NHS England

GP IT Specification Commissioning Support Pack

This document forms Appendix E of the Securing Excellence in Primary Care (GP) Digital Services -The Primary Care (GP) Digital Services Operating Model v 5

GP IT Specification Commissioning Support Pack

Published as an annex (Appendix E) to the Securing Excellence in Primary Care (GP) Digital Services: 2021 – 2023 Operating Model: 5th Edition

Version number: 4.0

First published: 2016

Updated: April 2021

Prepared by: Primary Care Digital Transformation, Operations and Information, NHS England

Classification: OFFICIAL

This information can be made available in alternative formats, such as easy read or large print, and may be available in alternative languages, upon request. Please contact england.digitalprimarycareengland@nhs.net

Contents

1. Introduction and Purpose

1.1 Clinical Commissioning Groups (CCGs), or any successor organisations, have delegated responsibility from NHS England to provide GP IT Services in accordance with the NHS obligations in the GP contract and CCG-Practice Agreement. CCGs should seek to secure quality services at value for money eg through using applicable framework contracts and to minimise the risk of fragmentation by considering at scale procurements in collaboration with other CCGs.

1.2 Where a contract for GP IT services is already in place and re-procurement is not scheduled in the near future this support pack will be of assistance to CCGs and their GP IT suppliers to:

- review current services and agree any changes needed
- ensure data needed by both parties is available to deliver high quality efficient services to general practices.

1.3 The Operating Model - Securing Excellence in Primary Care (GP) Digital Services, 2021-23, 5th Edition sets out how NHS England will achieve world class digital primary care systems that support flexible, responsive and integrated services for patients, giving them greater control over their health and care.

1.4 The CCG Practice Agreement should be signed by all general practices and CCGs to ensure the practices can receive NHS Funded GP Digital Services and that the responsibilities of both parties are clear.

1.5 This pack includes an updated template specification aligning with and supporting the requirements schedule in Appendix A of the Operating Model.

1.6 This pack sets out some of the key considerations when re-procuring GP IT services and a recommended process to support CCGs to tailor local GP IT specifications. It will be refreshed and updated as further good practice emerges and as the Operating Model is periodically updated. However, it should not be taken as an exhaustive or prescriptive guide.

1.7 This pack includes a template which when populated by CCGs, as part of a discovery process, will give an overview of the GP IT estate, local considerations and those services to be included in the specification.

1.8 The specification described in Table 1.1 and Table 1.2 may be used once the contract is awarded as the basis of Appendix 1 (Summary of Services Table) in the CCG Practice Agreement.

1.9 Tables 4.1, 4.2, 4.3, 4.4 and 4.5 may be used once the contract is awarded as the basis of Appendix 2 (Support & Maintenance Service Levels) in the CCG-Practice Agreement.

1.10 In procuring GP IT services CCGs should ensure where possible the services reduce likelihood of unlawful discrimination and promote Equality of Opportunity by supporting NHS compliance with the nine characteristics in its public sector equality duty as defined by the Equality Act 2010. Particular areas with patient facing aspects include access to records, online digital, telephone and video consultation and triage, electronic messaging for direct patient communication (e.g. Short Message Service (SMS)), public/patient WiFi, and data security.

2. The CCG Practice Agreement

2.1 CCGs should have a CCG Practice Agreement signed with each Practices in scope of this contract. These outline the terms governing the provision and receipt of GP IT Digital services. These terms should be reflected in the specifications, particularly highlighting any local requirements that have been added to the national template agreement, and shared with potential bidders to provide detail on the services that the new supplier would be supporting. The CCG Practice agreement requires CCGs to enter into data processing agreements for locally commissioned digital services on behalf of the practices. The Operating Model provides detail on the services to be provided under the terms of this agreement.

3. Scope of Service Recipients (Practices)

3.1 All general practices who have a signed CCG Practice Agreement should be included as a Service Recipient. Where there is no signed CCG Practice Agreement the practice should be considered outside the scope of this procurement

3.2 Primary Care Network services provided within a GP contract as a Directed Enhanced Service (DES) from April 2019 are within the scope of the service recipient (providing the host practice has signed the CCG Practice Agreement)

3.3 CCGs may wish to extend the procurement to include IT support for other organisations and services not operating under a GP contract e.g. a community provider. This is a local CCG decision at the discretion of the CCG. The CCG must ensure additional funding, other than the CCG allocated GP IT funds, are made available to support this

4. The Operating Model

4.1.1 The Operating Model is a commissioning framework which describes the financial operating arrangements, assurance arrangements and leadership required to support the effective delivery of GP IT services. The Operating Model also addresses the responsibilities of the NHS nationally, regionally and locally (through CCGs or any successor organisation) and of the general practice contractors. It defines a set of requirements which the CCG must

provide as Core and Mandated GP IT Requirements and those which can be locally prioritised as Enhanced GP IT Requirements to meet needs for local service improvement, change and transformation. The Schedule of Requirements provided in the Operating Model (Appendix A) can form the basis of a local specification but needs adaption to articulate the requirement which supports the CCGs delivery responsibilities and local needs.

4.1.2 This procurement support pack and specification template is an important supporting component of the Operating Model assisting CCGs to meet their responsibilities whilst also addressing local community requirements. Appendix A of the Operating Model includes a schedule of enabling requirements for GP IT, this can be used as a basis for the development of local GP IT specifications and is used as the basis for the template specification provided in this document. Although the CCG is required to meet all the defined Core and Mandated GP IT Requirements not all the requirements listed will be appropriate to include in every local specification. CCGs should be familiar with the requirements outlined within the Operating Model when they review their local GP IT specifications.

4.1.3 The Operating Model recognises the fundamental role that effective GP IT services will play in delivering the ambitions outlined within the NHS Long Term Plan and the General Practice Forward View (GPFV). It is essential that the procurement of GP IT support considers the wider strategic context of the service and tests how prospective bidders will provide not only the support required to deliver the business as usual GP IT requirements, but will also deliver efficiency savings, which will enable CCGs to reinvest in enhanced service developments that support and enable new models of care and local service integration.

4.1.4 The Operating Model v5 recognises the development of general practice provider organisations which hold multiple contracts in CCGs geographically dispersed in which case the CCG(s) may wish to consider the following dual approach:

- collaborating with the other CCGs to commission, through a lead CCG, a GP IT service operating across a wider geographical boundary

and:

- commissioning a local GP IT service, if appropriate in collaboration with other CCGs in the geographic locality, for those practices based in the CCG locality.

4.1.5 The Operating Model is regularly updated to reflect changing service needs, organisational developments, GP contract changes and the impact and lessons learned from major incidents such as Wannacry Cyber Attack (2018) and Covid-19 Pandemic Response (2020-21). Contracts for GP IT services need sufficient flexibility to adapt to such demands.

4.1.6 The Operating Model (v5) is effective from April 2021 to March 2023 and may be subject to addendum during that period. This pack is published as an appendix to the Operating Model and has been aligned with the content of the

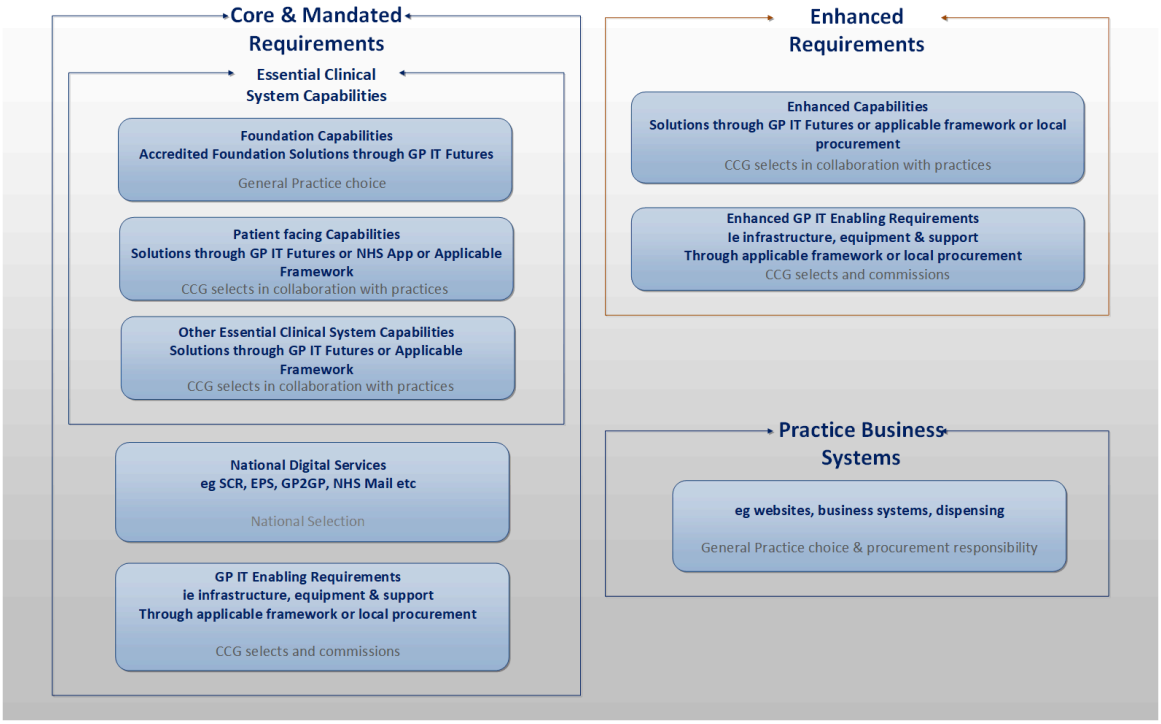
Operating Model. Potential bidders need to be able to respond to published revisions of the Operating Model over the term of the contract.

4.2 Core and Mandated GP IT Requirements

4.2.1 Core and Mandated GP IT Requirements are defined within the Operating Model as technologies and services required for the delivery of essential services under the GP contract or as otherwise nationally required are Core and Mandated GP IT Requirements. Through the CCG-Practice Agreement these are funded by NHS England for GP contractors.

Note: These are the core services to be commissioned by CCGs for general practices, to enable the effective delivery of primary care services and compliance with the GP Contract (including General Medical Services (GMS), Personal Medical Services (PMS) and Alternative Provider Medical Services (APMS) contracts).

Primary Care (GP) Digital Services Operating Model Requirements



4.2.2 As a minimum, the GP IT specification should include all 'Core and Mandated' requirements outlined within the Operating Model, where these are not delivered through alternative mechanisms for example, provisioned directly by the CCG, a shared service arrangement or procured from another provider. A key principle is to build on the best of existing service provision arrangements, addressing any shortcomings and ensuring any subsequent transfer of

services is effectively managed to avoid de-stabilising existing service provision.

4.2.3 CCGs should be clear within GP IT specifications about the kind of services that are required. For areas where the service is mature and stable, continuation of existing service provision may be a key requirement, together with expectations around service improvement. Where there are known challenges to current GP IT service arrangements, these should be clearly articulated within the tender documentation, with an outline of future service expectations to address these challenges. CCGs may wish to advise potential bidders to propose innovative and cost effective strategies to address current challenges. If there are any specific local requirements considered to be essential to maintaining service delivery locally, such as online technical support and first-line response to reduce the demand for onsite support, particularly in rural areas, these should be included within the specification. CCGs should however, be cautious about setting too many specific requirements of this type as bidders should be given flexibility to design and offer best value solutions.

4.3 Enhanced GP IT Requirements

4.3.1 Productive capabilities are met by the technologies, systems and support services which enable and improve efficiency and effectiveness of general practice including primary care at scale to support the delivery of the GP Forward View (GPFV). These

4.3.2 Transformational capabilities are met by the technologies, systems and support services which will enable new models of care and service integration. These services may be provided to facilitate broader service integration and inter-organisational sustainability and transformation initiatives.

4.3.3 Enhanced GP IT Requirements should be developed and agreed with practices locally to support local strategic initiatives and to improve service delivery. They will require local specification in line with local priorities and plans that should be included within tender requirements.

4.3.4 CCGs should outline local service transformation plans within GP IT specifications, particularly in relation to primary care, but also in relation to local Integrated Care Systems, to enable prospective bidders to best respond to local requirements within tender submissions. Bidders should be able to offer innovative service delivery arrangements and solutions, to support CCGs and general practice in delivering against the improvement and transformation of general practice services, as outlined in the GP Forward View and NHS Long Term Plan.

4.4 Standards

4.4.1 Within the Operating Model where applicable standards are attributed to individual requirements. These should be reflected in the service specification and bidders in their responses are expected to demonstrate how these standards will be met. Nationally recognised and published guidance is also shown attributed to individual requirements where appropriate. Where not mandatory as standards bidders are still expected to follow any such guidance shown.

4.4.2 There are a number of standards applicable to the Supplier at organisational level. (See Appendix 1 – Organisation Standards). Assurances should be sought from bidders that any accreditation or certification relevant to these standards fully applies to the scope of the services being procured. Use of an applicable framework such as HSSF will provide assurance on compliance with appropriate standards.

4.5 Cyber & Data Security

4.5.1 All parties ie CCGs, General Practices and potential bidders must understand and consider the impacts of:

- the threat to general practice business continuity and patient safety from potential cyber attacks
- compliance with the National Data Guardian's ten standards
- legal compliance by all parties with General Data Protection Regulation (GDPR) and the Data Protection Act (2018).

4.5.2 Detailed requirements on cyber and data security are incorporated into the Operating Model and the template specification provided in this document. CCGs as commissioners and general practices as data controllers must jointly ensure all parties fully meet these requirements through the procurement.

4.6 National Digital Services

4.6.1 These are digital services commissioned centrally by NHS and provided to, and used by, all NHS commissioned providers where applicable including general practices. There is no local choice in these solutions. Locally commissioned alternatives should not be commissioned or used. The provision of these services is therefore outside the scope of the GP IT Specification although local support necessary for practices to use these services is in scope.

4.7 Funding

4.7.1 Funding arrangements are outlined within the Operating Model. These aim to ensure that CCGs can provide the core & mandated requirements whilst also

having sufficient local flexibility to commission effective and responsive GP IT services that meet local need and support the development of new models of care whilst also ensuring:

- standardised high quality GP IT services
- alignment of GP IT operating arrangements with local strategies for general practice
- a foundation to underpin GP IT provision to enable service transformation

4.7.2 The first call on GP IT revenue funding locally is the provision of Core and Mandated Requirements for GP IT and PCN IT. Refer to the current Operating Model for details on funding sources and their application.

4.7.3 Financial envelopes should reflect the increased funding available to deliver the additional services in the Core and Mandated Requirements of GP & PCN IT as well as any additional funding required to deliver enhanced services.

5. Discovery Process

5.1 Local GP IT services can be detailed, complex and wide ranging for a number of reasons, for example legacy arrangements, community wide initiatives, individual practice requirements and variations in operational practice forms eg small local practice to a super pan-geographical or city wide practice. It is essential that the CCG embarks on this procurement with clarity on the services, assets, and liabilities in the local environment. Leaving the discovery process to take place as part of or alongside the service mobilisation process once the contract is awarded can lead to significant financial and service continuity risks for the CCGs and their GPs.

5.2 Assets which include IT hardware, software licences, staff access accounts and physical estate will attract support, maintenance and replacement costs. Potential bidders may use these asset profiles to calculate baseline service costs. Without this baseline information, planning and engaging constructively with the potential bidder on primary care service improvement and digitally enabled transformation will be compromised.

5.3 There may still be significant revenue costs associated with legacy and residual IT service contracts, for example software applications, Community of Interest Networks (COINS), remote access tokens, telephony etc. Both the CCG and the potential bidder need to have visibility of these and clarity on how they are to be managed and funded in the future. The distinctions given in the Operating Model for Core and Mandated GP IT Requirements, Enhanced GP IT Requirements and practice business requirements may be helpful in planning the future management of any legacy arrangements. Some legacy services may support healthcare providers other than practices, for example in shared primary care sites and shared infrastructure in which case the CCG (as commissioner) should consider how it wishes to support the provision of these in the future. CCGs should ensure that it does not duplicate the funding or resourcing of such services for practices and other providers. Exit strategies should be considered for legacy contracts where these have not been managed out of service at the time of publication of the Operating Model v5.

5.4 Given the importance of the above the commitment to ongoing collation and management of this information once the contract is awarded and service is mobilised should be seen as a critical delivery success factor of any Potential bidder.

6. The Primary Care Digital Maturity Assurance Tool

6.1 undertaking a re-procurement of GP IT services, CCGs should review the data available within Primary Care Digital Maturity Assurance Tool (PC DMAT), to assist their understanding of local levels of digital maturity across their primary care estate.

6.2 The PC DMAT is aligned to the Operating Model and outlines progress against 'Core and Mandated' GP Digital requirements and gives insight into progress against some elements of 'productive' and 'transformational' service delivery. This will help CCGs to identify gaps in current service provision and areas for future investment, together with supporting CCGs in considering the following questions:

Is there assurance that the commissioned GP IT services are secure, compliant and resilient and are of the required quality (i.e. fit for use and responsive) and supports the NHS meet its obligations in the GP Contract requirements and the CCG-Practice Agreement ?

Action: Review the Core and Mandated GP IT Requirements indicators

Where is investment needed to invest in the future to meet the ambitions of the General Practice Forward View (GPFV) ?

Action: Review the Productive GP IT indicators

Are areas for development and investment identified to support the development of Integrated Care Systems (ICS) and Sustainability and Transformational Plans (STPs) across the local community, learning from general practice innovation ?

Action: Review the Transformational GP IT indicators

The information available within the PC DMAT will provide important insight into existing and future GP IT service provision and should be shared with bidders as part of the procurement process to ensure that supplier responses are fit for purpose.

7. More General Questions

Evidence should also be sought to support more general questions:

- can value for money be demonstrated ?
- are commissioned services meeting the expectations and required standards including those related to cyber and patient safety ?
- are there opportunities for the CCG to share learning from general practice across the wider health and care system to meet the ambitions of the NHS Long Term Plan and the local ICS strategy?

8. Procurement Approach

CCGs are recommended to consider using an applicable Purchasing Framework underpinned by standards such as HSSF in procuring GP IT enabling services. Where a framework is not appropriate or cannot be used CCGs must be assured that they meet all necessary procurement, financial, organisation and requirement standards – see GP IT Operating Model.

8.1 Local Engagement

Where possible practices should be able to contribute to this specification through existing forums, GP IT representatives, practice manager groups etc. The cooperation of general practices is essential in this process as they are the primary service recipients. The CCG should ensure good communication routes are maintained with the general practices throughout the processes of discovery, service specification development, and procurement and service mobilisation.

.

8.2 Contract Length

The length of the contract awarded to a supplier is likely to affect the value for money the CCG can achieve. Longer contracts should drive greater investment in service transformation as suppliers seek to drive efficiencies and quality improvement. Although there may be uncertainties for CCGs on the future state CCGs should seek flexibility in the contract to enable the CCG and supplier to co-design the solution that best meets the CCG's needs. By taking this approach, and bringing in the suppliers at the start of a redesign process, suppliers will be able to spread the cost of transformation over multiple years and identify where efficiencies can be made that can (and should) be reinvested in further transformation and service improvement.

8.3 Developing a local specification

8.3.1 A specification template based on the current Operating Model is provided in Appendix 1. The ITT development process (Appendix 7) will assist CCGs further develop a locally appropriate specification.

8.3.2 Whilst not precluding bidders from offering innovative approaches CCGs should give consideration on how the following will be managed:

- services where demand is likely to link to volumes (eg of devices, users etc) and how incremental/organic growth can be accommodated (possibly using a tolerance level)
- specialist (expert) services (eg training, data quality, project management information governance etc) what will the available capacity be and how will it be managed.

8.3.3 Some requirements may be met by specialist providers eg HSCN, WiFi in which case these should be excluded from the specification although support for use of these services may still be needed eg through service desk, cyber security, and infrastructure.

8.3.4 CCGs are able to determine how they commission their GP IT services eg in collaboration with other CCGs, specific requirements commissioned separately. CCGs should refer to the Operating Model for further guidance on commissioning GP IT Services.

8.3.5 The template specification includes, as appropriate for each requirement, supporting notes on:

- *practice responsibilities* – this is for information only and should not form part of the service agreement as the practice is not a party to the contract. It should be removed.
- *CCG note* – this is for information for the commissioner and should be removed from the final document

9 Checklist of Key Questions for CCGs

Before publishing the ITT the CCG should have considered, as a minimum, the following questions:

9.1 Has the CCG reviewed the current GP IT service delivery arrangements with key stakeholders including primary care service users, to ensure their views are adequately reflected?

9.2 Are Cyber & Data Security understood locally and adequately reflected in the specification documentation, including mandatory responsibilities for all parties (refer to current versions of the Operating Model and NHS Digital).

9.3 Has the CCG reviewed the information available within the Digital Primary Care Maturity Assurance Tool to support the developing service specification? Is this information clearly articulated, including highlighting utilisation of this tool to potential bidders, as a means of identifying current progress towards digital maturity within primary care?

9.4 Has the CCG used the information available above to identify those existing service areas which need strengthening? Is this clearly articulated in the GP IT specification?

9.5 Does the financial envelope reflect the increase in Core and Mandated service delivery requirements, supported by the GP IT funding provision for 2021-23?

9.6 Has the CCG included sufficient information on the supported IT estate/primary care estate, local CCG Practice Agreements, in-flight projects and current service provision?

9.7 Has the CCG articulated general practice service improvement trends including new contracts, Primary Care Networks (PCN) & Integrated Care Systems (ICS)? What are the GP IT service requirements that will be needed to enable these? Is information provided in sufficient detail to allow the contract to be flexible to meet developing needs?

9.8 Has the CCG reviewed local strategic plans, including as a minimum insight into Local Digital Roadmap (LDR) digital strategy and Integrated Care Systems (ICS) digital strategy, to ensure procurement of GP IT services that will support changing demands on primary care, particularly in relation to enhanced service requirements?

9.9 Where there is an expectation that the successful bidder will develop innovative service offerings and provide service options, is this clearly articulated within the tender documentation?

9.10 How long does the CCG intend to award the contract for? Has the CCG considered the benefits of enabling a supplier to spread the cost of transformation over a longer period?

9.11 Has consideration been given to funding arrangements for enhanced service requirements? Where there is a need to access innovation funds i.e. Estates and Technology Transformation Fund (ETTF), is there an expectation on successful bidders to support such access arrangements and, if so, is this clearly articulated within the specification?

10 Support Tools Available

A data collation template is provided as part of this pack. This is an Excel file which can be downloaded and used locally. Note: it is a macro enabled Excel file so macros need to be enabled within Excel for this file only.

The spreadsheet has colour coded tabs to guide the user:

- green TABS show the sheet is available for data entry
- amber TABS indicate the cells in the sheet are part completed (fixed text or automatically populated) and part available for local data entry OR are provided as a draft template for local amendment if appropriate
- red TABS show the sheet is auto-populated or fixed text and local data cannot be entered into the sheet.

Cells are also colour coded:

- cells in Blue text have pre-set content or are automatically populated - do not attempt to amend these.
- cells in black text can be manually completed - in some cases there is a validation constraint or drop down lists to support data quality and consistency

Detailed instructions are given within the tool but the principle functions are:

- set the scope by selecting one or more CCGs (by either name or CCG code from a drop down list) which make up the procuring authority.

- optional - Choose up to three categories for this procurement (you may only need one)

- optional – amend the drop down lists in the Customised Reference tab.

- all eligible general practice contractors are pre-selected from the CCGs included. Identify the asset count, systems and services associated the practice (contractor) estate. Additional APMS or provider contractors can be added.

- identify the physical estate (locations) where the services are required – and the asset count associated with that estate.

- progress checklists and suggested external documents to include are provided.

- identify other assets and volumetric including hosted applications, standard (universal) desktop software, contracts, projects in flight or committed, key meetings requiring IT attendance.

- use the service specification template based on the Operating Model Schedule of Digital Requirements to identify if and how each of these requirements is in scope for each CCG. This template can be used for local review and approval and then with and the attached tables as part of the ITT Pack for issue to prospective bidders.

- automatically generate a clean set of unlinked tables (Excel file format) from the data entered. This should be provided as an attachment to the Word document (Appendix 1 Template) which references each table as appropriate. Using the template in Appendix 1 (GP IT Specification Template) review and amend as required the Detailed Service Specification.

- ensure these match the services that the CCG wishes to include in this procurement as selected in the Service Specification tab in the data collection template.

- template Questions – for inclusion in the GP IT Supplier Information Pack

- suggested exploratory topics for bidder presentations

- suggested Points of Consideration in Bidder Interviews

Appendix 1: GP IT Specification Pack Template

Summary

This Service Specification is aligned with the Operating Model: Securing Excellence in Primary Care (GP) Digital Services, 2021-23, 5th Edition. The CCGs detailed in Table 1.1 (attached) are accountable and responsible for the provision of GP IT Enabling IT services to support requirements set out in the Operating Model.

The GP IT Delivery Partner ("*the supplier*") must adhere to the service standards defined in the Operating Model. For the avoidance of doubt where a successor or addendum to the Operating Model is published during the course of this contract the supplier must meet the minimum requirements defined in said successor or addendum.

CCG Practice Agreements are in place between each CCG and their practices that outline the terms governing the provision and receipt of GP Digital services. Suppliers are required to deliver services in line with these agreements, or their successors. A copy of the locally agreed CCG Practice Agreement(s) is attached.

Organisation Standards

Suppliers must meet the minimum standards defined within the Operating Model including but not limited to:

- demonstrate compliance with all mandatory assertions in the NHS Data Security and Protection Toolkit (DSPT) for the relevant organisation type.*
- the organisation is accredited to Cyber Essentials Plus (CE+).*
- compliance as data processor with General Data Protection Regulation (GDPR) and the Data Protection Act (2018). This will include the provision of a compliant data Processing Agreement or equivalent to provide assurance, that the provider organisation is able to meet it's obligations as data processor required under the General Data Protection Regulation (GDPR) Compliance Guidelines.
- a commitment to adhere to and support implementation of the National Data Guardian ten standards on data security.
- the organisation will be accredited to ISO 22301 for Business Continuity Management OR will be compliant with the NHS England Business Continuity Management Framework. *
- well-developed disaster recovery and business continuity plans, reviewed, tested and validated annually for services critical to GP service continuity. These plans should include a response to threats to data security, including

significant breaches or near misses. These plans should be based on a Recovery Time Objective (RTO) of not more than 48 (actual) hours to enable the practice to deliver Essential Services.

- provision of service desk functions aligned with ITIL Version 4 (or equivalent) and operating to standards ISO 20000.

- applicable minimum standards are identified in Table 3.2 Secondary K.P.I.s (Quality Indicators).

- ensuring any sub-contracted supplier complies with the above standards as if such sub-contractor were the supplier.

*Note: Organisational standards may apply to whole organisation and all services it provides internally and externally or may be defined in more detail e.g. within the Information Security Management System (ISMS) scope or Business Continuity Management System (BCMS) scope. Bidder must provide assurance that any standards compliance or certification declared fully applies to the scope of the services being commissioned and to all other providers commissioned by the bidder to deliver the services.

Definitions

Term	Definition
Bidder	A prospective supplier for the services
Core and Mandated GP IT Requirements	The requirements for digital systems, technologies and services necessary to deliver Essential Services under the GP contract or as otherwise nationally mandated. Under the CCG-Practice Agreement these are funded by NHS for GP contractors.
Enhanced GP IT Requirements	Requirements for digital systems, technologies and services which may enable service improvement or transformation.
Essential Clinical System Capabilities	The patient management and clinical capabilities which are Core and Mandated GP IT Requirements enabled through accredited software applications and data solutions available through the GP IT Futures Framework.
Essential Services	Essential (patient care) services as defined in the GP Contract & Regulations
Extended Operational Support Hours	Operational Support Hours extended to

	support local GP contracts which provide GP and PCN services outside the core GP contract hours
GP Contract	The contract to supply primary medical services. This includes General Medical Services (GMS) contract, Personal Medical Services (PMS) agreement and Alternative Provider Medical Services (APMS) contract.
GP IT Enabling Requirements	Requirements for services e.g. infrastructure, equipment and support as necessary for practices to operate the solutions provided to meet Core & Mandated and Enhanced Capabilities provided and the National Digital Services
GP IT Operating Model	This document titled "*Securing Excellence in Primary Care (GP) Digital Services"* and preceding versions titled "*Securing Excellence in GP IT Services"*
High Severity Incident	An incident defined or classified as severity level 1 or 2 in NHS Digital Severity Level Guidelines
High Severity Incident Support Hours	24 hours / day, 7 days a week access for high severity incident management & business continuity
Managed GP IT Device	Any individual IT device which is part of the Managed GP IT Infrastructure
Managed GP IT Infrastructure	Any GP IT equipment, including desktops and mobile equipment, devices, applications or systems regardless of ownership, which is connected to or part of the GP IT infrastructure which the supplier supports and the security of which it controls.
National Digital Services	NHS centrally commissioned digital services provided to, and used as applicable by all NHS commissioned providers
NHS Owned IT Equipment	IT equipment purchased by the NHS using NHS funds (capital or revenue).
NHS Smartcard	Smartcards issued by an approved NHS Registration Authority to provide secure access controls to clinical and personal information by only those that have a valid reason to do so. This definition will apply to NHS approved alternatives or replacements to NHS smartcards.

	Note other smartcards, not NHS smartcards, may be used for other access control purposes.
Operating Model	The Primary Care (GP) Digital Services Operating Model as described in the document entitled Securing Excellence in Primary Care (GP) Digital Services: Version 5: 2021-23 published by NHS England, and in the publication of subsequent amendments and revisions
Operational Support Hours	Services to be provided for core GP contract hours, as detailed in the GP contract (between 08:00 - 18:30, Monday to Friday, excluding Public Holidays).
Practice	Any GP contract holder eligible to receive GP IT services with a signed CCG-Practice Agreement
Practice Business Requirements	The requirements for digital systems, infrastructure and organisation activities necessary to run the internal practice business and organisational governance which are the responsibility of the practice to provide.
Practice Business Support Systems	Systems and services which a practice may utilise for business purposes enabling the non-clinical business functions to operate and support the practice as a business organisation. Not directly related to patient care.
Practice Managed GP IT Equipment	Any IT equipment, including desktops, mobile equipment, multi- function copiers etc, regardless of ownership, which is managed by the practice or a contractor appointed by the practice and is not directly connected to the Managed GP IT Infrastructure
Practice Owned GP IT Equipment	IT equipment purchased by the practice or individual practice staff members
Practice Premises	An address specified in the GP Contract as one at which services are to be provided under the Contract. These locations will be registered with the Organisations Data Service (ODS).
Practice Staff	General Practitioners, practice employees and PCN staff as well as health & social care professionals individually commissioned directly by the practice.
Productive digital capabilities	Patient management and clinical capabilities which improve the efficiency

	& effectiveness of the contracted service and can be enabled through software application and data solutions. These are Enhanced GP IT Requirements
Shared Managed IT Infrastructure	Those components of the Managed GP IT Infrastructure which are shared by other organisations who are not recipients of this service.
Standard Service Hours	Services to be provided between 09:00 - 17:00, Monday to Friday, excluding Public Holidays.
Supplier	The successful bidder awarded contract to supply GP IT services as defined in this specification
Transformational digital capabilities	Patient management and clinical capabilities which enable transformed care, often extending beyond the practice and core GP Essential Services and can be enabled through software application and data solutions. These are Enhanced GP IT Requirements

Services must be available as a minimum for the Service Availability requirement stated for each requirement

Service Categories

The CCG is required to provide the following categories of service to practices

Category 1: Core & Mandated Requirements: Essential Clinical System Capabilities

Requirements, described as capabilities are met through accredited services procured from appropriate Frameworks such as the GP IT Futures Framework. The provision of services to meet these capabilities is therefore outside the scope of this service specification. However as they are required to be supported the services procured here will impact on the GP IT Enabling services required.

Category 2: Core & Mandated Requirements: National Digital Services

A number of digital services and systems are commissioned and provided nationally and are available at no local cost to all NHS commissioned providers including practices (where functionally appropriate). These are standard solutions with no element of local choice. Local alternatives should not be provided or used. The provision of these services is therefore outside the scope of this service specification. However as they are required to be supported these services will impact on the GP IT Enabling services required.

Category 3: Core & Mandated Requirements: GP IT Enabling Requirements

Infrastructure, services and support as required by the solutions selected to meet the essential clinical system capabilities and the national digital services. Where the solution is not provided through another route these will be within scope for this specification.

CCG Note	*CCGs should review the following requirements ensuring they are applicable to their local needs whilst meeting the requirements described in the Operating Model. CCGs should remove any requirement where it is sourced through another procurement route*

Category 4: Enhanced GP IT Requirements: Productive and Transformational Capabilities

These requirements, described as capabilities are met through assured services procured from an applicable Framework such as the GP IT Futures Framework, OCVC Framework, HSSF. The provision of services to meet these capabilities is therefore outside the scope of this service specification. However as they are required to be supported the services procured for practices here will impact on the GP IT Enabling services.

CCG Note	*These are subject to local prioritisation and the CCG should determine in collaboration with their practices which capabilities are needed locally and can be funded. If the capability is to be sourced through this procurement the CCG should develop a specification using the current Operating Model for guidance and standards.* *CCGs should be aware that any enhanced clinical or business capability chosen to be provided locally must also be supported with the GP IT Enabling requirements necessary – that may require an amendment to the previous specifications, an update to Table 5.4 or an additional specification here (category 6).* *The Enhanced GP IT Requirements listed in the Operating Model will provide some areas for the CCG and its practices to consider.*

Category 5: Enhanced GP IT Requirements: GP IT Enabling Requirements

Infrastructure, services and support as required by the solutions selected to meet the enhanced capabilities (Category 4) where these are not already provided under Category 3 requirements. Where the solution is not provided through another route these will be within scope for this specification.

CCG Note	*These are subject to local prioritisation and the CCG should determine in collaboration with their practices which capabilities are needed locally and can be funded. If the capability is to be sourced through this procurement the CCG should develop a specification using the current Operating Model for guidance and standards*

	The Enhanced GP IT Requirements listed in the Operating Model will provide some areas for the CCG to consider. Examples include • *CQRS Support* • *GP Data Quality Accreditation Service* • *Enhanced Infrastructure*

The Authority

The CCGs which constitute the Authority are seeking the following GP IT services:

Table 1.1 Services by CCG

Further summary details by heading is provided in

Table 1.2 Service Specification Summary

Detailed Service Specification

Category 3 Service Specification requirements:

GP IT Support Service Desk

Requirement	GP IT support service desk for all users which provides: • triage • incident management • problem management • request management • SLA reporting • access to notify and escalate high severity cyber or data security incidents
Transactional Services	Service Availability: Operational Support Hours An ITIL aligned or equivalent, management process for: • incidents, • problems, • requests, • change control. Access channels - there must be at least TWO of the following access routes available: • a single telephone number for logging calls, • a single email address for logging calls, • a web portal for logging and managing calls, • an app for logging and managing calls. It must be possible to log a call using at least one of these methods 24 hours a day, 7 days a week. Practices must be able to track the progress of logged calls/requests/incidents through any of these routes. To improve efficiency and responsiveness the service should include remote access in a secure manner subject to end user consent to desktop PCs for diagnostic and resolution purposes, including the management of remote working solutions. The service has clear and agreed priority incident categories, with minimum response and target fix times to ensure the safe and effective operation of GP digital services (see Table 4.4 Priority Assessment Matrix): • all calls are prioritised to the agreed standard see Table 4.4 Priority Assessment Matrix, in conjunction with the person reporting the incident. • a minimum standard should be agreed for the percentage of incidents resolved on first contact or within an agreed timeframe from call logging. (See Table 4.1 Primary K.P.I.s) • where 3rd party support is required for incident or problem management, there is a robust and effective resolution plan in place with agreed responsibilities and led by the GP IT service desk provider. This will include NHS 111-GP Connect issues reported to the service desk. Supported

	software and hardware will be scoped within the Summary Of Services (Appendix 1) in the CCG-Practice Agreement. • where 3rd party support is not available for required incident or problem management e.g. when outside 3rd party support hours the end user (practice) will be advised on timescales and any practical workarounds. The GP IT Service desk provider remains responsible for the incident until the 3rd party can take action to resolve. Availability: High Severity Incident Support Access must be available for out of hours high severity service incident alerting, logging and escalation in accordance with the approved business continuity and disaster recovery plans. This may not operate in the same way as support during operational service hours and response will be appropriate to the impact of the incident and *The Supplier's* Business Continuity and Disaster Recovery Plans.
Specialist Support Services	Service Availability: Standard Service Hours • SLA reporting
Applicable Standards	• ISO 20000 – IT Service Management Standard An ITIL aligned or equivalent, management process for: Incidents, Problems, Requests.
CCG Note	*Recommendation: The local SLA is based upon an agreed Managed GP IT Device OR user volume.*

Extended Operational Support

Requirement	An extension of services required over Operational Support Hours to meet the requirements of PCNs contracted to operate outside the core GP contract hours.
Transactional Services	Service Availability: Extended Operational Support Hours • GP IT Support Desk • registration authority • Essential Infrastructure • desktop infrastructure • remote access to clinical System • controlled digital environment • cyber security
Service Availability	Hours: {} Days of week: {} Exclusions: {}
Scope	The Practice Premises, practices and applications to be supported are identified in tables 5.1, 5.2 and 5.4
CCG Note	*CCGs should define hours and any exclusions (eg public holidays) to suit local requirements*

GP IT Equipment Asset Management

Requirement	The asset management and disposal of all NHS owned GP IT equipment
Out of Scope	GP IT equipment not NHS owned
Transactional Support Services	Availability: Standard Service Hours All NHS Owned GP IT equipment: • must be recorded in an accurate asset register • is subject to an approved GP IT equipment reuse and disposal policy and procedure - using authorised compliant contractors • on disposal must be recorded in an auditable log - this will include date of disposal, method of disposal and data destruction certificate (when the item has data storage capability).
Specialist Support Services	Disposal will be carried out by a contracted authorised specialist IT hardware disposal organisation (meeting standards listed below) Support CCG to develop and maintain a local IT equipment reuse and disposal policy
Systems and applications	All software, browsers and operating systems not supported or maintained by the supplier must not be used on NHS owned GP IT equipment.
Applicable Standards	• Waste Electrical and Electronic Equipment (WEEE) Regulations (2013) • NDG standard 8
Practice Responsibilities (for information only)	*To provide consumables e.g. for printers and other operating requirements to any standard specified in the local Warranted Environment Specification or as otherwise specified by the manufacturer of the equipment.* *NHS owned GP IT equipment does not require to be individually insured under practice policies (content insurance) however the practice should take reasonable steps to ensure the physical security of the equipment, protecting against loss, theft or damage.* *To ensure environmental requirements (eg air-conditioning and fire suppression) and power supply for NHS owned IT equipment on Practice Premises.* *Practices are responsible for the secure disposal of any practice owned IT equipment. Practices are advised to seek specialist advice (from commissioned GP IT Delivery Partner) on secure disposal of such IT equipment. CCGs may at their discretion offer practices the use of their commissioned GP IT Equipment disposal services.*

CCG Note	*A local IT equipment re-use and disposal policy is required* *A disposal service may be provided through a directly commissioned service by the CCG or through a sub-contract of this service*

Software Licence Management

Requirement	All software and operating systems installed and operated on managed GP IT equipment will be licensed and managed
Transactional Support Services	Availability: Standard Service Hours • advice on availability of licences • procurement of additional licences • maintain licence register
Specialist Support Services	Availability: Standard Service Hours • development and maintenance of a local Warranted Environment Specification (WES) • specialist support is available for W10 and Automatic Threat Protection (ATP) deployments.
Systems and applications	• all software (including operating systems) used on Managed GP IT Infrastructure must be approved and recorded on a software licence register which must confirm that the software is appropriately and legally licenced for such use and does not present a cyber security risk. • supported operating system & browser compliant with local WES. • software, browsers and operating systems not supported or maintained by the supplier must not be used on NHS owned or managed GP IT equipment. • anti-virus software, encryption software and effective patch and upgrade management for operating systems and anti-virus software must be in place • PC Windows Operating Systems must be at least Windows 10 (supported version). • identity agent (for NHS Smartcards). • Microsoft Office will be provided on NHS owned devices through Microsoft Office 365 for the NHS licences until 31st March 2023. CCGs should make plans for office functionality after this date. • NHS funded applications and software licences are provided for use on Managed GP IT Devices. Their use on other devices, including personal devices, must be approved by the CCG, or their commissioned GP IT Delivery Partner on the CCG behalf. Particular attention should be given to ensuring (i) patient identifiable data does not become accessible from unmanaged and potentially insecure IT infrastructure (ii) the end user conditions of use for the licence and/or application are complied with.
Applicable Standards	NDG standard 8

Registration Authority

Requirement	A Registration Authority is a function, which carries out the identity checks of prospective smartcard users and assigns an appropriate access profile to the health professional's role as approved by the employing organisation. NHS smartcards or other approved authenticators are required to access NHS Spine information systems and registration authorities' roles and responsibilities are defined by NHS policy. Where new authenticators are reviewed and approved it is expected the Registration Authority function would continue to support issuance of approved alternatives
Transactional Support Services	Availability: Operational Support Hours • unlocking of smartcards • position based access control (PBAC) configuration Availability: Standard Service Hours • issuing of NHS Smartcards (including ID checks / printing etc). • provide practices with a facility to notify the RA Services Provider when practice staff leave the practice organisation or no longer require RA access to the practice, and ensure access is removed within the agreed performance standards for user account management. • deprecation of old NHS Smartcards: To remove all series, 3, 4, 5 & 6 NHS Smartcards by March 2023. • locally support the target to deprecate the current Care identity Service (CIS) by September 2023 which will be replaced by the NHS Care identity Service 2 (CIS2).
Specialist Support Services	Availability: Standard Service Hours • registration authority service including policing 'Access Policy' and the delivery and management of role-based or position based access control and issuing of smartcards. • training of practice RA managers and sponsors. • training and awareness of how to use new authenticators and the risks when users don't manage sessions appropriately. • support of software to support national systems for example.) Identity Agent, CIS. • ensure adherence to access security policy. • advise practice RA managers and RA sponsors of configuration of business functions, completion of documentation and use of RA systems (for example. reset PINs). • involvement in national project roll out such as attendance

	at project boards to support project delivery. • production of RA reports
Systems and applications	Identity Agent CIS
Applicable Standards	• National Registration Authority Policy. • NDG Standard 4. Only accredited suppliers can provide this service.
Applicable Guidance	• Registration Authority Operations and Process Guidance Registration authority governance
Practice Responsibilities (for information only)	• *practices are responsible for determining which practice and other organisation staff can access practice data and system functions, and the (system) role of that staff member, through the Registration Authority process.* • *staff access to all systems processing patient identifiable data is regularly reviewed and updated by the practice using the NHS RA service (or other local practice access controls).* • *designation of RA manager for the practice*

NHS Mail Administration & Support

Requirement	The local administration of NHS Mail accounts
Out of Scope	National NHS Mail Service Desk Support for email solutions other than NHS Mail
Transactional Support Services	Availability: Standard Service Hours • creation, deletion of user and email accounts. • password resets, account unlocking etc. • setting up shared mailboxes and enabling distribution lists
Specialist Support Services	Availability: Standard Service Hours • providing local administrator (LA) support for example for access and support for NHS Mail, support for migration from local email services to NHS Mail. • provide practices with a facility to notify the GP IT Delivery Partner when practice staff leave the organisation or no longer require NHS Mail access, and ensure access is removed within the agreed performance standards for user account management.
Applicable Standards	• NDG Standard 4 • NHS Mail Acceptable Use Policy
Applicable Guidance	• NHS Mail Support Portal • Sending sensitive information to non-secure email addresses (including patients)
Practice Responsibilities (for information only)	*NHS Mail is the primary email system for practices* *Practices are responsible for authorising creation and removal of NHS mail accounts belonging to their practice organisation within NHS Mail* *Practices are responsible for ensuring the security of any data held in practice staff NHS Mail accounts under the practice organisation, and for the correct removal or archiving of such data when any member leaves the practice.* *Practices will have at least one securely managed and daily monitored NHS Mail account to receive clinical documentation.* *Practices should ensure practice staff follow all NHS Mail guidance and advice on cyber security in their use of NHS Mail eg phising, spam etc* Practices must ensue personal, sensitive or confidential information is never sent by NHS Mail unless it is sent to another NHS Mail account or an email account with the same security accreditation standards OR as an encrypted email if sent to a non-secure email address. Where NHS Mail is used as part of two way written communications with patients encryption must be used.

Essential Infrastructure

Requirement	The provision, maintenance and technical support of the necessary infrastructure to deliver Core and Mandated GP IT services
Transactional Support Services	Availability: Operational Support Hours • through GP IT Service Desk • break - fix incident and problem resolution
Infrastructure	Availability: Standard Service Hours Provision, maintenance and technical support of the necessary infrastructure to deliver core & mandated GP IT capabilities, to include: • network connectivity and access to core GP IT services at point of care, including main to branch site(s) connectivity. • local network services, including equipment, structured cabling and support. • interface between locally managed networks and HSCN-GP, nationally managed services (e.g. Windows Managed Services), Legacy N3 and community partner networks • file management, data storage and hosting services for core services. • provide access to secure, resilient off-site data storage facilities for all practice electronic patient identifiable and clinical data other than that stored in the DCS catalogue clinical systems and NHS Mail and as required to deliver clinical services to a standard not less than tier 3 data centre OR compliant with "Health and social care data: off-shoring and the use of public cloud services guidance". Note that off-site storage arrangements made under the Privacy Shield may now require review. Data controllers and processors should ensure that any data transfer follows the latest ICO guidance and advice. Ensure adherence to policy advice as issued to ensure such data centres minimise their environmental impact and support the NHS drive to reach Net Zero. • maximum use should be made of best practice to reduce costs and increase efficiency such as secure cloud hosting, server virtualisation and storage area networks. • all backups of shared data storage are configured and executed to support compliance with the data backup and recovery procedure to allow the agreed RPO (Recovery Point Objective). • where practices choose to use VOIP telephony *The Supplier* will provide advice and technical support regarding the use of practice network infrastructure and if applicable HSCN connections. Note: Individual practices remain responsible for the cost of their telephony services including any additional infrastructure costs.
Applicable Standards	• Tier 3 data centre. • The *supplier* and any subsidiary service and infrastructure

	provider will operate to any prevailing NHS security standards, including the Data Security and Protection Toolkit or equivalent industry standard.
Applicable Guidance	• NHS Digital Good Practice Guides • NHS and social care data: off-shoring and the use of public cloud services guidance – NHS Digital • NHSE/I Green Plan Guidance document (update due Spring 2021) • GP Advanced Telephony Specification Commissioning Support Pack (GP IT Operating Model v5)

Desktop Infrastructure

Requirement	A desktop device support service, which includes provision and maintenance of the Managed GP IT Device estate. All practice staff, who require access to digital capabilities to carry out their role, will have access to a desktop or laptop computer at locations within the Practice Premises where they work with access to the Foundation Solutions Where practice staff access desktop computers and laptops in patient facing environments they will, as operationally required, have access to local and networked printing facilities within the Practice Premises.
Transactional Support Services	Availability: Operational Service Hours • installation and support of all desktop computers and peripheral equipment related to core GP IT services • installation and support of all approved standard software and applications on desktop computers • anti-virus and malware protection (using Windows ATP), • access management and port control on all active desktop devices • encryption to NHS standards on all mobile/portable devices (NHS Digital: Data Security Standard 9: IT Protection) • remote desktop support management available to 100% of workstations
Specialist Support Services	Availability: Standard Service Hours • defined and documented standardised desktop image(s), with a formal change control management system. • compliance testing and installation of standard software products. • compliance testing of software upgrades with NHS national digital services. • development and maintenance of a local Warranted Environment Specification (WES) to include (i) minimum specifications for hardware to be used locally (ii) any required standards for operating and maintenance consumables needed for the hardware e.g. printers.
Infrastructure	• the GP IT infrastructure estate supporting GP IT includes desktop computers, laptops, printers and other equipment, as necessary to operate those solutions selected to meet the Core and Mandated and the enhanced capabilities as provided to the practices. • the GP IT infrastructure estate provided to practices includes desktop computers, laptops, printers and other equipment, as necessary for the practice to operate the digital services listed in the schedule: Appendix 1 – Summary Of Services within the local CCG-Practice Agreement. The CCG will fund such equipment subject to availability of funds, and reasonable and fair practice use.

	Equipment required specifically for diagnostic or treatment purposes eg specialist cameras, physiological measurement devices and IT equipment defined under General Practice Business Requirements is excluded from this requirement to provide. • an agreed desktop Warranted Environment Specification (WES) which as a minimum, meets the spine WES and the relevant clinical system requirements. • user desktop workstations and laptops must be locked down and well managed, with advanced tools, processes and policies in place to support diagnosis, repair and updates. Unauthorised users must not be able to install unlicensed and unauthorised software or change critical settings. • all (Windows) Managed GP IT Devices must use Windows 10 as minimum operating system managed through the Windows Managed Service which must include Advanced Threat Protection (ATP) installed, operational and attributed to the responsible organisation (CCG). Any configuration exceptions eg earlier versions of Windows, or in scanning folders or files must be based on a documented local risk assessment (carried out as part of the cyber security service). A custom support agreement (CSA) must be in place (at local cost) for any GP IT managed device(s) still requiring to use versions of Windows beyond their end of support dates where this for an unavoidable specified purpose. • the CCG will have a budgeted plan for desktop GP IT equipment refresh which includes: desktop PCs, laptops, monitors, scanners, smartcard readers, printers including dual bin feed printers for consulting rooms and front desk/office areas as necessary. • the CCG will ensure a continual refresh programme subject to availability of funds which identifies and replaces hardware where it has reached its service life. • a local IT refresh and replacement plan will define equipment standards, availability for practices (where appropriate by practice type, size, clinical system etc) and target service life by equipment category. • in support of the commitment to deliver a 'Net Zero NHS' investment in desktop infrastructure should minimise energy usage including (i) power saving on IT devices (ii) optimizing equipment life cycle (e.g. with VDI) to reduce manufacturing energy costs. • the refresh service will include assessment, procurement, rollout, asset tracking and secure disposal (see "Asset Management and Software Licencing Service").
Systems and applications	• unsupported or unmaintained software (by software supplier), browsers and operating systems must not be used on NHS Managed GP IT Infrastructure.

	• the capability for the central control of desktop security, patch control, access and software installation across the managed GP IT estate. • remove old versions of the IA Client from all Managed GP IT Devices replacing with v2.3+ • install new desktop components when required to support new NHS applications and services that support NHS Care Identity Service 2 (CIS2)
Applicable Standards	• NDG Standard 8. • Information Security Management: NHS Code of Practice • NHS Digital: Data Security Standard 9: IT Protection • https://digital.nhs.uk/services/spine/spine-technical-information-warranted-environment-specification-wes
Practice Responsibilities (for information only)	*To provide consumables eg for printers and other operating requirements to equipment manufacturer's standard or to any standard specified in the local Warranted Environment Specification* *Unsupported or unmaintained software (by software supplier), browsers or operating systems must not be used on NHS Managed GP IT Infrastructure.* *To ensure the physical security, protecting against loss, theft or damage, and environmental requirements (eg air-conditioning and fire suppression) and power supply for NHS Owned GP IT equipment on Practice Premises*
CCG Note	*Recommendation A local SLA should be based upon an agreed desktop estate volume.*

Remote access

Requirement	Practice staff have secure access outside the Practice Premises to the foundation solution and other essential clinical system capabilities as necessary to support clinical consultations and access to other core digital services eg email. This includes any necessary mobile and remote access infrastructure. The options for remote access are described below. To support resilience and business continuity requirements the service(s) provided should be able to support at least 60% of clinical and essential administrative practice staff working remotely
Out of Scope	Any remote access solutions not part of the Managed GP IT Infrastructure. Internet connectivity eg Broadband connections delivered into private homes or other places which are not Practice Premises Telephony access (see separate requirements) Mobile data and voice connectivity to equipment which is not a Managed GP IT Device Health & safety (including DSE and PAT) regulations for remote and home working
Transactional Support Services	Availability: Operational Service Hours Provision, maintenance and technical support of the necessary technology and supporting infrastructure to deliver remote access to the clinical system for consultation purposes. Where a Managed GP IT Devices is provided • the use of mobile computing systems is controlled, monitored and audited to ensure their correct operation and to prevent unauthorised access, supporting DSPT requirements for general practice. • this includes provision, maintenance and return to base support of software and managed infrastructure including mobile devices necessary to support clinical system access.
Infrastructure	Availability: Standard Service Hours The Remote Access solution will be provided either of the following options, or a combination of both.

A.
A Managed GP IT Device (eg laptop or desktop) with all software necessary for the role (as native application or in a VDI service) together with a token for secure VPN access and a smartcard reader.
Where a Managed GP IT Device is provided

- mobile devices must be locked down and well managed, with advanced tools, processes and policies in place to support diagnosis, repair and updates. Users must not be able to install unlicensed or unauthorised software or change critical settings.
- encryption to NHS standards on all mobile/portable devices (NHS Digital: Data Security Standard 9: IT Protection)
- connections between mobile/portable/remote devices to HSCN/N3 and the practice clinical system using public network services (internet) must be encrypted to approved NHS standards.

Refresh Programme (for Managed GP IT Devices)

- the CCG will have budgeted plan for mobile device refresh.
- the CCG will ensure a continual refresh programme which identifies and replaces mobile devices where it has reached the end of its service life.
- a local IT refresh and replacement plan will define mobile equipment standards, availability for practices (where appropriate by practice type, size, clinical system etc) and target service life by equipment category.
- the refresh service will include assessment, procurement, rollout, asset tracking and secure disposal.

B.
Using staff personal devices (also known as “Bring Your Own Device” – BYOD)
Where personal devices/BYOD are used

- a virtualised desktop infrastructure (VDI) service will be provided allowing access to the foundation solution and other essential clinical system capabilities as necessary with a token for secure VPN access and a smartcard reader.
- NHS applications approved for use over the public internet (eg web accessed NHS Mail – not local email

	programme such as Outlook) may be used • when used within Practice Premises BYOD equipment may only connect to the Managed GP IT Infrastructure using the Public WiFi-GP service • NHS Smartcard readers should be provided as required • an assurance process must be in place to ensure the personal devices are sufficiently secure including broadband firewall, secure WiFi, anti-virus software, dedicated user account, patch management and operating system updates. • mobile application management (MAM) and mobile device management (MDM) should be considered • support the CCG develop and implement a BYOD policy which must include cyber and data security, software licencing and ownership, data storage, support, data and security breaches, loss of device, and termination. NB: Staff cannot be mandated to use their personal devices for NHS purposes. Remote access solutions must not be used which bypass or otherwise reduce the effectiveness of the security measures within the GP IT Futures Framework Services, the National Digital Services and the Managed GP IT Infrastructure (including smartcard access). Specifically, the following remote access solutions should not be provided or supported: • use of a personal device (laptop or desktop) accessing clinical systems using either (i) client software installed on the personal device or (ii) desktop sharing software (ie remote desktop protocol (RDP) or equivalent) to remotely access a host device eg in the practice.
Systems and applications	• Software, browsers and operating systems not supported or maintained by *The Supplier* must not be used on NHS Managed GP IT Infrastructure.
Practice Responsibilities (for information only)	*Compliance with NHS and local information security standards and policies.* *Follow NHSX advice on using online consultations in primary care including (i) working collaboratively with local IT/technical teams to understand network issues, explore technology options and then with local Data Protection and Clinical Safety Officers for using technology within information governance, data security and clinical risk management guidelines (ii) robust*

	measures for patient/carer verification and authentication are in place
Applicable Standards	● NDG standard 8 ● Information Security Management: NHS Code of Practice ● NHS Digital: Data Security Standard 9: IT Protection ● NHS Mail Acceptable Use Policy
CCG Note	*Recommendation: The local SLA is based upon an agreed mobile estate volume. This requirement could be sourced through a separate contract*

Controlled Digital Environment

Requirement	The effective and secure management of the GP IT estate and GP Digital Services requires that there is an accurate and contemporaneous record of the digital environment and that the desktop estate can be updated and monitored centrally.
Out of Scope	Practice owned and practice managed GP IT equipment not connected to the Managed GP IT Infrastructure eg photocopier, practice provided telephony system. Personal devices
Transactional Support Services	Availability: Operational Service Hours • There must be the capability for the central control of desktop security, patch control, access and software installation for all desktops & laptops within the Managed GP IT Device estate. • Provide practices with a facility to notify *The Supplier* when staff leave the practice organisation or no longer require IT access, and ensure access is removed within the performance standards for user account management
Specialist Support Services	Availability: Standard Service Hours There will be an accurate and contemporaneous record of the following • GP IT hardware inventory and assets • software and software licences installed on devices within the Managed GP IT Device estate • Information Systems ie applications and data • Practice Premises where support services are provided and Managed GP IT Infrastructure is used • supported organisations (practices and others) • support contracts • users and access accounts All Managed GP IT Devices will be recorded individually on an electronic database. This will include a unique asset / serial number, location, date installed, planned replacement date. Low value accessory items (e.g. keyboard, mice etc) should be excluded. Where appropriate items can be aggregated e.g. mouse, keyboard, monitor to a single recordable asset. All IT equipment with data storage must be included. Managed GP IT Devices using Windows 10 operating system (see Desktop Infrastructure) will be managed through the Windows Managed Service which must include Advanced Threat Protection (ATP) installed, operational and attributed to the responsible organisation (CCG).
Applicable Guidance	Where centralised technologies are deployed assurances should be sought to ensure that the security, performance and resilience of GP Foundation Solutions, other DCS Catalogue solutions and National Digital Services are not compromised.

Practice Responsibilities (for information only)	*Practice owned and practice managed IT equipment not connected to the Managed GP IT Infrastructure eg photocopier, practice telephony system.* *Personal devices*

Cyber Security

Requirement	Cyber security management and oversight, including configuration support, audit, investigation, incident management and routine monitoring, relevant to the services and Managed GP IT Infrastructure • Protective technical and organisational measures to reduce the likelihood and impact of cyber security incidents • Management of high severity cyber security incidents • Oversight of management of low & medium severity cyber incidents • Disaster Recovery and Business Continuity plans for systems and infrastructure relevant to GP IT Services. • Supporting Practice Business Continuity Plans
Out of Scope	Disaster Recovery and Business Continuity Plans for national digital services and for GP IT Futures Framework will be managed nationally although these should be referenced in these plans as third party services.
Transactional Support Services	Availability: High Severity Incident Support. GP IT support **must include** access for out of hours **high severity service incident** alerting, logging and escalation in accordance with the approved business continuity and disaster recovery plans. Cyber-attacks against General Practice services are identified and resisted. *The Supplier* will support the CCG in the following: Urgent out of hours contacts and communication routes for all practices and suppliers should be held by the CCG and regularly maintained. The MHRA Central Alerting System (CAS) using email and mobile phone text alerts for general practices may allow CCGs to fulfil this requirement for practice contacts. CCGs should ensure practices have registered for this service using a practice generic email account (not an individual account). Action is taken as soon as possible following a cyber incident with a report made to the senior management within the commissioning CCG and the impacted practice within 12 working hours of detection. Significant cyber-attacks are to be reported in line with national guidance promptly following detection. For high severity incidents a Lessons Learned Report (with relevant action plan as appropriate) to be provided to the CCG within 2 weeks of the recorded resolution of the incident on the service desk.

	The Data Security Centre operated by NHS Digital offers a range of specialist services that help health and care organisations manage cyber risk and recover in the event of an incident. In the event of a national cyber incident being formally declared (e.g. by the NHS Digital Data Security Centre) *the supplier* and all other parties will fully cooperate and support the actions required by the NHS Digital and NHS England Emergency Preparedness, Resilience and Response (EPRR) team, (or any party with delegated authority). This may include providing urgent out of hours access to Practice Premises, digital systems and equipment. *The Supplier* will fully cooperate in any high severity cyber incident management and cyber related Business Continuity and Disaster Recovery Planning with any nationally commissioned organisation with geographical responsibility for coordination and management of high severity cyber incidents, as and when such a service is commissioned. Administration access rights for Active Directory configuration and services relevant to the Managed GP IT Infrastructure used by the practice must be strictly controlled to a limited number of named and technically qualified individuals as part of the overall managed infrastructure. Administration access rights for Office 365 should align to those for Active Directory. Administration Access rights for network configuration and equipment (eg routers, switches, firewalls, wireless access points etc) must be strictly controlled to a limited number of named and technically qualified individuals as part of the overall managed infrastructure. Generic (ie not assigned to an individual) administrator accounts must not be used.
Specialist Support Services	Availability: Standard Service Hours **Infrastructure** A Cyber Security service will be available to all practices encompassing all Managed GP IT Infrastructure and systems to ensure: • Provision of necessary IT security / cyber evidence to support DSP Toolkit for General Practice. • Audit and investigative services are available • Specialist (cyber Security) advice is available • There is a shared HSCN-GP security contact for practices. Monitoring through Active Directory to identify dormant accounts and operate a process to archive & disable these. Provide

	practices with a facility to notify the *The Supplier* when staff leave the practice organisation or no longer require IT access, and ensure access is removed within the performance standards for user account management (NDG Standard 4). **Business continuity and Disaster Recovery Plans** • *The Supplier* must develop and maintain a business continuity and disaster recovery plan (for services relevant to General Practice IT provision). These plans must include responses to a high severity data or cyber security incident and must be based on a Recovery Time Objective (RTO) of not more than 48 (actual) hours for Essential Services. • Business continuity and Disaster Recovery plans must be regularly reviewed (at least annually) and refreshed. In the event of a major event when the plan(s) is utilised a review of the plan will be triggered. • In the event of the Business continuity and/or Disaster Recovery plan being invoked where services relevant to GP Services were impacted (including IT security threats & incidents) the CCG should receive an initial report within 12 (working) hours of the incident and a full report including root cause and remedial actions within 2 weeks of the incident. **Practice Business Continuity Plans** • Support the CCGs to ensure business continuity plans are in place for all practices and are reviewed and approved as required under the CCG-Practice Agreement. • Advice & guidance to support the development of the digital element of practice BC plans, is available to practices when required. • In the event of a practice Business Continuity Plan being invoked specialist technical support will be available. Cyber alert notifications: Support CCGs to ensure: • Cyber alert notifications are acted on in line with suggested timescales. Action on high severity cyber alerts are evidenced through the NHS cyber alert service. • Confirmation is given within 48 hours that plans are in place to act on high severity cyber alerts. • A primary point of contact for the CCG or its GP IT Delivery Partner to receive and coordinate your organisation's response to Cyber alert notifications is registered. Note: Action might include understanding that an alert is not relevant to your organisation's systems and confirming that this is the case. **On-Site Assessments**

	• *The supplier* will co-operate with any on-site data and cyber security assessment carried out under NHS Digital's Data Security Assessment programme, or provide evidence of equivalent assessments or certification to a cyber security scheme approved within the Operating Model. **Organisational Awareness** • *The supplier* must allocate a senior level (e.g. director or equivalent) responsibility for cyber and data security within their organisation. **Supporting Projects** Advice for practices and the appointed project teams on cyber security considerations where projects involve • Change of Foundation Solution for the practice (including data migration activities). • Significant estate developments and new builds. • Deploying new technologies.
Infrastructure	• The Managed GP IT Infrastructure should be subject to penetration testing to National Cyber Security Centre (NCSC) standards at least annually. The scope of the penetration testing must be agreed by the CCG SIRO (or equivalent officer) and must include (i) checking that the default password of network components has been changed (ii) all webservers, on the Managed GP IT Infrastructure, the practices utilise. • Business Continuity arrangements for Managed GP IT Infrastructure must include the capability to isolate affected PCs from the network within no more than 48 (actual) hours of a cyber attack.
Systems and applications	• Password managers and Single Sign On (SSO) technologies can be provided or supported subject to prior security assessment. These tools where used should augment existing security and authentication controls and should not be used to bypass or reduce the effectiveness of accredited two part authentication controls (eg NHS smartcards). NCSC provides guidance on password managers.
Applicable Standards	• National Cyber Security Centre (NCSC) approved penetration testing • NDG Standards 6,7,8,9 • Data Security Standard 9 IT Protection (NHS Digital) • ISO 22301 (for Business continuity). • Data Security and Protection Toolkit (DSPT) • Information Security Management: NHS Code of Practice • *The Supplier* will be compliant with the following standards: • NHS Information Governance – to demonstrate

	satisfactory compliance as defined in the NHS Data Security and Protection Toolkit (DSPT) for the relevant organisation type. • Accreditation to Cyber Essentials Plus (CE+). • Accreditation to ISO 22301 for Business Continuity Management OR compliance with the NHS England Business Continuity Management Framework and registered for: • NHS Digital Cyber Alert Service
Applicable Guidance	• General Data Protection Regulation (GDPR) • Data Protection Act 2018 • Primary Medical Care Policy and Guidance Manual.
Practice Responsibilities (for information only)	• *Each Practice must have a named partner, board member or equivalent senior employee to be responsible for data and cyber security in the practice. This requirement further defines practice obligations within the CCG-Practice Agreement to identify the person with lead responsibility for IT matters in the Practice. The CCG as commissioner of GP IT services will be responsible for providing specialist support to this role but each practice remains accountable.* • *Practices will fully cooperate with an on-site cybersecurity assessment if invited to do so and will act on the outcome of that assessment, including implementing any recommendations where applicable to the practice.* • *Practices should provide urgent out of hours contacts and communication routes as well as access to Practice Premises, digital systems and equipment outside normal working hours.* • *When a cyber security incident takes place the practice should quickly establish if a personal data breach has occurred (in accordance with GDPR Article 33, refer to Recitals 85, 86, 87 & 88 for further detail) and if so take prompt steps to report and manage this (see Information governance and support).* • *Each practice will maintain a business continuity plan (BCP) approved by the CCG which should include a response to threats to data security.* • *Assurance will be provided through the general practice Data Security and Protection Toolkit which each practice is required under the CCG-Practice Agreement to complete annually.* • *Advice & guidance to support the development of the digital element of practice Business Continuity plans, is available to practices when required.* • *Although fewer hosted systems are now located within individual Practice Premises Business Continuity planning remains crucial. Assurances are also required from any*

	third parties, providing infrastructure and/or data processing services that they have robust Disaster Recovery Plans. • *All practice staff must complete annual NHS Data Security Awareness level 1 mandatory training*

Information Governance Support

Requirement	Information governance support, guidance and advice to support practice compliance with common-law duty of confidence, records management, information security, DSP Toolkit, Data Protection Act 2018 and Caldicott standards and to ensure all devices and systems are managed and used in a secure and confidential way.
Out of Scope	Legal Advice
Transactional Support Services	Availability: Standard Service Hours **Data Breaches** A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed. Any data breach (or near miss) of practice patient personal information will require actions by one or more of the following; • The individual practice as data controller. • National NHS commissioned GP Digital services suppliers as data processor(s). • *The Supplier* as data processor AND as specialist support service to practice. • Local health & social care providers where data has been shared as data processors. • Any other digital services supplier commissioned locally by the practice jointly or through a PCN or federation – as data processor. Practices will receive the following support: • The provision of advice and/or support to practices on the investigation of possible information security breaches and incidents. • Advice on incident/breach assessment and reporting via the incident reporting tool within the DSPT to NHS England and reporting to the ICO (dependent upon severity of incident). • Advice on assessment and reporting via the incident reporting tool within the DSPT to NHS England and ICO (dependent upon nature and severity of the breach). • Advice on post-incident reviews and recommended actions for practice implementation.

	• To lead or direct data breach reviews and investigations where highly specialist knowledge is required or complex multi–party issues are involved. *The Supplier* as data processor will: • To take action immediately following a data breach or a near miss, alerting promptly the practice as data controller and with a report made to the senior management within the CCG and the practice within 12 (working) hours of detection. • Report data breaches in line with NHS guidance (using the incident reporting tool within the DSPT) and legal requirements immediately following detection. • Provide a Lessons Learned Report (with relevant action plan as appropriate) to the CCG within 2 weeks of the recorded resolution of the incident on the service desk.
Specialist Support Services	Availability: Standard Service Hours **IG policy support** Support for the production and maintenance of local information governance policies and procedures for practices. Provision of advice and support to practices on approval, ratification and adoption of the policies for their organisation. **Support for Data Security and Protection Toolkit compliance** Provide advice and guidance to practices on how to complete the DSPT, including the collection and collation of evidence in support of DSPT submissions. Provide practices with evidence required for DSPT where this is held by the CCG or its commissioned IT providers. **IG consultancy and support** Provision of advice, guidance and support on IG related issues, including existing operational processes and procedures or new business initiatives. Advice and guidance on personal data access (but not extending to legal advice). **IG advice and Data Protection Officer (DPO) Support** Provision of advice, guidance and support on IG related issues including existing operational processes and procedures or new business initiatives to support practice designated Data Protection Officers including existing operational processes

	and procedures or new business initiatives. To include • Access for Practices during normal service hours to specialist qualified advice on GDPR matters. • Advice on compliance with GDPR obligations • Advice reflecting national guidance on GDPR compliance as it is published. • A review at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security. This may for example be a facilitated workshop at CCG level which would encourage shared learning. • Advice to support practices develop and maintain best practice processes that comply with national guidance on citizen identity verification, including "Patient Online Services in Primary Care - Good Practice Guidance on Identity Verification", that underpins the delivery of patient facing services, and assurance requirements as these are developed. • Advice to support practices achieve mandatory compliance with the National Data Opt Out policy by March 2020. **Reviews** • Published NHS Digital Good Practice Guides will be reviewed and where applicable incorporated into commissioned GP IT Services. • Support practices to review at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security. This may for example be a facilitated workshop at CCG level which would encourage shared learning. **Supporting Projects** Advice for practices and the appointed project teams on IG/DSP, data sharing, DPIA completion and cyber security considerations where projects involve • Change of Foundation Solution for the practice (including data migration activities) • New initiatives involving sharing patient data with third parties • Merging practices • Closing practices • Significant estate developments and new builds • Deploying new technologies This is not an exclusive list. Specialist support for projects beyond general advice for example preparing Data Privacy Impact

	Assessments should be resourced as part of the project plan.

Applicable Standards	• Data Security and Protection Toolkit (DSPT)
	• NDG Standards
	• Incident reporting tool for data security and protection incidents within the Data Security and Protection Toolkit
	• As minimum note & comply with:
	  ○ Records Management Code of Practice 2020
	  ○ Code of practice on confidential information
	  ○ Information security management NHS code of practice
	Supplier IG staff providing the service should be appropriately trained and qualified to recognised industry standards such as the British Computer Society (BCS) Practitioner Certificate in Data Protection or equivalent level recognised industry standard

Applicable Guidance	• NHS Digital Good Practice Guides • Patient Online Services in Primary Care - Good Practice Guidance on Identity Verification
CCG Note	*Data processing activities using general practice controlled personal data carried out by local CCG commissioned data processors will be identified and recorded in a data processing agreement as set out in the CCG-Practice Agreement in accordance with the digital services acquired and regularly reviewed.*
Practice Responsibilities (for information only)	*Individual practices as contractors are responsible for* • *reporting and managing personal data breaches-within 72 hours* • *communication of a "high risk" breach to individual patients as required under GDPR* • *reporting and managing data breach near misses* • *the production, approval and maintenance of (and adherence to) their IG and IT security policies but support will be provided.* • *submitting a Data Security and Protection Toolkit (DSPT) return annually as required under the CCG Practice Agreement and responsibility for this lies solely with the practice.* • *nominating a person with responsibility for practices and procedures relating to the confidentiality of personal data held by the practice* • *completion by all practice staff of annual data and cyber security training.* *As independent contractors are responsible for sourcing any legal advice they may require to support any of these activities.* • *the regular review of internal processes. This should include a review at least annually to identify and improve processes which have caused breaches or near misses, or*

	which force staff to use workarounds which compromise data security.

Data Protection Officer (DPO) Function

Requirement	A Data Protection Officer will be available (in addition the DPO support service) for practices to designate as their Data Protection Officer. A named Data Protection Officer could be shared between several practices. Note: Practices may choose to make their own DPO arrangements at their own cost.
Specialist Support Services	Availability: Standard Service Hours **DPO Function** A Data Protection Officer will be available (in addition the DPO support service) for practices to designate as their Data Protection Officer. A named Data Protection Officer could be shared between several practices. Note: Practices may choose to make their own DPO arrangements at their own cost.
Practice Responsibilities (for information only)	*Individual practices as contractors are responsible for* • *under GDPR legislation to designate their own Data Protection Officer (which can be shared), any practice is entitled to decline the commissioned IG Advice and DPO service and make their own arrangements and DPO appointment at their own costs. Practices appointing their own DPO must ensure appropriate qualifications and standard are met.*

Clinical Safety Assurance

Requirement	Clinical safety assurance advice and support
Out of Scope	The responsibility and burden of effort for Clinical Safety Assessment and assurance under DCB0129 rests with the system developer. This includes any third party software incorporated into the system. The requirement for this service is to secure assurance from system suppliers that this has been met during procurement or contract review stages.
Specialist Support Services	Availability: Standard Service Hours Ensuring that the necessary standards are met for management of clinical risk in relation to the deployment and use of health software. **Advice and Supporting Assurance** Advise CCG and practices on compliance with: Clinical Risk Management: Its application in the manufacture of health software DCB0129: during procurement Clinical Risk Management: Its application in the deployment and use of health IT systems DCB0160 (where required): during deployment and business as usual. Medical Device Directive where a system/software (or part of it) is classified as a medical device **Incident Management** Support and advice for practices in the identification, reporting and management clinical safety incidents (information system related) within practices. **Supporting Projects** Advice for practices and the appointed project teams on Clinical Safety (DCB0160) where projects involve • Change of principle clinical system for the practice (including data migration activities) • New initiatives involving clinical systems to support different or innovating ways of working • Reconfiguring clinical systems with the potential to bypass or deviate from internal system controls and safeguards • New clinical systems integrating with the principle clinical system • Decommissioning clinical systems eg when merging or closing practices • Deploying new technologies • Clinical system procurement including third party assurance This is not an exclusive list Support for projects beyond general advice for example preparing

	Clinical Risk Management Plan, Clinical Safety Case Records and Hazard Reports and supporting procurement activities should be resourced as part of the project plan.
Applicable Standards	• DCB0160: Clinical Risk Management: Its Application in the Deployment and Use of Health IT Systems. • DCB0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems. • EU Medical Devices Regulations (MDR). • EU In-Vitro Diagnostic medical device Regulations (IVDR). • Clinical Safety Management: Clinical Incident Reporting (NHS Digital) *Supplier* staff should be appropriately trained and qualified to recognised industry standards such as NHS Digital's Clinical Safety Officer Foundation Course or equivalent level recognised industry standard.
Applicable Guidance	Clinical Safety Guidance – NHS Digital Introductory guide to the new MDR & IVDR (MHRA)
Practice Responsibilities (for information only)	*Practices must report clinical safety incidents in line with national guidance.* *Practices as independent contractors are responsible for sourcing any legal advice they may require to support any of these activities*

Digital Services Procurement Support

Requirement	Supporting CCGs and practices with specialist procurement advice and specialist technical advice including advice on the procurement of capabilities through the GP IT Futures Framework
Out of Scope	Funding for the digital solution being procured and support for its deployment and implementation is not part of the procurement support service as this is an internal CCG (or general practice) responsibility
Specialist Support Services	Availability: Standard Service Hours **General Digital Procurement Support** • Provide strategic procurement advice, recommending collaboration and standard specifications to optimise efficiency and support costs • Advice and assistance in the development of outputs based specifications to support GP IT procurement projects • Advice on procurement of GP IT using national frameworks as appropriate • Advice on applicable standards and accreditations for procurement • Ensure the obligations on the data processor to the individual practice(s) as data controller are reflected in the contract, in particular with regard to reporting data breaches and near misses. • Accessing where applicable, the National Commercial & Procurement Hub to support CCG procurement • *The Supplier* **MUST** advise the CCGs if any procurement activity in support of GP IT on behalf of the CCG may represent a conflict of interest for *The Supplier* or potential procurement challenge **GP IT Futures procurement support** Supporting mini-competition work for the procurement by CCGs from the GP IT Futures Services Framework. Meeting practice capabilities within nominated CCG funding allocations whilst ensuring excellent value for money **Non-GP IT Futures procurement support** Practices and CCGs purchasing non-GP IT Futures Framework clinical systems and digital technologies which include hosting patient identifiable information are responsible for ensuring that the hosted solution provider (as data processor) meets standards detailed below.
Other Controls	Procurement legislation

Applicable Standards	• NHS England Financial Guidance. • NDG Standard 10 • Practices and CCGs purchasing non-GP IT Futures Framework clinical systems and digital technologies which include hosting patient identifiable information are responsible for ensuring that the hosted solution provider (as data processor) are able to: • provide Information Governance assurances for their organisation via the NHS Data Security and Protection Toolkit. • confirm that the manufacturer/developer of the system has applied clinical risk management as required under DCB0129 (Clinical Risk Management: it's Application in the Manufacture of Health IT Systems) during the development of the product procured. • confirm where the product procured is classified as a medical device the product complies with the medical device directives. • comply with the National Data Guardian's recommended ten Data Security Standards. • Comply as data processor with Data Protection legislation and the NHS DSP Toolkit. • contractually agree to it's the obligations as data processor to the individual practice(s) as data controller. This will include a compliant Data Processing Agreement. • if applicable, comply with national guidance on citizen identity verification, including "Patient Online Services in Primary Care - Good Practice Guidance on Identity Verification". • if applicable, comply with the National Data Guardian eight-point data sharing opt-out model.
CCG Note	*CCGs should ensure appropriate measures are taken to avoid any conflict of interest where The Supplier may also be a potential provider of the new services being procured*

Digital Services Contract Support

Requirement	Facilitating CCG GP IT delivery with support for contract and supplier management and technical support. Solutions procured through GP IT Futures Framework or directly by the CCG for use by its practices. As end users of services practices are required to comply with any end user terms and conditions of use but wherever the contract is held by the CCG or NHS Digital a support service is required to manage local technical and contractual issues on behalf of the practice with *The Supplier*.
Out of Scope	Support for contracts for practice business support systems Support for contracts held by parties other than CCG or NHS Digital. Support for contracts directly held by the practice. Payments and invoice processing for the contracted digital solutions is not part of the contract support service as this is an internal CCG (or general practice) responsibility.
Specialist Support Services	Availability: Standard Service Hours • Ongoing support for practice clinical systems including technical liaison with system supplier and clinical application support where not provided by system supplier. • In the event of any unresolved issues, escalate to suppliers on behalf of practices to facilitate a satisfactory resolution. • Assist CCG in its responsibility to monitor and escalate to NHS England clinical systems performance issues in relation to the use of services and solutions provided under the CCG-Practice Agreement. • Use of the GP IT Futures CRM to track clinical system capabilities deployed by practice. • Local management of service support contracts/supplier liaison on CCG behalf. • Ensure local GP IT Futures Framework contracts are current and accurate. • Assist CCG in informing Foundation Solution Suppliers of any changes to existing contracts (held by CCG / NHS), for example terminations due to practices changing foundation solution or changes arising from practice mergers. • Liaising with GP IT Futures Framework suppliers regarding future requirements and developments. • Management of ongoing system updates as necessary where these are not directly managed by the system supplier • Supporting practice data migration end to end process for GP IT Futures Foundation Solutions in line with applicable data migration standard.

Estates Strategy

Requirement	Provision of advice and guidance to support the development of GP estate relevant to the provision of GP IT services and systems
Out of Scope	Funding and resourcing support for new estates developments should be provided through the relevant business case for that development.
Specialist Support Services	Availability: Standard Service Hours • Advice on IT infrastructure requirements and standards • Identify, as required, suppliers for IT infrastructure and external services for example HSCN connectivity, WiFi-GP • Support development of associated business case for individual estates projects, including consideration of resource and funding requirements • Advice and guidance should include consideration of transformation opportunities, productive GP IT services and local digital strategy • *The Supplier* **MUST** advise the CCGs if any of the above activities on behalf of the CCG may represent a conflict of interest for the supplier or potential procurement challenge NOTE: Any increase in the managed GP IT estate will require agreement between the commissioners of primary care (NHS England/CCG) and GP IT services (CCG), GP and the IT delivery partner. The resourcing and funding for individual estate development projects should be incorporated into the overall business case for that development.
Practice Responsibilities (for information only)	*Practices should engage with CCGs at an early stage of planning any Practice Premises development or expansion which will impact of GP IT provision*
CCG Note	*Service provision should be agreed at an appropriate level and capacity within the SLA*

Clinical Systems Training and Optimisation

Requirement	Training service for practice staff to support the safe and effective use and optimisation of clinical systems.
Out of Scope	Training in generic basic IT skills, business administration systems and office systems
Specialist Support Services	Availability: Standard Service Hours The service should include training for: • GP IT Futures to meet core & mandated capabilities • National digital services And will include training requirements arising from: • Staff turnover, • Refresher training, • New system functionality. Review the Practice's training plan and may request changes to the plan in line with local priorities and plans for the deployment of services. Assist the CCG confirm its agreement to the training plan, amended as agreed by the parties. Training will be provided for Practice staff in line with each agreed practice training plan. All end users in practices are trained in the use of the Foundation Solutions and that this is delivered in line with the GP IT Futures Training Standard. **System Optimisation:** • Support practice optimisation of GP IT Futures Foundation Solutions and national digital services, by providing support, guidance and advice, including User Group facilitation to enable sharing of best practice **Training delivery should reflect:** • Practice training plans and staff training needs analysis, • Environment and estate accommodation and facilities, • Virtual and online delivery channels, • Resource availability, • User satisfaction and customer feedback.
Applicable Standards	• NHS IT Skills Pathway • GP IT Futures Framework Training Standard
Practice Responsibilities (for information only)	*Practices shall carry out a training needs analysis that identifies the Practice staff that require training in the use of the Core and Mandated capabilities provided to the practice* *Practices shall ensure that new starters receive adequate training before they use the Core and Mandated capabilities provided to*

	the practice *Using the output from the training needs analysis, practices shall prepare a training plan for the Practice which identifies the staff to be trained and the training to be provided by the CCG over a six month period or more as agreed by the parties.* *Practices shall make their staff available for training in line with any timetable agreed with the CCG or The Supplier and shall be responsible for the costs of making staff available for such training including backfill costs and travel costs.* *Practices shall maintain an up-to-date record of staff training.* *Practices can request and agree amendments to the training plan in line with new developments and the changing requirements of the CCG and the Practice.* *Practices shall ensure that all end users are trained to a minimum entry level standard as per the NHS IT Skills Pathway including use of relevant operating systems and office productivity software. Training in generic basis IT skills, business administration systems and office systems is the responsibility of the practice.*
CCG Note	*Recommendation: The local SLA should quantify training resources based on either the number of practice staff or the number of practices (weighted by population where appropriate).*

Data Quality Support

Requirement	Data quality training, advice and guidance
Specialist Support Services	Availability: Standard Service Hours. Comprehensive data quality advice and guidance service available to all practices, including training in data quality, clinical coding and information management skills. Development and delivery of a practice data quality improvement plan, where necessary and supporting practice DSPT submission (data quality assertions). This may be carried out at individual or practice group level as appropriate. The service should include advice and guidance for: • National data audits/extracts/reporting e.g. National Diabetes Audit, • General reporting, • Template development & template quality assurance • Spreading best practice, • Data migrations as part of system deployments, • Clinical/medical terminology, • SNOMED CT clinical coding standards and requirements, including training and facilitation for staff and associated support materials in order to support the effective transition to SNOMED CT and ongoing support to fully realise the benefits that can be achieved through the use of SNOMED CT, • Review of reports and templates to locally re-author within SNOMED CT. Failure to do so may mean reports and templates becoming out of date.
Applicable Standards	• SNOMED CT in General Practice / Standards Change Notice SCCI0034 Amd 35/2016 • Data Security and Protection Toolkit (DSPT) (data quality assertions) GP IT Futures Data Migration Standard
Practice Responsibilities (for information only)	*Individual practices are responsible for the quality of their patient records and the application and use of clinical terminology.*

Project and Change Management

Requirement	Formal P3M (Project, Programme and Portfolio Management) methodologies which are recognised and used in the deployment of GP clinical systems, local implementation of national solutions and major GP IT infrastructure changes or upgrades.
Specialist Support Services	Availability: Standard Service Hours Skilled project and programme management resources must be available, to deliver the planned programme of work, both nationally and locally driven. The service should include: • Programme management, • Project management, • Change management, • Benefit realisation support. Technical and specialist expertise should also be available through the relevant requirement to support projects. Supporting significant deployments and developments through and end to end project management of GP IT Futures Foundation Solutions, including: • Change of Foundation Solution for a practice including data migration activities (to GP IT Futures Data Migration Standard) and training (to GP IT Futures Training Standard) • New initiatives involving sharing patient data with third parties • Merging practices • Closing practices • Significant estate developments and new builds • Deploying new digital technologies This is not an exclusive list.
Applicable Standards	*Supplier* staff should be appropriately trained and qualified to recognised industry standards such as APMG in; project management – eg Prince II Practitioner, programme management – eg Managing Successful Programmes Practitioner, change management – eg Change Management Practitioner Or equivalent level recognised industry standard. GP IT Futures Data Migration Standard GP IT Futures Training Standard
CCG Note	*CCGs should ensure there is sufficient understanding of available capacity and how that capacity can be used eg This may be*

	provisioned within current SLA support arrangements or could be procured on an ‘as required’ basis.

National Digital Services Implementation

Requirement	Local promotion, deployment/implementation and support of National Digital Services, including SCR, EPS2, e-RS, GP (Patient) Online and GP2GP services.
Specialist Support Services	Availability: Standard Service Hours • Advise practices on current and planned national developments and solutions. • Maintain national tracking database, or any future replacement, with local status of system deployments, changes and updates as required nationally. • Local deployment programme for national systems implementation within practices, including benefits realisation, stakeholder engagement, business change support.

CCG Note: *The following:* ***GP IT Enabling Requirements*** *in Category 3 may be commissioned directly from a specialist provider or may be included in this specification*

Electronic messaging for direct patient communication

Requirement	Electronic messaging (SMS or equivalent) for direct individual patient clinical communication. The ability for practices to communicate short messages to patients, to a locally agreed standard/format, for example: • Reminders of forthcoming appointments • Requests for patients to make an appointment for example: immunisations, routine reviews, blood test • Notifications of 'missed' appointments (DNA's) • Notifications of 'normal' test results Supports two-way secure electronic text communication between patients, carers and practices
Transactional Support Services	• Vendor via local helpdesk
Systems and applications	• Provision of electronic messaging functionality ie SMS messaging, for direct unidirectional individual patient communication, to be utilised for clinical and associated administrative purposes.
Specialist Support Services	• Support for practices (through the IG and DPO service) for the preparation of DPIAs where required for electronic messaging. This may be provided as a shared activity across multiple practices.
Practice Responsibilities (for information only)	*Where electronic messaging is used to support the processing of Special Category (Sensitive) Data or for bi-directional communications a DPIA should be completed and regularly reviewed*
Applicable Standards	• Privacy and Electronics communications Regulations (ICO). • General Data Protection Regulation (GDPR) • Data Protection Act 2018 • Accessible Information Standard – Using email and text messaging for communicating with patients - Guidance • Compliance with digital token definition for use of SMS for paper token replacement for non-nominated prescriptions

WiFi-GP

Requirement	WiFi-GP access for staff and patients in all supported Practice Premises WiFi-GP services is an overlay service which enables patients to access online services, including the internet (subject to filtration), free of charge within Practice Premises. GP staff, together with other clinicians, can access the local NHS network. There is a capability for supporting roaming.
Out of Scope	Any end user or patient chargeable services arising from the use of the service.
Transactional Support Services	Availability: Operational Service Hours • Adequate support arrangements as outlined in the NHS WiFi-GP Technical & Security Policies and Guidelines are in place.
Specialist Support Services	Availability: Standard Service Hours • Provision of usage information to CCG commissioners
Infrastructure	Appropriate WiFi-GP services for practices ensuring: • National WiFi-GP security standards are followed • WiFi-GP service usage does not impact on core Practice activities in particular performance of GP IT Futures Foundation Capabilities and NHS national systems There is compliance with NHS data security & protection requirements, including appropriate content filtering.
Systems and applications	Unsupported or unmaintained software (by software supplier), browsers, operating systems or devices must not be used to access the “corporate” WiFi-GP network in the practice. Landing page Web page
Applicable Standards	Technical Policies and Guidance

HSCN-GP

Requirement	All Practice Premises are required to have appropriately sized HSCN connectivity capable of supporting their current and future business needs. Further information on connectivity types can be found on the NHS Digital website. • All future procurements for network connectivity to existing and new Practice Premises are required to provide gigabit capable connectivity which is usually delivered either as Fibre to the Premises (FTTP) services or Ethernet leased-line services where available. Re-procurement of HSCN contracts should take place at end of term to ensure continued value for money and enable practices to take advantage of new technology
Out of Scope	Encryption and protection of patient and sensitive data at the application layer Local network infrastructure
Transactional Support Services	Availability: Operational Support Hours • Through GP IT Service Desk to 3rd party • Break / Fix incident and problem resolution
Specialist Support Services	Availability: Standard Service Hours • HSCN services for practices • NHS Digital provides a central service coordination function to monitor CNSP and network performance and coordinate response to high severity service issues.
Infrastructure	• Networking services: Management and support for provision of connectivity and transition network services, including connections to main and branch practice sites as per national entitlement. • The Peering Exchange provides the highly available points of interconnection for the HSCN CN-SPs and the Transition Network
Systems and applications	• Advanced Network Monitoring (ANM)- monitors all Internet traffic from HSCN providing an advanced malware detection and prevention capability. • Network Analytics Services-monitors network flow metadata from HSCN to provide advanced threat detection and analytics • Where possible HSCN connections should be utilised to support hosted VOIP telephony. Practice Premises would need to be served by a HSCN connection that has sufficient bandwidth and is capable of a basic level of Quality of Service to support the prioritisation of VoIP traffic. Each individual CNSP can advise on these requirements. Prior to HSCN connections being used for the VOIP telephony system the CCG (it's commissioned GP IT Delivery Partner) and HSCN provider (CN-SP) will review (i) existing data services e.g. bandwidth (ii) changes required to Practice

	Premises network infrastructure to support security and Quality of Service (QoS) for satisfactory performance of both the telephony service and the practice Foundation Clinical System (iii) with the practice any other requirements for business continuity eg a local SIP service in case of HSCN connection failure. Individual practices remain responsible for the cost of their telephony services including any additional infrastructure costs. Practices may choose, at their expense, to install and use a dedicated connection in preference to HSCN.
Applicable Standards	HSCN Obligations Framework HSCN Compliance Operating Model HSCN Compliance Release and Configuration Note HSCN Mandatory Supplemental Terms The HSCN Obligations Framework covers a set of obligations which include adherence to policies and standards for interoperability, service (e.g. service management, testing and assurance) and governance. For example, it requires CN-SPs to provide connectivity services that are interoperable with all other CN-SPs and meet a UK Government assurance standard called CAS-T (CESG Assured Service Requirement for Telecommunications), including ISO 27001.
Applicable Guidance	HSCN compliance and migration: https://digital.nhs.uk/services/health-and-social-care-network/hscn-suppliers#compliance-documents HSCN migration checklist: https://digital.nhs.uk/binaries/content/assets/legacy/excel/n/k/hscn_migration_checklist_v1.1.xlsx HSCN overlays: https://digital.nhs.uk/services/health-and-social-care-network/hscn-technical-guidance/business-applications-guidance/n3-overlays-replacement-guidance HSCN Regional Migration Manager: https://digital.nhs.uk/services/health-and-social-care-network/new-to-hscn/hscn-procurement-options Further information: enquiries@nhsdigital.nhs.uk
Other Controls	• HSCN connection agreements • CNSP Compliance documents required by NHS Digital • Consumer Network Service Providers (CN-SP)-Local contracts with commissioners such as CCGs • If shared, local arrangements with partners (e.g. support and any associated funding).
Service Availability	99.95% minimum availability (as per ISO 27001)

Local Digital Strategy

Requirement	Strong local leadership to develop and deliver a local digital strategy and digital roadmap, including GP IT. The CCGs should: • Have access to horizon scanning and advice on best practice and digital innovation • Appoint a Chief Clinical Information Officer (CCIO) or equivalent accountable officer (dedicated or shared) who will provide (clinical) leadership for the development of local digital strategy including the development of GP IT services • Develop a commissioning-led digital strategy, supporting innovation, service improvement and transformation, with GP IT as a key component. This will support the development of Local Digital Roadmaps • Ensure CCG and GP requirements are represented in any relevant local, regional or national forum
CCG Note	*Availability: Standard Service Hours* *This is a direct CCGs responsibility* *CCGs may wish to commission specialist skills and resources to assist in developing their digital strategy*

Category 4 Service Specification requirements:

CCG Note	*These are subject to local prioritisation and the CCG should determine in collaboration with their practices which capabilities are needed locally and can be funded. If the capability is to be sourced through this procurement the CCG should develop a specification using the current Operating Model for guidance and standards.* *CCGs should be aware that any enhanced clinical or business capability chosen to be provided locally must also be supported with the GP IT Enabling requirements necessary – that may require an amendment to the previous specifications, an update to Table 5.4 or an additional specification here (category 5).* *The Enhanced GP IT Requirements listed in the Operating Model will provide some areas for the CCG and its practices to consider.*

Category 5 Service Specification requirements:

CCG Note	*These are subject to local prioritisation and the CCG should determine in collaboration with their practices which capabilities are needed locally and can be funded. If the capability is to be sourced through this procurement the CCG should develop a specification using the current Operating Model for guidance and standards* *List here requirements not already covered under category 3 requirements.* *The Enhanced GP IT Requirements listed in the Operating Model will provide some areas for the CCG to consider. Examples include* • *CQRS Support* • *GP Data Quality Accreditation Service* • *Enhanced Infrastructure*

Local Context

Significant changes driven by organisational pressures and policy continue to take place in primary care services in England. The primary care response to the Covid-19 pandemic in 2020-21 has driven forward operational changes enabled by digital technologies in a dramatic and fast changing manner. Future general practice needs to be supported with the best modern digital services if successful and sustainable improvements in care are to be delivered through such changes.

The Primary Care (GP) Digital Services Operating Model, Securing Excellence in Primary Care (GP) Digital Services, 2021-23, 5th Edition, provides a commissioning framework for the delivery of GP Digital services, including consideration of productive requirements to support primary care at scale and the broader health and care service transformation, in response to changing models of care outlined in the NHS Long Term Plan.

As commissioner of GP IT services, the CCG (and any successor organisation) is keen to ensure that local GP IT service provision arrangements are responsive to and reflect local needs and requirements. The following information aims to provide insight into local services and ambitions, which will help to inform potential bidders in relation to GP IT service delivery.

Potential bidders are invited to review and respond to this ‘local context’ information in their submissions specifically in relation to delivery of GP IT services as outlined within the service specification. This should include consideration of service provision arrangements for Core and Mandated GP IT service delivery and for potential innovations/innovative ways of working that could support the development of emerging primary care delivery models. This should also support ‘at scale’ digital

solutions that support the delivery of the GP Forward View, the Five Year Framework for GP Contract Reform (2019) and the NHS Long Term Plan.

CCG Note	*Bidders will be expected to demonstrate how GP IT services will be responsive to local needs and requirements, as part of any subsequent presentation and evaluation process. This should include how efficiency and effectiveness developments in the proposed core contracted service can be used to support these changes and where the bidder can offer enhancements, innovations and additions to these services to meet these local needs.*

Table 3.1 Locality Context

Outlines the local environmental and strategic context by CCG. This includes summary notes (by each CCG if appropriate) on the following

(i) Demographics/Landscape/Geography
(ii) Delivery of Care/Service Ambitions (this will include STP and ICS plans)
(iii) Local Digital Strategy/Plans (namely Local Digital Roadmaps)
(iv) Local Governance Arrangements Supporting Digital Strategy

NOTE: if a CCG wishes to provide more detailed information this can be done as an attached document or external URL link and references in Table 6.1 Documents and Checklist.

Table 3.2 CCG Data

Summarises key data relating to GP IT for each CCG as derived from the details provided for each practice contractor and physical sites.

Table 3.3 GP IT Existing Services

General contextual information on the existing GP IT services

Performance, Activity and Quality Indicators

CCG Note: The following tables are recommended indicators and can be adapted to meet local requirements.

Table 4.1 Primary KPIs

As the service provided is likely to operate shared systems and infrastructure across a number of contracts clarification is required on whether a KPI is reported as system wide or contract specific. These are based on the minimum standards set out in the Operating Model. Additional key indicators that enable the effective monitoring and management of this contract, including KPIs that reflect broader service provision arrangements i.e. training and data quality support services can be negotiated.

Table 4.2 Secondary KPIs

Lists secondary Key Performance Indicators (KPIs) and quality indicators. These include reference to external standards where applicable. Performance against a quality standard should be set at or near 100% (or very high). As there is often not a readily available quantifiable metric to measure compliance hence assessments are likely to be based on audits or exception/non-compliance reporting.

Table 4.3 Reporting Indicators

To support the requirement for regular and ad-hoc reporting in the effective management and delivery of this service a set of core activity indicators is given

Table 4.4 Priority Assessment Matrix

The recommended basis for logged incident and request prioritisations (developed from original prioritisation matrix in The Good Practice Guidelines for GP electronic patient records v4 RCGP/BMA).

Table 4.5 Volumetrics

A set of key volumetrics to underpin consistent reporting and communications in the delivery and oversight of this service**.** This includes a tolerance limit for each volumetric within which the service should be able to operate at agreed levels and standards.

General Practices and Physical Estate

This describes the local environment which requires support. Information supplied should relate directly to GP IT arrangements only and should not include CCG corporate arrangements. The “estate” refers to the assets (equipment, licences, user accounts, premises etc.) directly used by the GP contractors within the scope of this procurement. Assets used by other parties’ e.g. community providers sharing multipurpose premises should not be included by default, unless the authority has chosen to fund IT support services for these parties through this contract as an enhanced service.

Table 5.1 Practices

The general practice estate in scope to be supported by this service. The practices are automatically selected by CCG. These should all be GMS, PMS or APMS practices with a registered patient list and who have signed the CCG - Practice Agreement. In addition there is scope (at CCG discretion) to include (i) any other APMS practice who holds a registered patient list for “primary care essential services”, have signed the CCG Practice Agreement and where no other provision for IT services has been made (e.g. within their provider contract) and (ii) if locally funded any other provider or contractor for this procurement. Relevant estate and asset volumetrics requiring support are shown (Note a tolerance range for each

volumetric is given to allow for incremental changes in estate and assets – see Table 3.5)

Table 5.2 Physical estate

All sites where GP IT services are to be delivered. NOTE: this is not the same as the list of practices as there will be multi-occupancy sites (e.g. health centres) and practice branch surgeries included. Relevant estate and asset volumetrics requiring support are shown (Note a tolerance range for each volumetric is given to allow for incremental changes in estate and assets – see Table 3.5)

GP IT Environment and Services

Table 5.3 Standard Desktop Software

This includes an indicator of the number of standard desktop ("ghost") images supported by each CCG and whether the software listed is included in the standard ("ghost") image. GP IT Futures Foundation Solutions and NHS national systems are included. Standard desktop ("ghost") images should meet the locally agreed WES. NOTE: each practice is a discrete business entity and therefore variations in software used will exist between practices, although standard desktop ("ghost") images across a GP estate are still recommended as the standard platform.

Table 5.4 Hosted Applications

Those applications used and supported as part of the GP IT service whether internally or externally hosted. Note GP IT Futures Foundation Solutions and National Digital Services are not included.

Table 5.5 Projects

Projects committed or currently in flight as part of GP IT service provision. Those projects which are part of a national mandate on the CCG or practices are flagged as such and deployment support for these should be provided as part of the requirements "National Digital Services Implementation". Support for projects generally should be provided through the requirement for "Project and Change Management"

Table 5.6 Managed Contracts

A high level summary list of relevant third party contracts relating to GP IT services e.g. COINS, Remote Access Tokens. This should indicate where responsibility for funding and for contract management sits. It is important both *the supplier* and CCGs have visibility and an understanding on responsibilities for these contracts.
GP IT Futures Foundation Solutions and National Digital Services are not included

Table 5.7 Meetings

Those scheduled meetings where attendance by *the supplier* is required. Ad-hoc and fixed term project meetings do not need to be included here as they should be resourced as part of the project management service.

Other Information

Network and infrastructure equipment eg routers, wireless access points, servers etc whether located in Practice Premises or centrally if part of the Managed GP IT Infrastructure is also documented.

Documents and Checklist

Table 6.1 Documents and Checklist

This lists all the attached tables and their purpose and references all relevant documents which are attached or accessible through URL link provided.

Appendix 2: Template Questions – for inclusion in GP IT ITT Supplier Information Pack

Suggested questions for bidders and assessment response criteria for inclusion in the Call-Off ITT Supplier Information Pack.

1.1 Division of Service provision between suppliers/sub-contractors.

Bidders are required to complete the following table indicating all suppliers involved in delivery of the services, and the services which each supplier will provide.

Suppliers must also indicate the supplier ultimately responsible for the delivery, i.e. where a sub-contractor is used the supplier responsible for the relationship with the sub-contractor.

This information must be consistent with the information provided in the Suppliers Service Matrix

Name of supplier ultimately responsible for delivery of the service.	Supplier delivering the service indicated.	Service line	Service
[Insert supplier name – MUST be a supplier who is party to the final contract).	[Insert supplier/sub-contractor name]	[Insert the service line to which the services relate]	[Insert services to be supplied by the relevant supplier/sub-contractor as per the services detailed within the specification]

1.2 Organisational capability

Provide written biographies of the proposed Directors/Senior Team and key team members responsible for managing delivery of the Services and present an overview of your organisation (biographies included as an appendix to this question will not count against the page limit for this question)

Your response will be assessed against the extent to which it demonstrates the following requirements:

- Alignment of core capability and capacity of your organisation to requirements of the ITT
- Relevant breadth and depth of experience, capability and background of the senior team to manage delivery of the services
- Clear lines of responsibility and accountability for each service and how such accountabilities will be effectively integrated at the lead provider level
- Evidence of your organisation's ability to successfully manage delivery of the services in the proposed setting
- Evidence of your approach to the delivery of the services which demonstrate that your organisational development will be informed by learning gained from delivery of services and other commissioning support services
- Identify any specific responsibilities held by the team where these responsibilities are specifically mandated in this specification eg Cyber & Data Security

Provide a copy of the organisational structure for the staff team who will be delivering the services with a summary of the service that each team would provide and their skills and capability.

Your response will be assessed against the extent to which it demonstrates the following requirements:

- Delivery team(s) with defined and relevant functions
- Delivery team(s) dedicated to named authority organisations
- A proposed staffing structure that has the depth, breadth and skills mix to effectively deliver the services
- A staffing structure which clearly identifies the qualifications required for each role, particularly where a qualification is mandated in this specification eg Clinical Safety Officer
- An effective approach to providing a united service delivery team that works as a unit to provide a coordinated commissioning support service

How will you assure the quality of your services?

Your response will be assessed against the extent to which it demonstrates the following requirements:

- A robust approach to ensuring compliance with all relevant regulatory requirements, standards and best practice (evidence should be provided that these regulatory requirements, standards and best practice are understood);
- A rigorous approach to internal governance arrangements demonstrating how the organisation will internally hold itself to account;
- An effective approach to quality management;

- An effective approach to performance management to ensure delivery against the service specifications;

How would you go about working with the Authority, its GP membership and key local health economy partners including Sustainability and Transformation Partnership Leads to identify, test, design and plan organisational innovations of the type envisaged in the GP Forward View (GPFV) and NHS Long Term Plan?

Your response will be assessed against the extent to which it demonstrates the following requirements:

- An effective approach to understand and keep abreast of the range of innovative approaches that are being tested across England and which may have relevance to the local health economy;
- An effective approach to engaging with the authority and its GP members to test options and to formulate a vision for the future;
- A robust approach to assist the authority in planning and implementing the organisational development activities needed to realise any agreed vision.

1.3 Customer service / responsiveness

Outline your service delivery model, including your approach to flexing resource to support the anticipated fluctuations in GP IT demand.

Your response will be assessed against the extent to which it demonstrates the following requirements:

- A flexible approach to service delivery that ensures that you can supply the necessary capability, skills and capacity to meet demand throughout the general practice year;
- A flexible approach to managing fluctuations in GP IT workloads and delivering priorities within customer financial envelopes;
- How fluctuations in demand for GP IT arising from digital system upgrades, deployments, and GP IT estate changes are supported;
- Strong leadership and account management, especially during the mobilisation stage of the services;
- A united service delivery team that works as a unit to provide a coordinated GP IT service.

Outline your approach to delivering the service in partnership with the CCGs.

Your response will be assessed against the extent to which it demonstrates the following requirements:

- An effective approach to supporting the CCGs to meet their priorities and objective by aligning your service delivery priorities to those of the CCGs and their GP membership;

- An effective approach to delivering a service in line with the behaviours described in the “Authority Requirements” section of this Supplier Information Pack;
- An approach to ensuring good practice is shared between the members of the authority;
- How the CCG will be supported in the management of GP communities and representative local bodies e.g. LMCs.

How will you maintain and enhance customer-focused service delivery and what contribution will effective contract management make to this?

Your response will be assessed against the extent to which it demonstrates the following requirements:

- A robust approach to ensure that your services achieve each procuring authority’s service requirements, whether supplied directly by you or by your sub-contractors;
- An effective approach to achieve the performance standards required by the procuring authorities, in particular describing how you will address any performance issues arising, whether from services supplied directly by you or by your sub-contractors;

Describe your approach to measuring and monitoring customer (i.e. CCGs and GPs) satisfaction and the steps you take where satisfaction of customers is poor.

Your response will be assessed against the extent to which it demonstrates the following requirements:

- An open and transparent approach to gathering and presenting feedback which ensures customer views are correctly represented and issues with service delivery are appropriately highlighted;
- An approach to monitoring trends in service satisfaction and performance issues and pro-actively understanding, monitoring and/or remedying customer feedback, issues and concerns;
- A robust approach to ensuring ownership and single point of contact to handling complaints within and across services;
- An effective account management approach to customer satisfaction;
- You should evidence your response with reference to a relevant case study for a customer in a similar context.
-

1.4 Mobilisation

Provide an implementation plan outlining how services will be mobilised.
Your plan needs to demonstrate how you will maintain business as usual services to ensure CCG and GP patient services are not adversely affected by mobilisation and are able to deliver their statutory and contractual responsibilities.

Your response will be assessed against the extent to which it demonstrates the following requirements:

- A credible and realistic mobilisation plan which ensures minimal disruption to the authority and GP member practices (supported, as an appendix to your response to this question, by a Gantt Chart and associated timetable, which will not be included in the page limit for this question);
- Effective plans for staff engagement and customer (authority and GP) communications during mobilisation;
- An effective approach to engaging with other key stakeholders (supported by, as an optional appendix to your response to this question, a high level stakeholder engagement plan, which will not be evaluated and will not be included in the page limit for this question but can be referenced in your response) demonstrating how you intend to communicate with key stakeholders and service users;
- A robust approach to governance, quality assurance and risk management during the mobilisation period;
- A robust approach to Information Governance during the mobilisation.

1.5 GP IT - Service delivery

What do you consider to be the 3 to 5 main challenges in delivering safe and innovative GP IT solutions that are compliant with the latest NHS England Primary Care (GP) Digital Services Operating Model, yet at the same time support the development of Integrated Care Systems (ICS) ?

Your response will be assessed against the extent to which it demonstrates the following requirements:

- A robust approach to delivering GP IT service which conforms to the Core and Mandated GP IT Requirements in the latest NHS England Operating Model.
- A comprehensive understanding of the challenges in delivering safe and innovative GP IT services which should include reference to the NDG 10 Data Security Standards;
- Demonstration of an approach on how the Authority will be supported to optimise the opportunities in the Operating Model to assist in developing Integrated Care Systems (ICS) locally ?
- A comprehensive understanding of the benefits associated with agile working arrangement across primary care whilst ensuring that compliant information governance and cyber security is maintained;

How will your IT solution serve as an enabler for strategic primary care service improvement, within the context of the NHS long Term Plan and the development of Integrated Care Services, over the next 3 to 5 years?

Your response will be assessed against the extent to which it demonstrates the following requirements:

- A demonstrable understanding of national primary care service improvement initiatives such the Primary care Networks (PCN) Enhanced Service and the Integrated Care Systems (ICS) programme. Showing an effective approach to deploying innovation and improvement in support of these;
- A clear articulation of the tangible service improvements that would be delivered, when these would be realised and what additional technologies and services would be required to deliver these;
- A robust approach to measuring outcome-based success;
- Demonstrate awareness and consideration of the impact on GP services and IT services of the new models of care such as ICS.
- How the “Digital First” agenda would be supported

What do you consider to be the greatest challenges in delivering safe and innovative GP IT solutions that are compliant with the latest information governance and cyber-security requirements and how would you address these challenges? What specific IG & Cyber Security considerations will there need to be within the context of new models of care?

Your response will be assessed against the extent to which it demonstrates the following requirements:

- A comprehensive understanding of the challenges to delivering safe and innovative GP IT solutions that are compliant with the latest information governance and cyber-security requirements;
- Understanding the context of the general practice contractor environment and local provider organisations in relation to the respective of data controller roles and the integration of local services;
- An effective approach to addressing the challenges described above;
- A robust approach to ensuring safe and secure access to sensitive information such as patient records in remote, mobile and flexible working environments.

Outline your approach to driving service improvements and efficiencies while delivering the contracted services.

Your response will be assessed against the extent to which it demonstrates the following requirements:

- An effective approach to driving improvements in services provided across the CCG’s and the GP estate**;**
- A realistic and targeted approach to delivering efficiencies;

- You should evidence, as part of your response, the improvements and efficiencies you will make during each year of the service contract as outlined in your Price Submission;
- An effective approach to managing expectations in the event you are not able to deliver the full extent of GP requirements.

What IT enabled GP service improvements would you be expecting from your service that would directly benefit individual general practices?

Your response will be assessed against the extent to which it demonstrates the following requirements:

- A clear description of the IT enabled service improvements a practice would expect from the supplier's service delivery and an effective approach to realising these improvements.

How would your service delivery support the NHS Net Zero ambitions ?

Your response will be assessed against the extent to which it demonstrates the following requirements:

- How the service delivery and IT infrastructure investment and deployment will support the NHS Net Zero ambitions.

Appendix 3: Suggested Exploratory Topics for Bidder Presentations

1. Bidder to explain how they would support the CCG and its general practices in significant primary care estate development which includes:
   a. New integrated health centre build hosting five general practices (merging into three) and community teams from other healthcare providers (community trust and a mental health trust)
   b. The merger of three of these practices into one (i.e. reducing from five to three) where the three existing practices use a different clinical system from different suppliers, but have all agreed to move to a single practice instance of one hosted clinical system.
   c. Provision of new infrastructure in the building including HSCN, and WiFi

2. Bidder to explain how they would support the CCG and its general practices meet the challenges stated in the Operating Model ie

- **Keeping general practice safe**
- **Supporting general practice deliver their contracted services**
- **Enabling service improvement, transformation and digital innovations**
- **Supporting new models of care and contracts**
- **Supporting general practice meet patient's digital expectations**

Note although the bidder would not be required to provide all the services needed to meet the above challenges they will be required to support these services and work within an environment faced with these challenges.

Appendix 5: Suggested Points of Consideration in Bidder Interviews

1. How would the bidder approach resourcing the service for
   a. transactional services e.g. helpdesk, Registration Authority
   b. non-transactional services e.g. training, project management, Information Governance

2. Does the bidder understand the customer base in particular the relationship between GP contractors and the NHS ?

3. Does the bidder understand the Operating Model in particular the delegated responsibilities of the CCG for GP IT ?

4. What experience has the bidder in NHS IT and specifically in GP IT delivery ?

5. To what extent does the bidder understand the current NHS and the NHS Long Term Plan ?

6. How would the bidder approach managing the GP IT equipment estate in terms of refresh, disposal, using different technologies to extend operational life ?

7. How will the bidder ensure IT enablers for service integration in the local health community and the development of Integrated Care Systems are available ?

8. How will legacy contracts be handled ?

9. Are specialist services such as Clinical Safety, Information Governance, IT Security, Data Quality supported by access to necessary skilled resources ?

10. Can the bidder support the CCG with digital strategy and enablement of wider system transformation ?

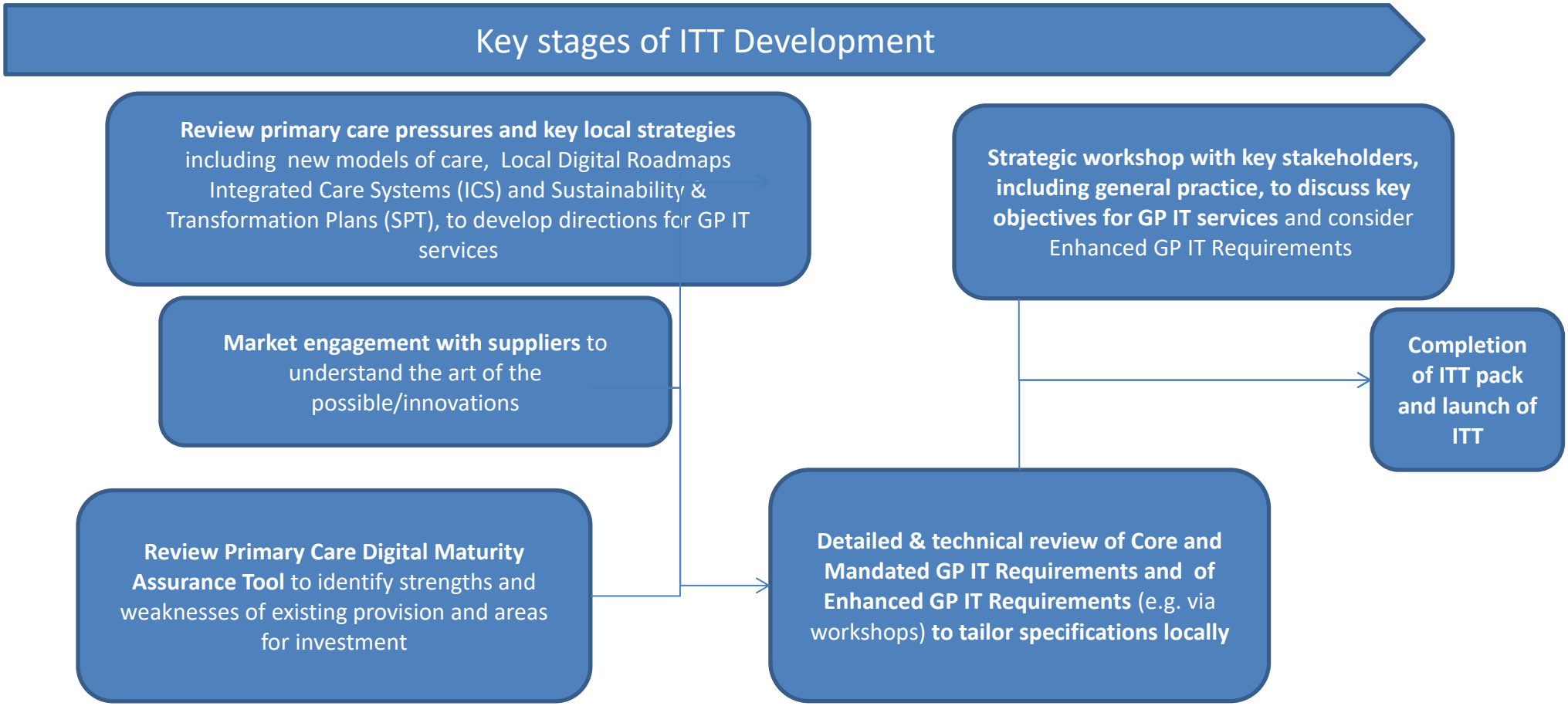
11. Will the bidder provide any data hosting services – if yes describe the arrangements including security, resilience, business continuity, could hosting, hosting outside England ?

12. Is the bidder aware of the National Data Guardian 10 data security standards(https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs) and the EU General Data Protection Regulation (GDPR), their implications for GPs and their responsibility as a supplier (including potentially as a “data processor”)

Appendix 6: Glossary of Terms

Term	Description
APMS	Alternative Provider Medical Services
BCP	Business Continuity Plan
CCG	Clinical Commissioning Group
CE +	Cyber Essentials Plus
COIN	Community Of Interest Network
CQRS	Calculating Quality Reporting Service
CRM	Customer Relationship management
CTV3	Clinical Terms Version 3
DES	Directed Enhanced Service
DPO	Data Protection Officer
DR	Disaster Recovery
DSPT	Data Security and Protection Toolkit
EPRR	Emergency Preparedness, Resilience and Response
ETTF	Estates and Technology Transformation Funds
GDPR	General Data Protection Regulation
GMS	General Medical Services
GP IT Futures Framework	The GP IT Futures Digital Care Services Framework Contract
ICO	Information Commissioner's Office
ICS	Integrated Care System
ISMS	Information Security Management System
LDR	Local Digital Roadmap
MHRA	Medicines and Healthcare products Regulatory Agency
National Commercial & Procurement Hub	National Commercial & Procurement Hub
NDG	National Data Guardian
ODS	Organisational Data Services
PC DMAT	Digital Primary Care Maturity Assurance Tool
PCN	Primary Care Network
PMS	Personal Medical Services
RTO	Recovery Time Objective
SFI	Standing Financial Instructions
SMS	Short Message Service
STP	Sustainability & Transformation Plan

Appendix 7 – Key stages of ITT Development



During this stage you should collect data to support the procurement including:

- Requesting and reviewing staff and asset information from incumbent supplier
- Gathering information on the volume of services currently provided e.g. number of GP practices supported
- Collate a pack of key documents for suppliers including practice agreements, the CCG's IT strategy, digital roadmap etc.