Primary Care Support Services Call-Off Terms

Schedule 2.3

Standards

PCSS Call-Off Terms
Schedule 2.3 (Standards)

1. Definitions

Unless defined within this Schedule, or in the Call-Off Order Form applicable to this Call-Off Agreement, the definitions in Schedule 1 of the Framework Agreement shall apply.

2. General

2.1 Throughout the term of this Call-Off Agreement, the Parties shall monitor and notify each other of any new or emergent standards which could affect the Supplier's provision, or the Customer's receipt, of the Services. Any changes to the Standards, including the adoption of any such new or emergent standard or policy, shall be agreed in accordance with the Change Control Procedure.

2.2 Where a new or emergent standard or policy is to be developed or introduced by the Customer, the Supplier shall be responsible for ensuring that the potential impact on the Supplier's provision, or the Customer's receipt, of the Services is explained to the Customer (in a reasonable timeframe), prior to the implementation of the new or emergent standard or policy.

2.3 Where Standards referenced conflict with each other or with Good Industry Practice, then the later Standard or best practice shall be adopted as a minimum by the Supplier. Any such alteration to any Standard(s) shall require the prior written agreement of the Customer and shall be implemented within an agreed timescale.

3. Technology and Digital Services Practice

The Supplier shall (when designing, implementing and delivering the Services) adopt the applicable elements of HM Government's Technology Code of Practice as documented at https://www.gov.uk/service-manual/technology/code-of-practice.html.

4. Open Data Standards Hub

4.1 The Supplier shall comply to the extent within its control with UK Government's Open Standards Principles as documented at https://www.gov.uk/government/publications/open-standards-principles, as they relate to the specification of standards for software interoperability, data and document formats in the IT Environment.

4.2 Without prejudice to the generality of Paragraph 2.2, the Supplier shall, when implementing or updating a technical component or part of the Software or Supplier Solution where there is a requirement under this Call-Off Agreement or opportunity to use a new or emergent standard, submit a Suggested Challenge compliant with the UK Government's Open Standards Principles (using the process detailed on Standards Hub and documented at http://standards.data.gov.uk/). Each Suggested Challenge submitted by the Supplier shall detail, subject to the security and confidentiality provisions in this Call-Off Agreement, an illustration of such requirement or opportunity within the IT Environment, Supplier Solution and Government's IT infrastructure and the suggested open standard.

4.3   The Supplier shall ensure that all documentation published on behalf of the Customer pursuant to this Call-Off Agreement is provided in a non-proprietary format (such as PDF or OpenDocument Format (ISO/IEC 26300: 2006/Amd 1: 2012 or equivalent)) as well as any native file format documentation in accordance with the obligation under Paragraph 4.1 to comply with the UK Government's Open Standards Principles, unless the Customer otherwise agrees in writing.

5.   Technology Architecture Standards

5.1   The Supplier shall produce, and provide the Customer with a copy of, full and detailed technical architecture documentation for the Supplier Solution in accordance with Good Industry Practice (for example, TOGAF (The Open Group Architecture Framework)) by the applicable dates in the Transformation Plan (and in any event prior to the end of the Transformation Period).

5.2   Where the Supplier proposes any changes to the architecture documentation provided at paragraph 5.1 (**"Architecture Change"**) it shall follow the procedure detailed in paragraphs 5.3 to 5.5 below and shall not implement any proposed changes until such time as the Customer has approved them.

5.3   The Supplier shall submit its proposals for any Architecture Change (**"Architecture Change Proposal"**) to the Customer in writing.

5.4   Following receipt of the Architecture Change Proposal from the Supplier, the Customer shall:

5.4.1   review and comment on the Architecture Change Proposal; and

5.4.2   notify the Supplier in writing that it approves or rejects the draft Architecture Change Proposal no later than twenty (20) Working Days after the date on which the draft Architecture Change Proposal is first delivered to the Customer.

5.5   If the Customer rejects the Architecture Change Proposal:

5.5.1   the Customer shall inform the Supplier in writing of its reasons for its rejection; and

5.5.2   the Supplier shall then revise the Architecture Change Proposal and shall re-submit the Architecture Change Proposal to the Customer for the Customer's approval. The provisions of Paragraph 5.4 and this Paragraph 5.5 shall apply again to any resubmitted Architecture Change Proposal, provided that either Party may refer any disputed matters for resolution by the Dispute Resolution Procedure at any time.

5.6   For the avoidance of doubt, the Supplier shall not implement any Architecture Change not approved by the Customer pursuant to the procedure in the above paragraphs 5.4 and 5.5.

PCSS Call-Off Terms
Schedule 2.3 (Standards)

6. Accessible Digital Standards

The Supplier shall comply with (or with equivalents to):

6.1.1 the World Wide Web Consortium (W3C) Web Accessibility Initiative (WAI) Web Content Accessibility Guidelines (WCAG) 2.0 Conformance Level AA; and

6.1.2 ISO/ IEC 13066-1: 2011 Information Technology - Interoperability with assistive technology (AT) - Part 1: Requirements and recommendations for interoperability.

7. Service Management Software Standards

7.1 Subject to Paragraphs 2 to 4 (inclusive), the Supplier shall reference relevant industry and HM Government standards and best practice guidelines in the management of the Services, including the following and/or their equivalents:

7.1.1 ITIL v3 2011;

7.1.2 ISO/IEC 20000-1 2011 "ITSM Specification for Service Management";

7.1.3 ISO/IEC 20000-2 2012 "ITSM Code of Practice for Service Management";

7.1.4 ISO 10007:2003 "Quality management systems - Guidelines for configuration management"; and

7.1.5 BS25999-1:2006 "Code of Practice for Business Continuity Management" and, ISO/ IEC 27031:2011, ISO 22301:2012 and ISO/ IEC 24762:2008 in the provision of the BCDR Plan.

7.2 For the purposes of management of the Services and delivery performance the Supplier shall make use of Software that complies with Good Industry Practice including availability, change, incident, knowledge, problem, release deployment, request fulfilment, service asset and configuration, service catalogue, service level and service portfolio management. If such Software has been assessed under the ITIL Software Scheme as being compliant to "Bronze Level", then this shall be deemed acceptable.

8. Environmental Standards

8.1 The Supplier warrants that it has obtained ISO 14001:2004 (or equivalent) certification for its environmental management and shall comply with and maintain certification requirements throughout the Term. The Supplier shall follow a sound environmental management policy, ensuring that any goods and the Services are procured, produced, packaged, delivered, and are capable of being used and ultimately disposed of in ways appropriate to such standard.

8.2 The Supplier shall comply with relevant obligations under the Waste Electrical and Electronic Equipment Regulations 2006 in compliance with Directive 2002/96/EC and subsequent replacements (including those in compliance with Directive 2012/19/EU).

8.3   The Supplier shall (when designing, procuring, implementing and delivering the Services) ensure compliance with Article 6 and Annex III of the Energy Efficiency Directive 2012/27/EU and subsequent replacements.

8.4   The Supplier shall comply with the EU Code of Conduct on Data Centres' Energy Efficiency. The Supplier shall ensure that any data centre used in delivering the Services are registered as a Participant under such Code of Conduct.

8.5   The Supplier shall comply with the Customer and HM Government's objectives to reduce waste and meet the aims of the Greening Government: IT strategy contained in the document "Greening Government: ICT Strategy issue (March 2011)" at https://www.gov.uk/government/publications/greening-government-ict-strategy.

9.   Hardware Safety Standards

9.1   The Supplier shall comply with those BS or other standards relevant to the provision of the Services, including the following or their equivalents:

   9.1.1   any new hardware required for the delivery of the Services (including printers), shall conform to BS EN 60950-1:2006+Al2:2011 or subsequent replacements. In considering where to site any such hardware, the Supplier shall consider the future working user environment and shall position the hardware sympathetically, wherever possible;

   9.1.2   any new audio, video and similar electronic apparatus required for the delivery of the Services, shall conform to the following standard: BS EN 60065:2002+Al2:2011 or any subsequent replacements;

   9.1.3   any new laser printers or scanners using lasers, required for the delivery of the Services, shall conform to either of the following safety Standards: BS EN 60825-1:2007 or any subsequent replacements;

   9.1.4   any new apparatus for connection to any telecommunication network, and

   9.1.5   required for the delivery of the Services, shall conform to the following safety Standard: BS EN 41003:2009 or any subsequent replacements.

9.2   Where required to do so as part of the Services, the Supplier shall perform electrical safety checks in relation to all equipment supplied under this Call-Off Agreement in accordance with the relevant health and safety regulations.

10.   Information Governance

10.1   The Supplier shall maintain a minimum of level 2 performance (**"Required Level"**) against all requirements in the IG Toolkit.

10.2   The Supplier shall perform, and publish, an information governance self-assessment exercise

in order to confirm compliance with the IG Toolkit. The Supplier shall subsequently undertake, and publish, a further information governance self-assessment exercise in each Contract Year, with both the initial self-assessment and any further assessment to be submitted within such timescales as required by the IG Toolkit and/or the Information Governance Operational Protocol.

10.3   If, at any time, the Supplier is non-compliant with any part of the IG Toolkit, this shall constitute a Notifiable Default under Clause 41.1 of the Call-Off Terms.

10.4   The Supplier shall, at its own cost, at least once each Contract Year commission an independent audit of the assessment which it performs pursuant to paragraph 10.2. The Supplier shall make the result of this audit available to the Customer, who shall in its absolute discretion have the right to publish this information.

10.5   In the provision of the Services at all times the Supplier will comply with the Cyber Essentials requirements detailed at paragraph 3.4.3.11 of Schedule 2.5 (Security Management) to the Call-Off Terms.

10.6   The Supplier shall nominate an Information Governance Lead, a Senior Information Risk Owner and a Nominated Caldicott Lead, each of whom shall be Key Personnel and a member of the Supplier's board of directors.

10.7   The Supplier shall adopt and implement the recommendations of the Caldicott Information Governance Review and the Government Response to the Caldicott Review in the provision of the Services.

10.8   If there is an Information Security Incident the Supplier shall, in addition to complying with any obligations under paragraph 8 of Schedule 2.5 (Security Management) to the Call-Off Terms, inform the appropriate individuals as identified in the Security Incident Management Procedure, who shall decide, with reference to the Internal Incident Reporting Procedure whether it is to take any further action, including but not limited to, notifying relevant regulatory bodies or publishing such Information Security Incident.

Annex 1

Industry Standards

The following are Industry Standards for the purposes of this Call-Off Agreement:

Open Data Standards Hub
ISO/IEC 26300: 2006/Amd 1: 2012 or equivalent
Technology Architecture Standards
The Open Group Architecture Framework
Accessible Digital Standards
World Wide Web Consortium (W3C) Web Accessibility Initiative (WAI) Web Content Accessibility Guidelines (WCAG) 2.0 Conformance Level AA
ISO/ IEC 13066-1: 2011 Information Technology - Interoperability with assistive technology (AT) - Part 1: Requirements and recommendations for interoperability
Service Management Software Standards
ITIL v3 2011
ISO/IEC 20000-1 2011 "ITSM Specification for Service Management"
ISO/IEC 20000-2 2012 "ITSM Code of Practice for Service Management"
ISO 10007:2003 "Quality management systems - Guidelines for configuration management"
BS25999-1:2006 "Code of Practice for Business Continuity Management"
ISO/ IEC 27031:2011, ISO 22301:2012 and ISO/ IEC 24762:2008 in the provision of the BCDR Plan
Environmental Standards
ISO 14001:2004
EU Code of Conduct on Data Centres' Energy Efficiency
Hardware Safety Standards
BS EN 60950-1:2006+Al2:2011 or any subsequent replacements

PCSS Call-Off Terms
Schedule 2.3 (Standards)

BS EN 60065:2002+Al2:2011 or any subsequent replacements
BS EN 60825-1:2007 or any subsequent replacements
BS EN 41003:2009 or any subsequent replacements
Information Security Standards
ISO/ IEC 27001:2013
ISO/ IEC 27002:2013
Incident Reporting Procedures
Internal Incident Reporting Procedure
External Incident Reporting Procedure
Other Requirements
The 'National Vulnerability Database' as set out by NIST http://nvd.nist.gov/cvss.cfm
Microsoft's 'Security Bulletin Severity Rating System'

Annex 2

Public Sector Standards

The following are Public Sector Standards for the purposes of this Call-Off Agreement:

Technology and Digital Services Practice
HM Government's Technology Code of Practice, as documented at: https://www.gov.uk/service-manual/technology/code-of-practice.html
Open Data Standards Hub
UK Government's Open Standard Principles, as documented at: https://www.gov.uk/government/publications/open-standards-principles
Standards Hub, as documented at: http://standards.data.gov.uk/
Environmental Standards
Greening Government: IT strategy contained in the document "Greening Government: ICT Strategy issue (March 2011)", as documented at: https://www.gov.uk/government/publications/greening-government-ict-strategy
Information Governance
IG Toolkit
Information Governance Operational Protocol
Cyber Security Requirements
Cyber Essentials requirements at: https://www.cyberstreetwise.com/cyberessentials/files/requirements.pdf
the "10 steps to Cyber Security" guidance as documented at: https://www.gov.uk/government/publications/10-steps-to-cyber-security-advice-sheets
Other Requirements

PCSS Call-Off Terms
Schedule 2.3 (Standards)

CESG End User Devices Platform Security Guidance at: (https://www.gov.uk/government/collections/end-user-devices-security-guidance--2).
UK Government Communications Electronics Security Group , including the Commercial Assurance Product Scheme, End User Devices Platform and Certified Professional Certification
UK Government Communications Electronics Security Group
Public Sector Network framework
NHS England policies as set out at: http://www.england.nhs.uk/about/policies/
NHS Employment Check Standards available at http://www.nhsemployers.org/RecruitmentAndRetention/Employment-checks/Employment-Check-Standards/Pages/Employment-Check-Standards.aspx
Data Subject Access Request Procedure