Maidstone and Tunbridge Wells NHS Trust

Ref: FOI/GS/ID 6402

Please reply to:
FOI Administrator
Trust Management
Maidstone Hospital
Hermitage Lane
Maidstone, Kent
ME16 9QQ
Email: mtw-tr.foiadmin@nhs.net

19 November 2020

Freedom of Information Act 2000

I am writing in response to your request for information made under the Freedom of Information Act 2000 in relation to compliance requirements for any potential suppliers of software.

You asked:
What are the pre-requisite compliance requirements for any potential suppliers of software at your NHS Trust? Kindly list the specific requirements for your Trust, which includes but is not limited to the following:

- *Data governance policies that suppliers must prescribe to in order to secure tenders;*
- *Compliance requirements;*
- *ISO standards (i.e. ISO 2701);*
- *Frameworks;*

Any other badges or accreditation required.
For context, this FOI request is in reference to non-clinical software (not a medical device) for senior management that aggregates data around patient flow (i.e. breaches, patient journeys, medical records, and resources consumed) across departments scraped from the ERP and other software.

Trust response:

Please find below a copy of the NHS MODEL AGREEMENT FOR SERVICES SCHEDULES, SCHEDULE 2.3 STANDARDS

MODEL AGREEMENT FOR SERVICES SCHEDULES

SCHEDULE 2.3

STANDARDS

Standards

DEFINITIONS

In this Schedule, the following definitions shall apply:

"NHS Standard Contract"	means the model commissioning contract or contracts published by NHS England (or any successors to the relevant part of its functions) from time to time pursuant to its powers under regulation 17 of the National Health Service Commissioning Board and Clinical Commissioning Groups (Responsibilities and Standing Rules) Regulations 2012. For the purposes of this Contract "NHS Standard Contract" shall also refer to any variants of the NHS Standard Contract produced by NHS England from time to time;
"Standards Hub"	the Government's open and transparent standards adoption process as documented at http://standards.data.gov.uk/; and

GENERAL

The Supplier shall comply with the Standards to the fullest extent applicable.

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

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

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

INTEROPERABILITY STANDARDS

The Supplier shall be required to provide the Services, Deliverables and any Goods in accordance with such interoperability standards as may be published by NHS England from time to time. Standards are anticipated to include, but are not limited to:

(a) information governance and security standards that make clear what data may be shared, for what purpose; and what protections are required to keep that data secure;

(b) clinical standards enabling clinicians to safely exchange data with each other with a common understanding of the meaning of the data;

(c) technical standards that will allow systems to talk reliably and securely with each other using common standards for data and transmission;

(d) use of national services, such as the National Record Locator Service, to enable connection across these Local Care Record Exemplars to enable information to be available at the point of care for an individual as they move across geographical boundaries; and

(e) implementation guidance standards.

The Supplier shall be required to publish the meta-data including data quality rules, processing rules, and data specifications information to support the Standards' development. Until the emergent standard is approved for national use, the Supplier shall be required to map the data according to mapping rules and meta-data information published via the Authority. Where a Standard is to be changed or new or emergent standard is to be developed or introduced by the Authority, NHS England, NHS Digital or any other relevant organisation, the Authority will engage in relation to such change or new or emergent standard through a competent standards framework management organisation with the intention that the Supplier will be able, through such standards framework management organisation (such as INTEROPen (http://www.interopen.org) to comment and engage with the Authority and/or NHS England, NHS Digital or any other relevant organisation (as applicable) on the potential impact on the Supplier's provision, or the Authority's receipt, of the Services, Deliverables and any Goods.

The Supplier shall provide the Services, Deliverables and any Goods in accordance with the interoperability standards set out below:

(a) NHS Number to be available at the point of care;

(b) SNOMED CT implemented across all settings of care;

(c) Dictionary of Medicines and Devices (dm+d) implemented across all venues of care;

(d) utilisation of GS1 standards for barcoding;

(e) utilisation of ICD11 for the classification of diseases;

(f) implementation of FHIR based specifications i.e. CareConnect;

(g) utilisation of Unified Codes for Units of Measure (UCUM) to represent all units of measures in clinical systems and across messaging products;

(h) staff and citizen facing identity services adopt use of FIDO and related public key-based specifications;

(i) staff and patient facing services apps support OpenID Connect for single-sign-on; and

(j) Open APIs for access to clinical services and patient records support OAuth2.

NATIONAL CONTRACT STANDARDS

The Supplier shall be required to provide the Services, Deliverables and any Goods in accordance with any applicable standards set out in the NHS Standard Contract as published by NHS England from time to time including but not limited to any standards on the interoperability of information technology systems, applications, tools, software and/or hardware.

TECHNOLOGY AND DIGITAL SERVICES PRACTICE

The Supplier shall (when designing, implementing and delivering the Services, Deliverables and any Goods) 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.

INFORMATION STANDARDS COMPLIANCE

The Supplier shall at all times comply with the NHS Information Standards to the extent that such standards are relevant to the Services, Deliverables and any Goods delivered by the Supplier to the Authority. The NHS Information Standards are documented online at https://digital.nhs.uk/data-and-information/information-standards as updated from time to time.

Where relevant to the Services, Deliverables and any Goods, the Supplier shall ensure that they comply with the NHS Clinical Information Standards documented online at https://digital.nhs.uk/about-nhs-digital/our-work/nhs-digital-data-and-technology-standards/clinical-information-standards to ensure that information about the health and care of individuals can be securely shared and compared across the health care sector.

DIGITAL, DATA AND TECHNOLOGY STANDARDS

The Supplier shall at all times comply with the NHS Digital, Data and Technology Standards as outlined online at https://digital.nhs.uk/about-nhs-digital/our-work/nhs-digital-data-and-technology-standards.

This obligation shall include the Supplier complying with any current and future versions of the NHS Digital, Data and Technology Framework also documented online at the website listed in Paragraph 7.1 of this Schedule.

CYBER STANDARDS

The Suppliers shall provide the Services, Deliverables and any Goods in accordance with the following standards:

(a) Cyber-Essentials+ across the stack as well as at network level;

(b) The process, people and technology standards from the 10 Data and Cyber Security Standards; and

(c) Design digital services using the NHS Digital service manual (https://beta.nhs.uk/service-manual/).

OPEN DATA STANDARDS & STANDARDS HUB

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/open-standards-principles, as they relate to the specification of standards for software interoperability, data and document formats in the IT Environment.

The Supplier shall ensure that all documentation published on behalf of the Authority pursuant to this Agreement is provided in a non-proprietary format (such as PDF or Open Document Format (ISO 26300 or equivalent)) as well as any native file format documentation in accordance with the obligation under Paragraph 9.1 to comply with the UK Government's Open Standards Principles, unless the Authority otherwise agrees in writing.

The Supplier shall ensure that all documentation describing the data sourced or utilised within the IT Environment, including but not limited to meta-data including data specifications, data quality rules, and processing rules are published and updated regularly to promote bottom-up standards creation process. The Supplier shall also ensure the consistent mapping to national or emergent standards during the standards development phase which will be published on the Standards Hub.

TECHNOLOGY ARCHITECTURE STANDARDS

The Supplier shall produce full and detailed technical architecture documentation for the Supplier Solution in accordance with Good Industry Practice. Documentation produced in compliance with TOGAF 9.2 or its equivalent, shall be deemed to have been produced in accordance with Good Industry Practice.

ACCESSIBLE DIGITAL STANDARDS

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

(a) the World Wide Web Consortium (W3C) Web Accessibility Initiative (WAI) Web Content Accessibility Guidelines (WCAG) 2.1 Conformance Level AA; and

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

SERVICE MANAGEMENT SOFTWARE & STANDARDS

Subject to Paragraphs 2 to 9 (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:

(a) ITIL v4 2019;

(b) ISO/IEC 20000-1 2018 "ITSM Specification for Service Management";

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

(d) ISO 10007 "Quality management systems – Guidelines for configuration management"; and

(e) BS25999-1:2006 "Code of Practice for Business Continuity Management" and, ISO/IEC 27031:2011, ISO 22301 and ISO/IEC 24762:2008 in the provision of "IT Service Continuity Strategy" or "Disaster Recovery" plans.

For the purposes of management of the Services (including development and supply of Deliverables and Goods) 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.

ENVIRONMENTAL STANDARDS

The Supplier warrants that it has obtained ISO 14001 (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 Deliverables, 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.

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).

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

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.

The Supplier shall comply with the Authority 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.

HARDWARE SAFETY STANDARDS

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

(a) any new hardware required for the delivery of the Services, Deliverables and any Goods (including printers), shall conform to BS EN 60950-1:2006+A12:2011 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;

(b) any new audio, video and similar electronic apparatus required for the delivery of the Services Deliverables and any Goods, shall conform to the following standard: BS EN 60065:2002+A12:2011 or any subsequent replacements;

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

(d) any new apparatus for connection to any telecommunication network, and required for the delivery of the Services Deliverables and any Goods, shall conform to the following safety Standard: BS EN 41003:2009 or any subsequent replacements.

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

STANDARDS FOR PROVIDERS OF ONLINE PRIMARY CARE SERVICES

Not Used.

STANDARDS FOR DATA DRIVEN TECHNOLOGY, MACHINE LEARNING & ARTIFICIAL INTELLIGENCE

The Supplier shall, where applicable, comply with the principles of the Department of Health Social Care Code of Conduct for data-driven health and care technology dated February 2019, which may be accessed at https://www.gov.uk/government/publications/code-of-conduct-for-data-driven-health-and-care-technology/initial-code-of-conduct-for-data-driven-health-and-care-technology. The Supplier shall:

(a) understand users, their needs and the context;

(b) define the outcome and how the technology will contribute to it;

(c) use data that is in line with appropriate guidelines for the purpose for which it is being used;

(d) be fair, transparent and accountable about what data is being used;

(e) make use of open standards;

(f) be transparent about the limitations of the data used and algorithms deployed;

(g) show what type of algorithm is being developed or deployed, the ethical examination of how the data is used, how its performance will be validated and how it will be integrated into health and care provision;

(h) generate evidence of effectiveness for the intended use and value for money;

(i) make security integral to the design (keep systems safe by safeguarding data and integrating appropriate levels of security); and

(j) define the commercial strategy (including IP).

STANDARDS SPECIFIED BY THE MHRA

The Supplier shall, where applicable, comply with the standards and guidance set out in the Medicines and Healthcare products Regulatory Agency website which can be accessed at https://www.gov.uk/government/organisations/medicines-and-healthcare-products-regulatory-agency.

CLINICAL RISK MANAGEMENT STANDARDS

The Supplier shall, where applicable, comply with the following standards set out at https://digital.nhs.uk/services/solution-assurance/the-clinical-safety-team/clinical-risk-management-standards:

(a) DCB0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems; and

(b) DCB0160: Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems.

LHCR PROGRAMME TECHNICAL CAPABILITIES

The Supplier Solutions shall, where applicable, adhere to any technical capabilities that enable the following within a LHCR:

(a) Core Interoperability Services – Open APIs;

(b) Core Interoperability Services – Record Location;

(c) Core Interoperability Services – Event Management;

(d) Core Interoperability Services – Longitudinal Care Record;

(e) Core Interoperability Services – Personal Health Records (PHRs);

(f) Reference Services – Metadata Management;

(g) Reference Services – Reference Data Management;

(h) Reference Services – Information Standards;

(i) Reference Services – Master Patient Index;

(j) Data Services – Data Rules Management;

(k) Data Services – Data Discovery Support;

(l) Data Services – Data Transfer and Dissemination;

(m) Data Services – Data Integration;

(n) Data Services – Data Processing;

(o) Data Services - De-identification/Re-identification;

(p) Information Governance and Security – Patient Choices;

(q) Information Governance and Security - Information Governance Implementation;

(r) Information Governance and Security – Authorisation and Authentication;

(s) Information Governance and Security - Care Record Access Audit;

(t) Information Governance and Security – Cyber Security; and

(u) Analytics – Analytics.

The references in Paragraph 19.1 above to 'Core Interoperability Services', 'Reference Services', 'Data Services', 'Information Governance and Security' and 'Analytics' are references to the headings and descriptions outlined in the 'LHCRE Funding Agreement' available upon request from NHS England, via email, at england.phmsupport@nhs.net.

PRSB COMMON CORE INFORMATION STANDARDS

The Supplier shall, within 6 months of its endorsed publication date, comply with all of the standards listed in the Professional Record Standard Body (PRSB) – Core Information Standards to be published online at https://theprsb.org/standards/coreinformationstandard/ or such other address as is communicated to the Suppliers by the Authority from time to time.

Failure to comply with the Standard listed in this Paragraph 20 of this Schedule within the agreed timeframe shall be deemed to constitute a material Default which may result in the Authority terminating this Agreement.

INFORMATION GOVERNANCE FRAMEWORK FOR INTEGRATED HEALTH CARE

The Supplier shall comply with all of the standards listed in the 'Local Health and Care Records – Information Governance Framework for Integrated Health and Care' from time to time, available upon request from NHS England at england.phmsupport@nhs.net.

INFORMATION STANDARDS NOTICES

The Supplier shall at all times, comply with any Information Standards Notices published, from time to time, by the Data Coordination Board online at https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/information-standards-notices.

STANDARDS SPECIFIC TO THIS ACTIVITY

All the provisions of the Authority's policies and rules and as updated from time to time to meet changes in statues or regulations with which the Authority and the Authority Service Recipients will comply.

All standards listed in the Output Based Specification and listed below as updated from time to time.

Medical Devices Directive 93/42/EEC

Medical Devices Regulations 2002 (SI 2002/618)

Confidentiality Code of Practice
https://digital.nhs.uk/binaries/content/assets/legacy/pdf/8/9/copconfidentialinformation.pdf

"Health Service Circular - Data Protection Act 2018 - Protection and Use of Patient Information": https://www.gov.uk/data-protection/the-data-protection-act

Caldicott Guardian's Manual:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/581213/cgmanual.pdf

BS ISO/IEC 27001 and BS ISO/IEC 17799, for Information Systems

BS EN 13485: Medical Devices Quality Management Systems – Requirements for Regulatory Purposes

ISO 9001 Quality management systems

Management and other relevant future standards in the ISO/IEC 27001 series.

The Care Records Guarantee:
http://webarchive.nationalarchives.gov.uk/20130513181011/http://www.nigb.nhs.uk/pubs/nhscrg.pdf

Records Management NHS Code of Practice 2016.
https://digital.nhs.uk/binaries/content/assets/legacy/pdf/n/b/records-management-cop-hsc-2016.pdf

Security Policy No. 4 of HMG Security Policy Framework, December 2009.

Guidelines for the specification, implementation and management of information technology (IT) systems in hospital transfusion laboratories BCSH 2014

All relevant current National and European legislation or official guidelines including, but not limited to: “Better Blood Transfusion”. “The Blood Safety and Quality Regulations 2005”. “The Blood Safety and Quality (Amendment) Regulations 2005”. “Guidelines for compatibility procedures in blood transfusion laboratories” (Transfusion Medicine, 2004, 14, 59-73). “Guidelines for blood bank computing” (Transfusion Medicine 2000; 10, 307-314). “Guidelines on hospital blood bank documentation and procedures” (Clinical and Laboratory Haematology 1998; 10, 265-273). “Directive 2002/98/EC Of The European Parliament And Of The Council of 27 January 2003”. “Directive 2004/33/EC Of The European Parliament And Of The Council of 22 March 2004”. NHS Data Model and Dictionary Service

MHRA – Blood safety and quality regulations

Human Tissues Authority

Royal College Pathology

Medical laboratories — Requirements for quality and competence (ISO 15189)

Operational Productivity Review, Lord Carter, 2016

The Carter Reviews (2006 & 2008)

Pathology Quality Service KPI proposals, RCP, July 2013

Five Year Forward plan, NHS England 2014

NHS Services – open seven days a week: everyday counts

Pathology QA Review 2014, Barnes & Huntley

Pathology Commissioning Toolkit, DoH 2012

Public Health England Standards for Microbiological Investigations

Decommissioning and the disposal of all MS, redundant MS and Hazardous Waste (as defined in the Hazardous Waste Regulations 2005 and/or List of Wastes Regulations (England) (2005) and/or the Waste Electrical and Electronic Equipment Regulations 2006 in accordance with legislation, including Framework Directive 2006/16/EC, of the European Parliament and of the Council of 7th February 2006, and 2008/98/EC, of the European Parliament and of the Council of 19th November 2008, and including the Hazardous Waste Regulations (2005), List of Wastes Regulations (England) 2005, Landfill Regulations (2002), and directive 2002/96/EC of the European Parliament and of the Council of 27 January 2003, and 2003/108/EC, of 8th December 2003 including subsequent amendment directives (2009) on Waste Electrical and Electronic Equipment (WEEE), Good Industry Practice or manufacturers guidelines, plus any subsequent/new laws/regulations/standards

National Institute for Health and Care Excellence

United Kingdom Accreditation Service

NHS England and NHS Improvement Pathology Quality Assurance Dashboard

National Data Guardian 10 Data Security and Protection Standards – evidenced by annual completion of the Data Security and Protection Toolkit. https://www.dsptoolkit.nhs.uk/