SCHEDULE 8.6

BUSINESS CONTINUITY AND DISASTER RECOVERY

1 DEFINITIONS

1.1. In this Schedule, the following definitions shall apply:

"Business Continuity Plan"	has the meaning given in Paragraph 2.2(a)(ii);
"Business Continuity Services"	has the meaning given in Paragraph 4.2(b);
"Disaster"	the occurrence of one or more events which, either separately or cumulatively, mean that the Services, or a material part of the Services will be unavailable for period of 24 hours or which is reasonably anticipated will mean that the Services or a material part of the Services will be unavailable for that period;
"Disaster Recovery Plan"	has the meaning given in Paragraph 2.2(a)(iii);
"Disaster Recovery Services"	the services embodied in the processes and procedures for restoring the Services following the occurrence of a Disaster;
"Disaster Recovery System"	the system identified by the Supplier in the Supplier Solution which shall be used for the purpose of delivering the Disaster Recovery Services;
"Related Service Provider"	any person who provides services to the Authority in relation to this Agreement from time to time.

2 BCDR PLAN

2.1. Within 120 Working Days from the Effective Date the Supplier shall prepare and deliver to the Authority for the Authority's written approval a plan, which shall address the Authority's requirements set out in Annex 2 of this Schedule 8.6 and detail the processes and arrangements that the Supplier shall follow to:

(a) ensure continuity of the business processes and operations supported by the Services following any failure or disruption of any element of the Services; and

(b) the recovery of the Services in the event of a Disaster.

2.2. The BCDR Plan shall:

(a) be divided into three parts:

(i) Part A which shall set out general principles applicable to the BCDR Plan;

(ii) Part B which shall relate to business continuity (the **"Business Continuity Plan"**);

(iii) Part C which shall relate to disaster recovery (the **"Disaster Recovery Plan"**); and

(b) unless otherwise required by the Authority in writing, be based upon and be consistent with the provisions of Paragraphs 3, 4 and 5.

2.3. Following receipt of the draft BCDR Plan from the Supplier, the Authority shall:

(a) review and comment on the draft BCDR Plan as soon as reasonably practicable; and

(b) notify the Supplier in writing that it approves or rejects the draft BCDR Plan no later than 20 Working Days after the date on which the draft BCDR Plan is first delivered to the Authority.

2.4. If the Authority rejects the draft BCDR Plan:

(a) the Authority shall inform the Supplier in writing of its reasons for its rejection; and

(b) the Supplier shall then revise the draft BCDR Plan (taking reasonable account of the Authority's comments) and shall re-submit a revised draft BCDR Plan to the Authority for the Authority's approval within 20 Working Days of the date of the Authority's notice of rejection. The provisions of Paragraph 2.3 and this Paragraph 2.4 shall apply again to any resubmitted draft BCDR Plan, provided that either Party may refer any disputed matters for resolution by the Dispute Resolution Procedure at any time.

3 PART A OF THE BCDR PLAN AND GENERAL PRINCIPLES AND REQUIREMENTS

3.1. Part A of the BCDR Plan shall:

(a) set out how the business continuity and disaster recovery elements of the Plan link to each other;

(b) provide details of how the invocation of any element of the BCDR Plan may impact upon the operation of the Services and any services provided to the Authority by a Related Service Provider;

(c) contain an obligation upon the Supplier to liaise with the Authority and (at the Authority's request) any Related Service Provider with respect to issues concerning business continuity and disaster recovery where applicable;

(d) detail how the BCDR Plan links and interoperates with any overarching and/or connected disaster recovery or business continuity plan of the Authority and any of its other Related Service Providers in each case as notified to the Supplier by the Authority from time to time;

(e) contain a communication strategy including details of an incident and problem management service and advice and help desk facility which can be accessed via

multi-channels (including but without limitation a web-site (with FAQs), e-mail and phone) for both portable and desk top configurations, where required by the Authority;

(f) detail how the BCDR Plan should be used for training purposes and for reference during an actual invocation or rehearsal;

(g) reference that the Authority will maintain a closely linked set of documents that outline their own processes, especially re. communications to User Organisation executives;

(h) contain a risk analysis, including:

(i) failure or disruption scenarios and assessments and estimates of frequency of occurrence;

(ii) identification of any single points of failure within the Services and processes for managing the risks arising therefrom;

(iii) identification of risks arising from the interaction of the Services with the services provided by a Related Service Provider; and

(iv) a business impact analysis (detailing the impact on business processes and operations) of different anticipated failures or disruptions;

(i) provide for documentation of processes, including business processes, and procedures;

(j) set out key contact details (including roles and responsibilities) for the Supplier (and any Sub-contractors) and for the Authority;

(k) identify the procedures for reverting to "normal service";

(l) set out method(s) of recovering or updating data collected (or which ought to have been collected) during a failure or disruption (incorporating the expected recovery times set out in Annex 3 of this Schedule 8.6) to ensure that there is no more than the accepted amount of data loss and to preserve data integrity;

(m) identify the responsibilities (if any) that the Authority has agreed it will assume in the event of the invocation of the BCDR Plan; and

(n) provide for the provision of technical advice and assistance to key contacts at the Authority as notified by the Authority from time to time to inform decisions in support of the Authority's business continuity plans.

3.2. The BCDR Plan shall be designed so as to ensure that:

(a) the Services are provided in accordance with this Agreement at all times during and after the invocation of the BCDR Plan;

(b) the adverse impact of any Disaster, service failure, or disruption on the operations of the Authority is minimal as far as reasonably possible;

(c) it complies with the relevant provisions of ISO/IEC 27002 and all other industry standards from time to time in force; and

(d) there is a process for the management of disaster recovery testing detailed in the BCDR Plan.

3.3. The BCDR Plan shall be upgradeable and sufficiently flexible to support any changes to the Services or to the business processes facilitated by and the business operations supported by the Services.

3.4. The Supplier shall not be entitled to any relief from its obligations under the Performance Indicators or to any increase in the Charges to the extent that a Disaster occurs as a consequence of any breach by the Supplier of this Agreement.

4 BUSINESS CONTINUITY PLAN - PRINCIPLES AND CONTENTS

4.1. The Business Continuity Plan shall set out the arrangements that are to be invoked to ensure that the business processes and operations facilitated by the Services remain supported and to ensure continuity of the business operations supported by the Services including, unless the Authority expressly states otherwise in writing:

(a) the alternative processes (including business processes), options and responsibilities that may be adopted in the event of a failure in or disruption to the Services; and

(b) the steps to be taken by the Supplier upon resumption of the Services in order to address any prevailing effect of the failure or disruption including a root cause analysis of the failure or disruption.

4.2. The Business Continuity Plan shall:

(a) address the various possible levels of failures of or disruptions to the Services;

(b) set out the services to be provided and the steps to be taken to remedy the different levels of failures of and disruption to the Services (such services and steps, the "**Business Continuity Services**");

(c) specify any applicable Performance Indicators with respect to the provision of the Business Continuity Services and details of any agreed relaxation to the Performance Indicators in respect of other Services during any period of invocation of the Business Continuity Plan; and

(d) clearly set out the conditions and/or circumstances under which the Business Continuity Plan is invoked.

5 DISASTER RECOVERY PLAN - PRINCIPLES AND CONTENTS

5.1. The Disaster Recovery Plan shall be designed so as to ensure that upon the occurrence of a Disaster the Supplier ensures continuity of the business operations of the Authority supported by the Services following any Disaster or during any period of service failure or disruption with, as far as reasonably possible, minimal adverse impact.

5.2. The Disaster Recovery Plan shall be invoked only upon the occurrence of a Disaster.

5.3. The Disaster Recovery Plan shall include the following:

(a) The technical design and build specification of the Disaster Recovery System;

(b) details of the procedures and processes to be put in place by the Supplier in relation to the Disaster Recovery System and the provision of the Disaster Recovery Services and any testing of the same including but not limited to the following:

(i) data centre and disaster recovery site audits;

(ii) backup methodology and details of the Supplier's approach to data backup and data verification;

(iii) identification of all potential disaster scenarios;

(iv) risk analysis;

(v) documentation of processes and procedures;

(vi) hardware configuration details;

(vii) network planning including details of all relevant data networks and communication links;

(viii) invocation rules;

(ix) Service recovery procedures and timetable; and

(x) steps to be taken upon resumption of the Services to address any prevailing effect of the failure or disruption of the Services;

(c) any applicable Performance Indicators with respect to the provision of the Disaster Recovery Services and details of any agreed relaxation to the Performance Indicators in respect of other Services during any period of invocation of the Disaster Recovery Plan;

(d) details of how the Supplier shall ensure compliance with security standards ensuring that compliance is maintained for any period during which the Disaster Recovery Plan is invoked;

(e) access controls to any disaster recovery sites used by the Supplier in relation to its obligations pursuant to this Schedule;

(f) special delivery instructions for Printed output;

(g) proposed organisational structure;

(h) testing and management arrangements; and

(i) normal Service resumption procedures and timescales following rectification of the

Disaster event.

6 REVIEW AND AMENDMENT OF THE BCDR PLAN

6.1. The Supplier shall review and maintain the BCDR Plan (and the risk analysis on which it is based):

(a) on a regular basis and as a minimum once every 6 months;

(b) within three calendar months of the BCDR Plan (or any part) having been invoked pursuant to Paragraph 8; and

(c) where the Authority requests any additional reviews (over and above those provided for in Paragraphs 6.1(a) and 6.1(b)) by notifying the Supplier to such effect in writing, whereupon the Supplier shall conduct such reviews in accordance with the Authority's written requirements. Prior to starting its review, the Supplier shall provide an accurate written estimate of the total costs payable by the Authority for the Authority's approval. The costs of both Parties of any such additional reviews shall be met by the Authority except that the Supplier shall not be entitled to charge the Authority for any costs that it may incur above any estimate without the Authority's prior written approval.

6.2. Each review of the BCDR Plan pursuant to Paragraph 6.1 shall be a review of the procedures and methodologies set out in the BCDR Plan and shall assess their suitability having regard to any change to the Services or any underlying business processes and operations facilitated by or supported by the Services which have taken place since the later of the original approval of the BCDR Plan or the last review of the BCDR Plan and shall also have regard to any occurrence of any event since that date (or the likelihood of any such event taking place in the foreseeable future) which may increase the likelihood of the need to invoke the BCDR Plan. The review shall be completed by the Supplier within the period required by the BCDR Plan or, if no such period is required, within such period as the Authority shall reasonably require. The Supplier shall, within 20 Working Days of the conclusion of each such review of the BCDR Plan, provide to the Authority a report (a **"Review Report"**) setting out:

(a) the findings of the review;

(b) any changes in the risk profile associated with the Services; and

(c) the Supplier's proposals (the **"Supplier's Proposals"**) for addressing any changes in the risk profile and its proposals for amendments to the BCDR Plan following the review detailing the impact (if any and to the extent that the Supplier can reasonably be expected to be aware of the same) that the implementation of such proposals may have on any services or systems provided by a third party.

6.3. Following receipt of the Review Report and the Supplier's Proposals, the Authority shall:

(a) review and comment on the Review Report and the Supplier's Proposals as soon as reasonably practicable; and

(b) notify the Supplier in writing that it approves or rejects the Review Report and the

Supplier's Proposals no later than 20 Working Days after the date on which they are first delivered to the Authority.

6.4. If the Authority rejects the Review Report and/or the Supplier's Proposals:

(a) the Authority shall inform the Supplier in writing of its reasons for its rejection; and

(b) the Supplier shall then revise the Review Report and/or the Supplier's Proposals as the case may be (taking reasonable account of the Authority's comments and carrying out any necessary actions in connection with the revision) and shall re-submit a revised Review Report and/or revised Supplier's Proposals to the Authority for the Authority's approval within 20 Working Days of the date of the Authority's notice of rejection. The provisions of Paragraph 6.3 and this Paragraph 6.4 shall apply again to any resubmitted Review Report and Supplier's Proposals, provided that either Party may refer any disputed matters for resolution by the Dispute Resolution Procedure at any time.

6.5. The Supplier shall as soon as is reasonably practicable after receiving the Authority's approval of the Supplier's Proposals (having regard to the significance of any risks highlighted in the Review Report) effect any change in its practices or procedures necessary so as to give effect to the Supplier's Proposals. Any such change shall be at the Supplier's expense unless it can be reasonably shown that the changes are required because of a material change to the risk profile of the Services.

7 TESTING OF THE BCDR PLAN

7.1. The Supplier shall test the BCDR Plan on a regular basis (and in any event not less than once in every Contract Year). Subject to Paragraph 7.2, the Authority may require the Supplier to conduct additional tests of some or all aspects of the BCDR Plan at any time where the Authority considers it necessary, including where there has been any change to the Services or any underlying business processes, or on the occurrence of any event which may increase the likelihood of the need to implement the BCDR Plan.

7.2. If the Authority requires an additional test of the BCDR Plan, it shall give the Supplier written notice and the Supplier shall conduct the test in accordance with the Authority's requirements and the relevant provisions of the BCDR Plan. The Supplier's costs of the additional test shall be borne by the Authority unless the BCDR Plan fails the additional test in which case the Supplier's costs of that failed test shall be borne by the Supplier.

7.3. The Supplier shall undertake and manage testing of the BCDR Plan in full consultation with the Authority and shall liaise with the Authority in respect of the planning, performance, and review, of each test, and shall comply with the reasonable requirements of the Authority in this regard. Each test shall be carried out under the supervision of the Authority or its nominee.

7.4. The Supplier shall ensure that any use by it or any Sub-contractor of "live" data in such testing is first approved with the Authority. Copies of live test data used in any such testing shall be (if so required by the Authority) destroyed or returned to the Authority on completion of the test.

7.5. The Supplier shall, within 20 Working Days of the conclusion of each test, provide to the SMB a report setting out:

(a) the outcome of the test;

(b) any failures in the BCDR Plan (including the BCDR Plan's procedures) revealed by the test; and

(c) the Supplier's proposals for remedying any such failures.

7.6. Following each test, the Supplier shall take all measures requested by the Authority, (including requests for the re-testing of the BCDR Plan) to remedy any failures in the BCDR Plan and such remedial activity and re-testing shall be completed by the Supplier, at no additional cost to the Authority, by the date reasonably required by the Authority and set out in such notice.

7.7. For the avoidance of doubt, the carrying out of a test of the BCDR Plan (including a test of the BCDR Plan's procedures) shall not relieve the Supplier of any of its obligations under this Agreement.

7.8. The Supplier shall also perform a test of the BCDR Plan in the event of any major reconfiguration of the Services or as otherwise reasonably requested by the Authority.

8 INVOCATION OF THE BCDR PLAN

8.1. In the event of a complete loss of service, or in the event of a Disaster, the Supplier shall immediately invoke the BCDR Plan (and shall inform the Authority promptly of such invocation). In all other circumstances, the Supplier shall inform the Authority and seek consent to invoke the BCDR Plan and the Supplier shall not invoke or test the BCDR Plan without the prior consent of the Authority.

ANNEX 1 - FACILITATION OF THE BCDR PLAN

1. In addition to backups taken as part of housekeeping, and in line with the BCDR Plan, the Supplier will ensure a nightly system backup will be taken of the following which will then be moved to secure off-site storage:

1.1. the ESR Production Solution in the Production Data Centre; and

1.2. the ESR Disaster Recovery Solution in the Disaster Recovery Data Centre.

2. Security copies will be stored at a separate site from the hardware, and retained for a period reasonably agreed with the Authority. A log of off-site security copies will be maintained.

3. The Supplier will regularly maintain:

3.1. an Asset Register as more particularly described in Schedule 2.1.

3.2. information describing how the Assets are utilised in the ESR Solution;

3.3. a library of complete and accurate information enabling the on-going operation and maintenance of the Solution that would enable the complete re-creation/re-build of the Solution;

3.4. this information to be supplied to the Authority on a quarterly basis.

ANNEX 2 - AUTHORITY REQUIREMENTS FOR THE BCDR PLAN

1. The Authority requires:

1.1. Provision of a separately located Disaster Recovery System for the ESR System, provided to support Disaster Recovery Services;

1.2. Disaster Recovery Services providing recovery within the permissible recovery time set out in Annex 3 including all relevant archive logs;

1.3. Provision of an infrastructure that supports performance and regression testing where the Supplier shall provide the equivalent of 100% of the ESR Production Solution;

1.4. That Disaster Recovery Services are available for the entire ESR Production Solution unless stated otherwise.

2. It is envisaged that the Supplier infrastructure supporting performance and regression testing may also support the Disaster Recovery Services.

3. The Supplier will provide that:

3.1. The ESR Solution will be sited and Services provided from a minimum of two data centres;

3.2. Disaster Recovery Services are in place for printing and courier services. In summary:

(a) As part of ESR Services, bureau printing (see Schedule 2.1, Section 4.7.5 "Timetables and Processing Control") will be provided with a Disaster Recovery server located at a separate location for printing and dispatch;

(b) In the event of a failure at the main site, ESR printing will be re-directed to the Disaster Recovery server; and

4. Disaster Recovery Services for the ESR Solution:

4.1. will build upon the inbuilt resilience of the ESR infrastructure to ensure full utilisation of the available systems;

4.2. will be achieved through a combination of backups and database log files, closely linked to the backup procedure set out in Annex 1 of this Schedule 8.6; and

4.3. will include recovery of the NHS Interface Hub infrastructure, system and application software and reconciliation of all live interfaces sent through it.

5. Disaster Recovery Services for NHS Interface Hub:

5.1. With regard to failover, the Supplier will ensure:

(a) In the event of a hardware failure on the primary processor system, or LAN (local area network) connection, there should be a failover processor and failover network connection available;

(b) Network connectivity must failover if the primary network connection fails;

(c) There will be no failover on the NHS Interface Hub DR infrastructure;

(d) The solution must continue to operate if a Hard Drive unit fails, and the data from the failed drive should remain available via the Raid (or equivalent) system; and

(e) The Perl scripting language must be available and operational.

5.2. In the event of a total unavailability of the production NHS Interface Hub, the Supplier will ensure:

(a) a warm Disaster Recovery service will be available that will involve a processor, network connectivity and storage (of equivalent level to the production server) being available at an alternate location. Changes to the file system on the primary server in the Production Data Centre should be copied across to the Disaster Recovery server within 30 minutes, enabling continuity of service in the event of a Disaster. In addition a full copy of operating system and application data should be copied to the Disaster Recovery Data Centre in each 24 hour period;

(b) as part of the annual Disaster Recovery test, the Supplier must demonstrate that updated files have been copied over from production to DR as required;

(c) in the event of a Disaster Recovery, the Disaster Recovery server needs to be available on the same URL and IP address that the ESR Production Solution uses or web browser and FTP connections, so that end users do not need to reconfigure anything to access the Disaster Recovery Services; and

(d) The necessary support should be available from the Supplier to enable the NHS Interface Hub service to be recovered on the ESR Disaster Recovery Solution whilst the ESR Production Solution is also being recovered on the ESR Disaster Recovery Solution.

ANNEX 3 – BCDR TABLE OF EXPECTED RECOVERY TIMES

Definitions for DR Requirement

Warm Standby

- Hardware for DR instance pre-defined.
- Operating System Environment pre-existing. May be live (running) or on a disc/backup
- Application, Configuration, Database, and/or Data available in a recent backup at DR site.
- For Production systems - most recent live Transactions and incoming/outgoing interface files secured at DR site. Maximum data loss of 15 minutes
- Full documentation available at DR Site to enable invocation of DR

Cold Standby

- Hardware for DR instance not necessarily pre-defined. In case of Disaster this will be identified from exiting pool of Hardware. Assumption that there will be sufficient Hardware for all DR instances to be created.
- Operating System Environment not predefined. Assumption that environment can be allocated/created with minimal delay.
- Application, Configuration, Database, and/or Data available in a recent backup at DR site.
- For Production systems - most recent live Transactions and incoming/outgoing interface files secured at DR site. Maximum data loss of 15 minutes
- Full documentation available at DR Site to enable invocation of DR

Information redacted under section 43 of the FOIA