, parity fields and checksums.

8.4.8 The Supplier shall ensure that checks, balances and reconciliations are in place to ensure that the clinical semantic and syntactic meaning of the Source Data is preserved.

8.4.9 The Supplier shall implement a series of data integrity checks on the Data Extract.

8.4.10 The Target System Supplier shall create and maintain a stable and documented file format for data entry onto the Target System.

8.4.11 The Target System Supplier shall ensure that the Data Transformation routines contain algorithms to detect and reject erroneous data which will not map into the Target System data set or is incomplete in any way.

8.4.12 The Target Systems Supplier shall create procedures and suspense files to control and correct any data which is rejected by the Data Transformation activity.

8.4.13 The Target System Supplier or third party supplier shall transform the Source Data from the Data Extract into the format required to load the data onto the Target System.

8.4.14 The Target System Supplier or third party supplier shall load the Transformed Data into a trial environment and produce an agreed series of summary reports, as set out in 4.5, to evidence completeness, correctness and accuracy of Transformed Data.

- 8.4.15 The Target System Supplier shall conduct as many iterations of the transformation and trial load activity as are required to address, to the satisfaction of the Practice, all of the errors, omissions and irregularities found.
- 8.4.16 The Target System Supplier shall record in the Issue Log the errors, omissions and irregularities found and set out how each will be resolved whether by adapting the Data Transformation activity or as part of the Practice's data cleansing activities.
- 8.4.17 The Target System Supplier shall check the final cut of Transformed Data and provide the Practice with access to the Transformed Data for review and sign off.
- 8.4.18 The Target System Supplier shall supply and import a full and complete set of extracted data (including attachments) into a trial environment for Practice checking during the Data Transformation stage of the migration process.
- 8.4.19 The Target System Supplier or third party supplier shall provide the Practice with sufficient data, tools and access to the trial environment to enable the Practice to check the Transformed Data for errors, omissions and irregularities as set out in Appendix A.
- 8.4.20 The Data Extract Supplier shall provide Data Extracts as requested by the Target System Supplier.
- 8.4.21 The Data Extract Supplier shall carry out data integrity checks on the Data Extract to ensure that it is complete, uncorrupted and in the correct format for the migration
- 8.4.22 The Data Extract Supplier shall provide clinical and technical support as required to address any issues, errors and irregularities found in the Data Extract and/or the Transformed Data.

8.5 Practice Roles and Responsibilities

- 8.5.1 The Practice shall conduct checks on the Transformed Data. The Supplier shall support the Practice in this activity by providing the checklist, in line with NHS CFH Transformation and Cleansing Guidance for GP Data Migrations, NPFIT-FNT-TO-DQM-0161. Any additional checks that the Practice may identify in the Clinical Safety Case should also be conducted. The Practice should ensure that there is the appropriate resource made available to resolve any issues discovered.
- 8.5.2 Practices shall be responsible for reviewing and validating the translation of all clinical codes used in the Source System into those to be used in the Target System.
- 8.5.3 The Practice shall perform an independent end-to-end audit and sampling of the Transformed Data set as agreed in the Clinical Safety case.
- 8.5.4 Where non-standard codes have been identified, the Practice will be required to map these codes to the relevant coding system.

8.5.5 Once the Issue Log has been reviewed by the PCT and the Practice and approval for Business Go-Live has been provided by the PCT on behalf of the Practice, which will also require a final sign off by the Practice, the Supplier shall obtain a final Data Extract.

8.5.6 The Practice shall sign off the final cut of Transformed Data prior to Approval for Business Go-Live to indicate that:

- the Practice's review of the Transformed Data set has been completed and has not raised any significant Clinical Safety concerns;
- adequate evidence has been provided by the Supplier to the Practice, to evidence the implementation of the controls set out within the Clinical Safety Case;
- any work off plan put forward by the Supplier does not contain any significant Clinical Safety issues;
- all anomalies have been reviewed by the Practice and corrections applied.
- all errors, omissions and irregularities in the Issue Log have been addressed prior to Business Go-Live.

8.6 Data Transformation - Output

- Updated Issue Log setting out how any errors, omissions and irregularities have been addressed;
- Practice approved cut of Transformed Data for Business Go-Live;
- Confirmation from the Practice to the Authority (via the PCT) that the Data Transformation has been signed off.

9 Data Load into the Target System

9.1 Data Load into the Target System - Applicability

Stage 5 of the Data Migration Process is the loading of the Transformed Data into the Target System and shall take place from Data Extract through to Data Load and, finally, when the Practice is ready to Go-Live.

9.2 Data Load into the Target System Service Description

9.2.1 The Supplier shall load the Transformed Data into the Target System and provide a business continuity service. The Practice shall verify that the data that has been migrated.

9.3 Authority/PCT Roles and Responsibilities

9.3.1 The PCT and NHS CFH shall sign off the Deployment Verification Report on behalf of the Practice following the Deployment Verification period.

9.4 Supplier Roles and Responsibilities

Target System Supplier

9.4.1 The Supplier shall ensure that the business continuity plan, as per section 4.2 , and cut over plans are in place. The cut over plan shall describe the activities that all parties perform during the cut-over period between the final Data Extract and Target Business Go-Live.

9.4.2 The Target System Supplier shall load the Transformed Data onto the Target System. The cut over period between the final Data Extract and Target System Business Go-Live shall be no more than 5 calendar days.

9.4.3 The Target System Supplier shall clearly set out the method by which the Practice will record patient data during the cut-over period.

9.4.4 The Target System Supplier shall Go-Live with the Target System following receipt of the necessary PCT and Practice approvals as set out in 8.5 .

9.4.5 The Target System Supplier shall work with the Practice to load and verify the data recorded by the Practice during the cut-over period onto the live Target System.

9.4.6 The Target System Supplier shall prepare the Deployment Verification Report following completion of the Deployment Verification period. The Deployment Verification Report shall be submitted for review by the Practice against the Deployment Verification Criteria before submission to the authority as part of Compliance or PCT (subsequent migrations).

Source System Supplier

9.4.7 The Source System Supplier may be required to provide a final Data Extract on completion of the cut-over period.

9.5 Practice Roles and Responsibilities

- 9.5.1 The Practice shall record patient data during the cut-over period prior to Target System Go-Live in accordance with the Target System Supplier's instructions.
- 9.5.2 The Practice shall perform a data verification of the completed Data Load, using tools provided by the Target System Supplier, in the manner defined in the Clinical Safety Case.
- 9.5.3 The Practice shall approve Go-Live in conjunction with the PCT.
- 9.5.4 The Practice shall monitor the Deployment Verification Criteria.
- 9.5.5 The Practice shall review the Deployment Verification Report and confirm successful completion of the Deployment Verification Period to the PCT.

9.6 Data Load into the Target System Output

- Live Target System;
- Update to mapping tables, migration process and lessons learned as applicable;
- Deployment Verification Report signed off by the PCT;
- Safety Closure Report produced by the Supplier.

10 Retention of the Source System

10.1 Retention of the Source System - Applicability

10.1.1 Stage 6 of the Data Migration Process is where the Practice may require access to the Source System for a period following Business Go-Live with the Target System. Two examples of why this may be required are:

- to access data to support medico-legal cases;
- to enable extraction of additional data from the Source System for the cut-over period between the final Data Extract and Business Go-Live with the Target System.

10.1.2 The period of system retention should be agreed by the PCT, the Practice and the Supplier of the Source System.

10.2 Retention of the Source System - Service Description

10.2.1 The Supplier of the Source System shall continue to provide the Practice with access to the Source System and support for a run off period which will be agreed under the terms of the GPSoC Call Off Agreement or relevant existing contract with the Supplier of the Source System.

10.2.2 The expectation is that such access will be required for up to 3 months from Business Go-Live with the actual duration to be agreed by the PCT, the Practice and the Supplier of the Source System. If longer term access to the Source System is required on an ad hoc basis, such access shall be part of the provision in section 11 of Data and Audit Trail Retrieval.

10.2.3 The Supplier of the Source System shall continue to support the source system from Business Go-Live where requested by the PCT or the Practice. Access to the Source system will not be for everyday Practice use and the volume of access should demonstrate this.

10.3 Authority/PCT Roles and Responsibilities

10.3.1 The PCT shall agree the run off period for the Source System with the Practice.

10.3.2 The PCT shall issue a Change Control Notice against the relevant Call Off Agreement, or existing contract with the Supplier of the Source System, to confirm the amended requirement for the system and support services and the required run off period, making provisions for an extension of the run off period in the event that this is required.

10.3.3 NHS CFH funding for the previous GPSoC System will cease 2 months after the Business Go Live date for the new system in the practice. If the planned Business Go Live date is delayed, the PCT will need to notify the exiting GPSoC supplier of the revised Business Go Live date. NHS CFH funding will then be available for 2 months after the revised Business Go Live date.

10.3.4 There are three options available to a practice following migration from the source system:

- the practice retains the source system (Retention of Source System Service) with a reduced level of support from the supplier. The PCT will need to terminate the existing GPSoC Core Service in the practice and take up the lower cost Retention of Source System Service. The PCT will need to give notice to the source supplier no less than 1 month before the planned Business Go Live date for the target system, as the minimum notice period under the GPSoC agreements is 3 months and NHS CFH will not fund the Source System for more than 2 months after Business Go Live. The PCT should order the Retention of Source System service to commence immediately after the completion of the notice period for the source service.
- the practice retains the source system with full support for more than 2 months after Business Go Live.
- remove the source system and call on the Data and Audit Trail Retrieval service from the source supplier if the PCT or Practice require data from the source system to be restored from a final back up tape or other storage medium. The PCT will need to give notice to the source supplier no less than 1 month before the planned Business Go Live date for the target system, as the minimum notice period under the GPSoC agreements is 3 months and NHS CFH will not fund the Source System for more than 2 months after Business Go Live. The Data and Audit Trail Retrieval service can be ordered on an ad hoc basis to allow the practice to access different aspects of the medical record using the same screen presentations as would have been available to the practice at the time the final data extract from the source system (e.g. if required by the practice to defend a medico legal case).

10.4 Supplier Roles and Responsibilities

10.4.1 The Source System Supplier shall continue to provide services to the Practice in accordance with the amended contract.

10.4.2 The Data Extract Supplier shall provide a final Data Extract, as detailed in section 7 .

10.4.3 The Source System Supplier shall decommission the applicable and relevant services supplied to the Practice upon completion of the run off period ensuring that data is kept secure until it may be securely deleted.

10.5 Practice Roles and Responsibilities

10.5.1 Ten days before the completion of the run off period, the Practice shall confirm to the PCT that the Source System can be decommissioned or agree an extension with the PCT.

10.6 Retention of the Source System - Output

- Decommissioned Source System;
- A fully documented Data Extract supplied encrypted in an electronic format by the Source System Supplier.

11 Data and Audit Trail Retrieval

11.1 Data and Audit Trail Retrieval - Applicability

11.1.1 Stage 7 of the Data Migration Process provides Practices, for medico-legal purposes, with access to the medical records contained in the Source System together with the associated audit trail following any migration where the audit trail has not been transferred to the Target System.

11.1.2 The expectation is that such access will be required on an ad hoc basis and that the specific requirements associated with the retention and retrieval of data will be confirmed in line with developing Department of Health policy and professional requirements.

11.2 Data and Audit Trail Retrieval - Service Description

11.2.1 To support possible Department of Health policy the Supplier (or another third party supplier) shall provide a service which enables the Practice to access all medical records and associated audit trail stored on the Source System at the time of the final Data Extract.

11.2.2 The final Data Extract shall be loaded into the version of the Source System which was in use at the time that the Data Extract was taken, providing the Practice with access to its data in the form that it would have last seen the data in the Source System.

11.2.3 The service provided will enable the Practice to access different aspects of the medical record using the same screen presentations as would have been available to the Practice at the time the final Data Extract was taken.

11.3 Authority/PCT Roles and Responsibilities

11.3.1 The Authority shall confirm Department of Health policy in respect of Data and Audit Trail Retrieval and set out the requirement for this service in line with that policy.

11.3.2 The Authority shall ensure that the method of access to Practice data enables continuing access to the data in the event that the Supplier or third party supplier ceases to trade.

11.3.3 The PCT shall contract for the Data and Audit Trail Retrieval service on behalf of the relevant Practice and ensure that there is a secure repository for the Practice's Source System data.

11.4 Supplier Roles and Responsibilities

11.4.1 The Supplier/third party supplier shall provide the access to the requested data, using the Data and Audit Trail Retrieval service, within 3 days of receiving a formal request from the PCT.

11.4.2 The Supplier/third party supplier shall conduct a test load of the final Data Extract which shall be approved by the Practice as an accurate representation of the Practice's data.

11.5 Practice Roles and Responsibilities

11.5.1 The Practice shall ensure that a secure copy of the final Data Extract is stored.

11.5.2 The Practice shall review and approve the accuracy of its data following a test load of the final Data Extract by the Supplier/third party supplier.

11.6 Data and Audit Trail Retrieval - Output

- Arrangements in place for Practice access to Source System data and audit trail for that Practice.

12 Post Go-Live Data Quality

12.1 Post Go-Live Data Quality - Applicability

12.1.1 Stage 8 of the Data Migration Process ensures that Practice's should have plans in place to maintain data quality post-migration and to address any known issues with the Practice data identified at the time of migration to the Target System.

12.2 Post Go-Live Data Quality - Service Description

12.2.1 The Practice has responsibility for maintaining and improving data quality on the Target System. The Practice, through the PCT, may commission services from the Supplier or a third party supplier to assist the Practice in this activity.

12.3 Authority/PCT Roles and Responsibilities

12.3.1 The PCT shall provide facilitators in line with the requirements of the Direct Enhanced Services to assist the Practice in improving data quality.

12.4 Supplier Roles and Responsibilities

12.4.1 Where the Supplier or a third party supplier has been commissioned to assist with the data cleansing activity the Supplier shall provide data reports and checklists produced in respect of the live data to assist the Practice in the data cleansing activity.

12.4.2 Following a significant migration and data cleanse the Supplier shall provide:

- a suitable set of automated reports and checks to allow the Practice to continue monitoring data quality for an agreed period of time following initial data load and Business Go-Live;
- on call resource to resolve critical data issues post Business Go-Live;
- a routine set of data quality checks, reports and balances to support on going data quality improvement by the Practice.

12.5 Practice Roles and Responsibilities

12.5.1 The Practice shall amend live data in the Target System in order to improve the quality of coding and data entered into the Target System.

12.6 Post Go-Live Data Quality - Output

- Practice data that has been validated in line with the approved data accreditation standards.
- Any outstanding data anomalies have been addressed and resolved. This should be performance managed by PCT.

Appendix A – Source Data Checks

[DN: To be populated by Supplier with example reports etc]

Appendix B – Product Descriptions

DN: Note that populated versions of the Patient Safety Assessment and Clinical Safety Case are available as input into target supplier's clinical safety products.



Patient Safety
Assessment template



Clinical Safety Case
template



Safety Closure
Report template

GPSoC Data Migration Specification

NPFIT-PC-PMG-DEL-0020.07

23/07/2008 APPROVED V2.0

Appendix C – Data Migration Deliverables

DN: Suppliers are requested to complete the 'Supplier equivalent deliverable' column with the names of the Suppliers equivalent products. Unless stated, the Supplier referenced here is the Target Supplier.

CAPGP Stage	DM Stage	Deliverable	Description	Responsible	Template	Supplier Deliverable	Equivalent
Initiation	1	Project Initiation Document		Supplier	Y		
Initiation	1	Data Migration Plan		Supplier			
General	1	Data Migration Process		Supplier			
General	4	Mapping Tables		Supplier			
Initiation	1	Issue Log		Supplier			
Initiation	2	Data Improvement Plans		Practice			
Initiation	2	Data Quality Report		Supplier			
Prep for Go-Live	All	Patient Safety Assessment		Supplier	Y		
Prep for Go-Live	All	Clinical Safety Case		Supplier	Y		
Prep for Go-Live	All	Clinical Safety Closure Report		Supplier	Y		
Prep for Go-Live	3	Validated Data Extract		Supplier (or Source Supplier)			
Prep for Go-Live	4	Test Report		Supplier			
Prep for Go-Live	4	Site Readiness Criteria		Supplier	Y		
Prep for Go-Live	4	File Format		Supplier			
Prep for Go-Live	4	Signed off Transformed Data		Supplier			
Prep for Go-Live	4	Approval for Go-Live		Supplier			
Prep for Go-Live	5	Business Continuity Plan		Supplier			
Prep for Go-Live	5	Cut Over Plan		Supplier			
Deployment Verification	5	Deployment Verification Report		Supplier	Y		
Deployment Verification	6	Final Source Data Extract		Supplier (or Source)			

GPSoC Data Migration Specification

NPFIT-PC-PMG-DEL-0020.07

23/07/2008 APPROVED V2.0

CAPGP Stage	DM Stage	Deliverable	Description	Responsible	Template	Supplier Deliverable	Equivalent
				Supplier)			
Deployment Verification	6	Decommissioned System		Source Supplier			
Deployment Verification	7	Access to audit Trail in Source system		Source Supplier			
Deployment Verification	8	Data Quality Improvement Plan in line with standards		Practice			