Securing Excellence in Primary Care (GP) Digital Services

The Primary Care (GP) Digital Services Operating Model

2021-2023 V5

Securing Excellence in Primary Care (GP) Digital Services

The Primary Care GP Digital Services Operating Model 2021-23

Publishing approval number: PAR399

Version number: 5

First published: 2012

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

Equality Statement

Promoting equality and addressing health inequalities are at the heart of NHS England's values. Throughout the development of the policies and processes cited in this document, we have:

- Given due regard to the need to eliminate discrimination, harassment and victimisation, to advance equality of opportunity, and to foster good relations between people who share a relevant protected characteristic (as cited under the Equality Act 2010) and those who do not share it; and
- Given regard to the need to reduce inequalities between patients in access to, and outcomes from healthcare services and to ensure services are provided in an integrated way where this might reduce health inequalities

Contents

Foreword

Response, resilience and sustainability

General practice is the heart of the NHS, and the NHS relies on it to survive and thrive.

The pandemic has presented the NHS with its greatest challenge since it was established in 1948. Despite already coping with growing demand General Practice rose to the challenge of continuing to work during unprecedented and extremely difficult times. Rapid and widescale changes to traditional ways of working have been implemented in order to provide safe and accessible care to patients, with primary care teams embracing digital tools such as remote working, online triage, online, video and telephone consultations.

The importance of strong clinical and digital leadership to enable digital transformation has been robustly demonstrated, supporting and promoting the accelerated and widespread adoption of digital tools by General Practice. These have enabled more efficient, flexible and resilient ways of working. This has helped practices to meet growing demand from patients by providing choice of digital channels, supporting transformation and innovation for modern general practice.

The publication of this 5th Operating Model for General Practice Digital Services comes at an extremely pertinent time, building on and sustaining the achievements and lessons learned during the pandemic and providing the framework to maintain the momentum of change.

Recent events have shown that for general practice, business continuity and resilience is the ability to respond to major events and new priorities, while also ensuring sufficient flexibility to rapidly reconfigure and realign as needed to maintain business as usual activity. Providing the capability for such resilience and flexibility whilst continuing to ensure the safety of General Practice is a key theme of this Operating Model. There is understandably high public expectation of patient safety and data security in our electronic patient record systems.

Although still a core practice responsibility the critical importance of modern advanced telephony systems in general practice is recognised and we have taken a number of steps to support and guide practices in this area.

We are starting to see the impacts of Primary Care Networks (PCNs) and recognise that ensuring the availability of the right technologies and support are essential to their success.

As integrated care system (ICS) organisations are established, digital tools and electronic communications enabled by readily accessible shared infrastructure across local health systems are critical. The next iteration of this Operating Model will require significant change to align with integrated care boards (ICBs).

In addition 2020 saw a major commitment to deliver a net zero NHS by 2040. In general practice, digital systems and tools that reduce staff and patient travel and continue to progress towards a paper free environment for patient records are important enablers to reduce our carbon footprint.

Of course the technologies are only enablers and although we clearly need digital tools, infrastructure and support fit for use, it is our staff and our patients who need the access, confidence and skills to use them to the full to realise the benefits.

This Operating Model continues to recognise the challenges faced in general practice and the need for Clinical Commissioning Groups (CCGs) to continue to ensure investment is directed appropriately. It remains critical that commissioners responsible for the provision of GP IT services are fully aware of and enact the requirements of the Operating Model. It is vital that digital service delivery, transformation and innovation continues to be at the forefront in supporting new models of care

We are grateful for the support of NHS colleagues, CCGs, General Practice, BMA, RCGP and GP IT Delivery Partners that have contributed to the development of this framework.

Lloyd Baker
Programme Director
Digital Primary Care
NHS Transformation Directorate

1 Executive Summary

The NHS provides general practices with digital services as required by the GP Contract and the CCG-Practice Agreement. Details of how these digital services should be provided, the standards they should meet and how they are funded are published in this document, also known as the “GP IT Operating Model”.

CCGs have devolved responsibility to provide these services to their practices and this document provides a regularly updated commissioning framework to assist CCGs in this. CCGs and their commissioned GP IT Delivery Partners should make full use of this guidance to ensure their practices are fully supported with world class digital services. By necessity this is a comprehensive and consequently lengthy document. Practices will find the general practice quick reference section helpful in using this document.

The six challenges identified in the previous version of this document remain equally relevant today. One of these challenges is keeping practices and their patients safe and elements addressing cyber security, information governance and patient safety have been reviewed and updated.

Following the general practice response to the Covid-19 pandemic a number of significant additions have been included:

- Remote access as a means of enhancing practice efficiency and resilience will be available to support at least 60% of normal practice operational capacity. CCGs and practices must review and ensure only robust and cyber safe methods of remote access are used.
- Online and video consultations will continue to be encouraged and are now supported as a mandated digital service.
- GP telephony systems remain the responsibility of the individual practice but additions have been made to encourage and assist practices move away from legacy telephone systems to advanced cloud based VoIP systems. This includes a GP Advanced Telephony Specification Commissioning Support Pack.
- The importance of resilience and business continuity for practices and also for the commissioned GP IT Delivery Partners. CCGs should review practice Business Continuity Plans in the context of the experiences of the pandemic response, including how digital technologies can better support practice resilience.

These changes will also support pressures on general practice already recognised before the pandemic arising from growing patient demand and workforce challenges.

Funding sources and allocations have changed in particular to support digital transformation in general practice. Full details are provided in Primary care SDF and GP IT funding guidance 2021/22. PCN staff IT needs are now aligned and included with the GP IT revenue and capital allocations.

Not all digital services are centrally commissioned. CCGs, ICS, PCNs and individual practices can now make use of a number of assets included in the appendices ie lists of relevant purchasing frameworks, a procurement checklist and a commissioning support

pack (with template specifications) for GP IT enabling services and for advanced GP telephony services.

The Digital Primary Care Maturity Assurance Model will continue to develop and underpin the tracking of local and national progress in meeting the mandated requirements in this Operating Model and other enhanced and transformational digital improvements.

In the evolving landscape of local healthcare delivery general practices are developing innovative and different ways of structuring and delivering services. This document provides guidance on supporting sub-contracted practice services, and supporting practice organisations working across multiple CCGs.

As the ICS become established this document will continue to support general practice but will be revised as necessary to align to new and evolving arrangements. It is expected that the revisions will be significant for the next iteration.

2 Introduction

This document sets out the revised Operating Model for the provision of high-quality general practice digital services, building upon 'Securing Excellence in GP IT Services', first published in December 2012 and subsequent editions published in 2014, 2016 and 2019.

2.1 Purpose – what does this document do?

The Operating Model is a **commissioning framework** supporting the provision of digital services required for general practices and PCNs:

- defining the digital requirements for general practice as clinical and business capabilities and the necessary IT enablers
- attributing standards (and guidance) to these requirements to ensure quality, safety and compatibility
- assigning responsibilities for the commissioning, provision and utilisation of these requirements

This document provides a description of the specific arrangements that NHS England will put in place for GP digital services to:

- explain how the NHS will fulfil its obligations regarding GP digital services and support under the CCG-Practice Agreement
- inform general practice of what to expect in the provision of GP digital services, and what is expected of general practices in receiving those services
- explain how the NHS will ensure key strategic digital programmes and digital mandates across the health and care system are reflected and supported in general practice
- ensure digital technologies are available to enable service improvement, transformation of care arrangements and patient digital engagement with primary care
- define the responsibilities of all principal stakeholders in the delivery and utilisation of digital services for general practice
- set a requirement for regular review to ensure this Operating Model addresses the needs of a changing commissioning and provisioning healthcare environment
- provide assurance that quality and value are being maintained and delivered consistently across primary care services within the NHS
- ensure digital enablers are available and used to support the NHS commitment to net zero carbon emissions

This document sets out the following key elements that will be necessary to support the effective delivery of GP digital services:

- the operating arrangements including financial procedures and associated controls
- the governance arrangements, including stakeholder roles and responsibilities

- the leadership necessary, in commissioning, operational delivery and clinical engagement, to achieve excellence

2.2 Definitions

The following definitions are used in this document

Term	Definition
Additional GP Contract Digital Capabilities	Additional digital systems, technologies and services needed to deliver elements of a GP Contract in addition to providing Essential Services, e.g. an APMS contractor providing walk in services, minor injuries, GP out of hours etc. These are Enhanced Requirements
Clinical System	The digital application used by the practice to store and manage its electronic patient records provided through GP IT Futures Foundation Solution AND any additional integrated or interfaced applications
Commercial and Procurement Hub	The NHS England and NHS Improvement-funded 'Commercial and Procurement Hub' supports primary care customers with all aspects of procurement, including buying via the Digital Care Services (DCS) Catalogue and the purchase of solutions and service for the Health Systems Support Framework.
Core and Mandated 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.
Digital Care Services Catalogue	The Digital Care Services Catalogue Agreement which includes GP IT Futures Framework and the DFOCVC Framework
DFOCVC Framework	The Digital First Online Consultation and Video Consultation Framework Contract accessible within the Digital Care Services Catalogue.
Enhanced Access	Enhanced Access services offered by PCNs from October 2022
Enhanced 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 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 and Regulations
Foundation Capabilities	The six capabilities defined under GP IT Futures Framework which must be fulfilled to provide a Foundation Solution for general practice.
Foundation Solution	A solution (or group of solutions) which maps to the GP IT Futures Framework foundation capability set
Foundation Solution Supplier	Any supplier who provides the Foundation Solutions
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 Delivery Partner	GP IT Delivery Partners are organisations commissioned by CCGs to deliver IT services for GP Practices as required under this Operating Model. Where CCGs provide these services directly, they take on the same responsibilities as the commissioned GP IT Delivery Partners.
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 Futures Framework	The GP IT Futures Framework Agreement accessible within the Digital Care Services Catalogue. Provides accredited clinical systems for primary care including Foundation Solutions.
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 as severity level 1 or 2 using NHS Digital Severity Level Guidelines. This highlights the NHS Digital approach to severity level guidance. Local interpretation or clarification may be needed.
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 GP IT Operating Model (see above)
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 GP 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 and social care professionals individually commissioned directly by the practice.
Public Authorities	NHS organisations (and general practices) which provide public services as defined under relevant legislation including the Freedom Of Information Act 2000 and the Data Protection Act 2018

The NHS England and NHS Improvement-funded 'Commercial and Procurement Hub' is available to support primary care customers with all aspects of procurement, including buying via the Digital Care Services (DCS) Catalogue.

2.3 About the Operating Model

Since the publication of the first GP IT Operating Model in 2012 the document has been welcomed as a definitive reference point for direction on the digital services to be provided to general practices and the responsibilities of the parties involved.

In updating the Operating Model NHS England has with the positive support of general practice and their professional bodies considered the following:

- the former GP Systems of Choice (GPSoC) framework, the previous GP IT Operating Models and earlier guidance have, with strong clinical engagement and a progressive inclusion of digital services in the GP Contract been successful in realising a highly digitised general practice estate with a large percentage of paper free processes. We must continue to build on this success.
- the key role of digital technology to underpin general practice resilience and business continuity
- general practice continues to lead the NHS in the adoption of patient facing digital systems

NHS England recognises a number of significant drivers and trends:

- the introduction of new models of care and contracts
- the requirement to protect general practice including cyber security, data security and digital clinical safety
- the immense pressures on general practice from patient demand, workforce capacity, service transformation, financial constraints and public expectations.
- the need to support general practice working at scale including PCNs, multi-site practices, and super-partnerships
- introduction of fresh digital solutions and innovation – including Digital Care Services (DCS) Catalogue
- delivering on the digital commitments made in the NHS Long Term plan and the GP Contract (2019)
- lessons learned from the 2020-21 Covid-19 Response and the 2021 vaccination programme
- the NHS commitment to net zero emissions
- the development and evolution of Integrated care Systems (ICS)

The NHS and its supporting care systems and providers continue to change and evolve. This Operating Model is based on the knowledge and understanding at the time of publication and covers the period April 2021 to March 2023.

It mandates a number of digital requirements which must be provided by the NHS to meet its obligations under the CCG-Practice Agreement and to support the GP Contract. CCGs as local commissioners should not view this as defining the limits of local investment in digital services for general practice, but as the minimum set of essential digital services to be provided to practices.

Additional requirements described in this Operating Model as enhanced digital requirements may be the enablers to those service changes which deliver significant benefits. CCGs therefore need to work with local general practices to invest effectively in digital technologies which will enable and underpin service improvement and transformation.

General practices need to utilise and embrace these digital tools making the necessary service changes to realise the benefits they can deliver.

Changes made in this revision include:

- continued emphasis on ensuring the security and safety of digital services in general practice
- an enhanced emphasis on improving practice resilience and business continuity through digital enablers
- the covid-19 pandemic response and vaccination programme lessons learned and their impact on this Operating Model
- updated funding guidance including new sources of funding and guidance on direct practice funding
- updated commissioning of GP IT services guidance to assist management of digital first provider organisations operating across multiple CCGs
- aligning GP IT to support NHS Net Zero Carbon commitments
- a new appendix listing the applicable framework contracts, including GP IT Futures, which support this Operating Model
- guidance and a template specification to support practices procuring Advanced Telephony Solutions although GP telephony remains a practice responsibility.
- Registration Authority and Desktop Infrastructure requirements updated to be ready to support new approved authentication approaches
- the following become Core and Mandated Requirements:
    - Remote Access – revised and updated
    - Online and Video Consultation
- the following are no longer Core and Mandated Requirements:
    - clinical servers for local hosting
    - compliance with and reference to EU Falsified Medicines Directive (FMD) have been removed as this was not part of the EU withdrawal agreement

The scope of the Operating Model continues to reflect the ambition stated in the preceding version for a single Digital Primary Care Operating Model aligned to primary care commissioning and providing a framework which ensures digital technology fully supports and enables new models of care.

2.4 Organisational Scope

The obligation on the NHS to provide GP contractors with accredited electronic patient record systems and the infrastructure and services necessary to support and enable these systems locally remains the underpinning rationale for this Operating Model. This in turn defines the organisational scope for the Operating Model as follows:

2.4.1 Organisations in scope:

- General Practices and providers contracted under the GP Contract (this includes GMS contracts, PMS agreements and APMS contracts) to provide Essential Services and where a CCG-Practice Agreement is in place
- PCN services provided by the above General Practices under the new Network Contract Direct Enhanced Service (DES)

Note: see section on sub-contracting of services

2.4.2 Stakeholders:

- primary stakeholder organisations including CCGs, General Practices, NHS England and NHS Improvement and NHS Digital
- secondary stakeholder organisations including commissioned GP IT delivery providers, accredited suppliers under DCS Catalogue frameworks and the Health and Social Care Framework (HSSF), GPC England, LMCs and others representing and supporting general practice nationally and locally

2.4.3 Organisations out of scope:

- other primary care contractors
- providers contracted through the NHS Standard Contract
- direct support to GP Federations and similar collaborative organisational forms, setup as separate organisational entities to provide services to general practice contractors and/or to secure and deliver non-GMS services e.g. through a standard NHS provider contract
- General Practices contracted under the GP Contract (this includes GMS contracts, PMS agreements and APMS contracts) where a CCG-Practice Agreement is NOT in place

Note any of the above organisations however may find this Operating Model useful as a reference to service requirements and standards.

2.4.4 Services out of scope:

- services outside the GP Contract provided by practices for example occupational health services
- Dispensing practices (approximately 1,000) operating under NHSEI Standard Contract arrangements for pharmaceutical dispensing regulations require software and digital infrastructure to operate the dispensing function. These services are outside the scope for the receipt of GP IT digital services under this Operating Model.

2.5 Covid-19 Pandemic Response Lessons Learned

Just as the previous Operating Model incorporated lessons learned from the Wannacry global cyber incident in 2017, this Operating Model takes account of the significant, positive and negative, lessons learned from the Covid-19 response and vaccination programme during 2020-21. These are described later in this document.

2.6 Key Challenges

This revised Operating Model seeks to address the following contemporary challenges for a digitally enabled general practice:

- **keep general practice and patients safe:**
  - a strong emphasis on security and safety of digital technologies used in general practice
- **support general practice deliver their contracted services:**
  - IT infrastructure provided to a standard which allows the practice to efficiently and effectively use the capabilities identified in this Operating Model
  - supporting practice resilience and business continuity with digital enablers
- **enable service improvement, transformation and digital innovations:**
  - support for GPs and CCGs to prioritise and invest in technologies which improve practice efficiency and service transformation
  - supporting the commitment to deliver a Net Zero NHS
- **support new models of care and contracts:**
  - support for the PCN Direct Enhanced Service (DES) and ICS
- **support general practice meet patient's digital expectations:**
  - requirements to support GP Contract commitments on patient facing digital services
- **build on success and learn lessons:**
  - recognising and building on success of GP Systems development, former GPSoC Framework and previous Operating Models
  - learning lessons from national crisis events Wannacry (2017) and Covid-19 (2020-21)

How the Operating Model addresses each of these challenges is described under section 8 in this document.

2.7 Good Practice Guidelines

The "Good Practice Guidelines for GP electronic patient records" (last published as version 4 2011) is under revision, with an online resource format expected to replace a

single published document. Once published this will supersede the 2011 Version 4 document in this Operating Model.

3 The CCG-Practice Agreement

A CCG-Practice Agreement was published in 2019. All CCGs are required to sign this agreement with each general practice (holders of a General Medical Services (GMS) contract, Personal Medical Services (PMS) agreement or Alternative Provider Medical Services (APMS) contract) offering Essential Services.

This Agreement provides clarity and assurance on the requirements for the provision and use of digital services available to general practices under this Operating Model as shown in Figure1 below. CCGs (or any successor organisation) must therefore ensure a signed CCG-Practice Agreement is in place before providing these services to a practice.

3.1 The Agreement

- Confirms that the CCG can provide funded GP digital services to defined standards under this Operating Model to the general practice. This will provide a single reference point identifying practices receiving GP digital services.
- References the Operating Model as defining the scope of digital requirements to be provided and standards applicable to those requirements
- Describes how accreditation required under the GP Contract will be assured for the solutions procured
- Defines categories for service availability
- Requires the practice as the “end user” organisation to comply with any terms and conditions of use for NHS commissioned systems made available to the practice
- Defines processes for the management of change requests, escalations and disputes relating to the delivery of services under the Agreement

3.2 The Agreement Schedules

Four schedules as appendices are included in the Agreement:

- appendix 1 – Summary of services (for individual practice)
- appendix 2 – Support and maintenance service levels (local content)
- appendix 3 – Escalation procedure (local content)
- appendix 4 – Business justification form (standard template)

These schedules should be reviewed

- not less than every 12 months
- when there is a change to the content of any schedule
- on request for review by either party

New schedules or schedule changes should be agreed with both parties through a local Agreement Addendum.

3.3 Organisational Changes

The CCG-Practice Agreement will by variations (clauses 13.4, 13.5) continue to apply in the event of the merger of practices or CCGs.

The obligation, to support practices under the CCG-Practice Agreement and as detailed in this Operating Model includes supporting the impact on GP digital services arising from local General Practice contractor changes for example practice mergers and closures.

At the point CCG successor organisations are established the agreement will transition under the relevant transfer scheme. No further action in respect of this agreement will be required.

3.4 Data Processing Agreement Requirements

As controller each practice is responsible for securing assurance on the General Data Protection Regulation (GDPR) compliance of both any contract for third party system or service which processes patient data and of the activities of the third party as processor.

NHS Digital or the CCG may undertake this assurance on behalf of general practices (for example via a framework or other NHS procurement) with the practice remaining ultimately accountable as controller.

Digital services commissioned by the NHS nationally, including those available through frameworks (for example DFOCVC Framework) made available under the Digital Care Services (DCS) Catalogue, have agreed data processing agreements and measures in place to which all parties must comply.

The CCG-Practice Agreement references, in addition to each party's obligations under current data protection legislation, the Data Processing Deed which governs data processing activities under the GP IT Futures Framework.

Where such Agreements/Deeds are available CCGs should include a reference (and link) to the relevant data processing agreement(s) in Appendix 1 – Summary of Services Table within the CCG-Practice Agreement.

Where the practice directly puts in place arrangements with a third party which include the processing of patient data for example a PCN service provider, a GP Federation as separate legal organisation entity, an NHS Trust, a digital service (software or hosting) provider, or physical record handling organisation (for example scanning or archiving services) this falls outside the scope of the CCG-Practice Agreement. The individual practice must take necessary steps, including documentation, to ensure the digital service commissioned meets robust standards relating to information governance, including the supplier's compliance with current data protection legislation.

3.5 Accountability and Responsibilities

The CCG-Practice Agreement describes the respective practice and CCG responsibilities for the provision and receipt of GP digital services. Detailed accountability and responsibilities for all parties involved in the Operating Model are given in Appendix B.

3.6 Review

Following publication of this Operating Model a review of the CCG-Practice Agreement will commence to consider the impact of new developments include the establishment of ICS and the establishment of new frameworks for general practice digital services involving data processing activities.

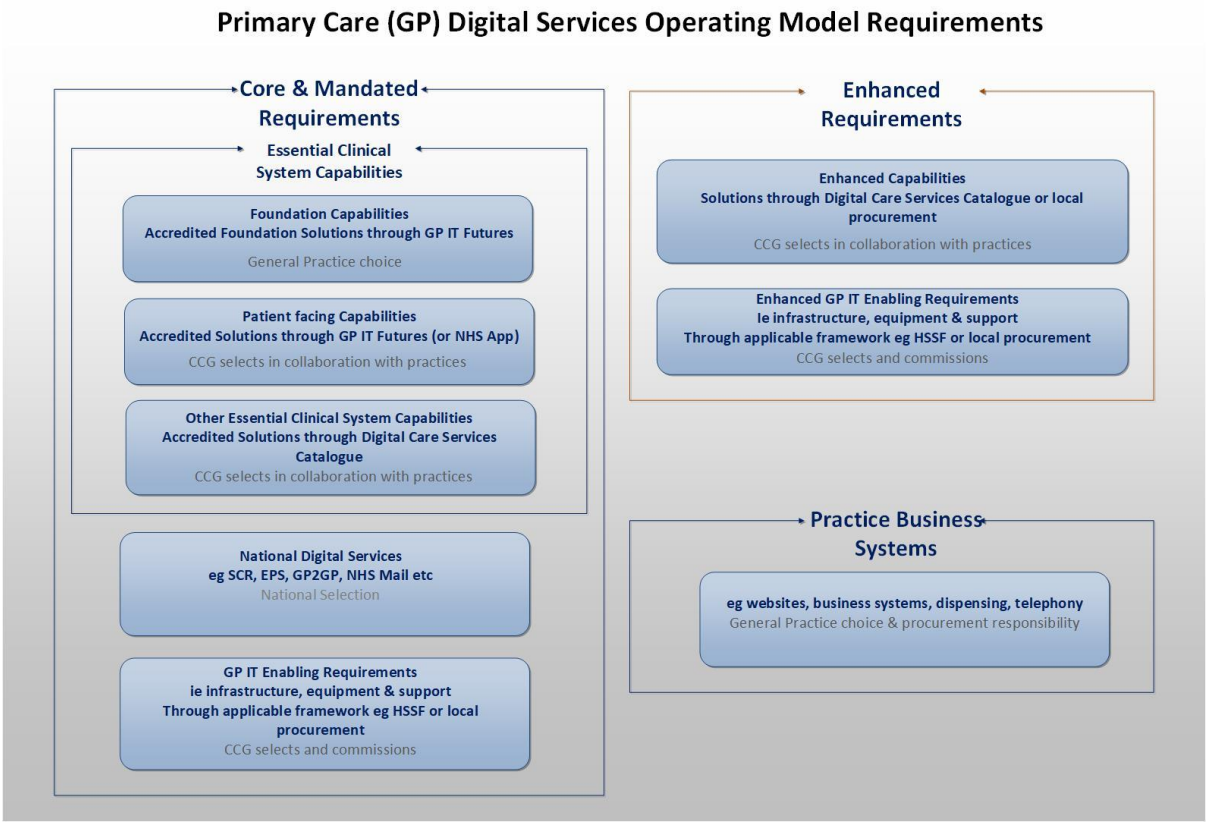
4. Requirements and Capabilities

Digital capabilities necessary to enable the practice to fulfil its obligations under the GP Contract are described here. Digital solutions will be provided to meet these requirements which in turn will be supported by a GP IT Enabling Requirements for example infrastructure, equipment, service desk, training. GP IT Enabling Requirements are therefore scoped by those digital solutions (for example Clinical Systems) provided under this Operating Model. All requirements are described in Appendix A.

Where published standards are appropriate and available these are assigned to the requirement and should be met when the service is commissioned.
Responsibilities for fulfilling these requirements (for example commissioning, delivery, assurance, usage) are described in Appendix B.

When commissioning services locally the GP IT Enabling Requirement described may need further development and clarification as part of the local procurement service specification. A GP IT specification commissioning support pack as described in Appendix E is provided to assist CCGs in this task.

Figure 1: Requirements and capabilities under this Operating Model.



Note: CCG collaboration with practices will include CCGs consulting with Local Medical Committees (LMCs) representing local practices
See Appendix A for detailed requirements.

4.1 Core and Mandated Requirements

The digital solutions and IT enablers required for the delivery of Essential Services under the GP Contract or as otherwise nationally required are Core and Mandated Requirements. Through the CCG-Practice Agreement these are funded by NHS England for GP contractors.

4.1.1 Essential Clinical System Capabilities – patient management and clinical capabilities which can be enabled through software application and data solutions. These solutions must be accredited through the GP IT Futures Framework.

4.1.1.1 Foundation Solutions – To meet the six Foundation Capabilities practices will choose the best fit Foundation Solution(s) from those available in the catalogue.

4.1.1.2 Non-Foundation Solutions – To meet the other Essential Clinical System Capabilities commissioning CCGs will collaborate with local general practices to choose the best solutions from those available in the catalogue. LMCs should be consulted as appropriate.

4.1.2 National Digital Services – digital services commissioned centrally by NHS and provided to, and used by, all NHS commissioned providers as applicable. There is no local choice in these solutions. Local alternatives must not be commissioned.

4.1.3 GP IT Enabling Requirements – namely infrastructure, equipment and support services as required by the solutions selected to meet the Essential Clinical System Capabilities and the National Digital Services.

4.2 Enhanced Requirements

Requirements for digital solutions and IT enablers which are not core and mandated (see above) but which enable service improvement and transformation. Provision of services to meet these requirements through commissioner funding is secondary to meeting Core and Mandated Requirements and is subject to local prioritisation.

4.2.1 Productive digital capabilities – patient management and clinical capabilities which improve the efficiency and effectiveness of the contracted service and can be enabled through software application and data solutions. Accredited solutions to meet these capabilities will be available through the Digital Care Services (DCS) Catalogue .

4.2.2 Transformational digital capabilities – patient management and clinical capabilities which enable transformed care, often extending beyond the practice, which can be enabled through software application and data solutions. Accredited solutions to meet these capabilities will be available through the Digital Care Services Catalogue and through Health Systems Support Framework (HSSF).

4.2.3 Additional GP Contract digital capabilities – Additional digital systems, technologies and services needed to deliver those elements of a GP Contract additional to providing Essential Services, for example an APMS contractor providing walk in services, minor injuries etc.

4.2.4 GP IT Enabling Requirements – any extension of the core GP IT Enabling Requirements (4.1.4) necessary to support and enable the enhanced capabilities above (4.2.1, 4.2.2, 4.2.3).

In providing services to meet these Enhanced Requirements CCGs should have regard to the following points:

- CCGs have an obligation to ensure requirements already met through NHS funded services or funded through other routes (for example GP global sum, provider baseline tariff) are not also funded as Enhanced Requirements.
- A “capability” where met should be supported by the GP IT Enabling Requirements necessary to access and utilise that capability for example infrastructure, equipment, service desk, specialist support.
- Where a CCG chooses to commission a solution to meet an Enhanced Requirement any standards referenced in this document and applicable to that requirement must be met.

- Enhanced does not infer a capability of lesser importance, only that the relevance and appropriateness will be dependent on the locality context and provision of these services must be secondary to meeting Core and Mandated Requirements.
- Many enhanced digital capabilities will be enablers for service/business change which can realise significant benefits to the NHS, patients and general practice.

4.3 Practice business requirements

The requirements for digital systems, infrastructure and organisation activities necessary to run the internal practice business and organisational governance and are the responsibility of the practice to provide:

- practice business support systems
- practice buildings and estate
- practice operating costs
- practice legal and regulatory responsibilities
- practice websites
- dispensing services

Although responsibility for commissioning and provision of these requirements is out of scope they may be indirectly linked using common infrastructure, standards, assurance, interoperability and security. In such cases practices are required to comply with any relevant technical and security standards.

The infrastructure and general support required to operate these services (namely desktops, printers, network connectivity) can at the discretion of the CCG be funded and provided as “enhanced GP IT Enabling Requirements” where this allows the practice to operate more efficiently and is considered affordable locally.

CCGs are encouraged to consider developing local purchasing frameworks for general practice business support systems and services to facilitate better value for money. Practices can procure from such frameworks to secure better value for money and assurances on cyber security, data security and clinical safety using the standards and guidance referenced in this Operating Model.

CCGs will encourage and provide technical advice to practices to migrate to advanced telephony systems suitable for General Practice which meet the template specification attached to Appendix E. These assist practices manage peak demand, operate telephone and video consultations, improve practice resilience and business continuity and increase workforce flexibility options with remote and home working.

4.4 Service availability & Incident Response

GP digital services must be provided for the hours the general practices are contracted to offer primary care services. Some services however need only be available for restricted “office” hours whilst others may be required for longer hours with appropriately adjusted support levels.

Support for GP digital services needs to:

- match the contracted hours of General Practice services
- reflect business critical digital functions
- support extended access
- respond to high severity cyber incidents (through business continuity and disaster recovery planning)

The following are the minimum service availability requirements:

4.4.1 Standard Service Hours – Services to be provided between 09:00 – 17:00, Monday to Friday, excluding Public Holidays. This will include, in addition to the operational support services, those services which do not require an immediate response at any time within the GP contracted hours but which should be available during normal “office” hours.

4.4.2 Operational Support Hours – Services to be provided for core GP contracted hours, as detailed in the GP Contract (between 08:00 – 18:30, Monday to Friday, excluding Public Holidays). This will cover the provision of services required to respond at any time during the hours required under the GP Contract.

4.4.3 Extended Operational Support Hours – As part of the GP IT enabling services to support PCNs under this model CCGs must commission Extended Operational Support Hours. Support provided during the Extended Operational Support Hours should ensure the continuity of Essential Services. From October 2022 this will support PCN Enhanced Access services. The CCG will consult with PCNs, practices and LMCs to determine the scope of and any applicable restrictions to the “Extended Operational Support Hours” including:

- exceptions (for example public holidays)
- practice premises, practices and operational services supported
- applications supported

4.4.4 High Severity Incident Support Hours – All practices must have access with 24 hour 7 day availability to log a High Severity Incident or request using one of the following methods:

- telephone
- email
- web portal (internet accessible)
- app

GP IT enabling services must provide:

- monitoring of logged High Severity Incidents outside Operational Support Hours
- incident escalation of High Severity Incident to 24 hour 7 day response as necessary whether raised locally or nationally
- a business continuity plan and associated disaster recovery plans which provide the necessary response outside standard operating hours including the mobilisation of resources necessary to manage the incident and meet Recovery Time Objectives (RTO)
- a business continuity response based on a 48 (actual) hour Recovery Time Objectives (RTO) for the practice to provide Essential Services

See requirements for Cyber Security, Clinical Safety Assurance, Service Desk, and Information Governance.

4.4.5 Systems and Infrastructure Availability – Critical systems and infrastructure should provide 24 hour 7 day availability with individual contracts defining % availability and support hours. Examples include Clinical Systems (Foundation Solutions), NHS applications, Health and Social Care Network (HSCN), WiFi, Local Networks and GP online and video consultations

4.4.6 Third Party Support Availability – Where a supported service requires third party referral, advice or action for resolution the capability of that service may be limited outside the support hours contractually offered by the third party. In such cases resolution of incidents or problems should be prioritised and based on work around or contingency solutions. In the case of High Severity Incidents and activated business continuity (BC) and disaster recovery (DR) plans third party activities should be integral within these plans.

4.5 Accreditation, Choice and Selection of Solutions

General practices, which use computerised patient records, are required through the GP Contract to use an accredited clinical system. The accreditation is determined by the inclusion of the required capability in the GP IT Futures Framework. Each practice can determine the most appropriate Foundation Solution from the accredited solution(s) offered in the framework to meet the six Foundation Capabilities described in Appendix A. CCGs and practices will then jointly select the practice's choice of accredited Foundation Solution, subject to the conditions described in the CCG-practice Agreement.

National Digital Services are commissioned centrally and provided to practices to be used directly or through their clinical system interfaces. There is no local choice or selection of such solutions.

All other capabilities for example online consultation systems or document management systems will be met by solutions determined by the CCG in collaboration with practices and then jointly selected by the CCG and practices. Unlike Foundation Capabilities the use of accredited solutions is not contractually mandated although compliance with standards attributed to the capability should be considered essential. In all cases CCGs

should only procure solutions which meet the standards referenced in this Operating Model and whenever possible should use an appropriate national framework contract (see Appendix C). Compliance with CCG Standing Financial Instructions (SFIs) will require demonstration of value for money and product quality and safety. Within any single CCG, practice requirements may vary and therefore in some circumstances procurement of more than one solution may be appropriate. Where GP IT Futures notional CCG funds are used the solutions can only be sourced through the GP IT Futures Framework.

GP IT Enabling Requirements will be commissioned by the CCG to the standards assigned to the requirement commissioned (See Appendix A).

Table 1: Summary of Solution Selection and Mandatory Accreditation

Requirement	Choice of Solution	Procurement Routes
National Digital Services	NHS Digital or NHS England	N/A
Core and mandated essential clinical capabilities – GP IT Futures Foundation Capabilities	General Practice chooses its Foundation Solution	Must be accredited and sourced through the GP IT Futures Framework
Other core and mandated essential clinical capabilities: not Foundation Capabilities	Commissioning CCG in collaboration with practices	Applicable Framework including DCS Frameworks (see Appendix C)
GP IT Enabling Requirements	Commissioning CCG	Applicable Framework or local CCG procurement*
Enhanced Capabilities and Requirements	Commissioning CCG in collaboration with practices	Applicable Framework including DCS Frameworks (see Appendix C) or local CCG Procurement*
Practice Business Requirements	General Practice	Practice Responsibility

* “local CCG procurement” will be subject to compliance with standards in this Operating Model and NHS procurement and financial obligations

4.6 De-commissioning of services

The CCG may de-commission a service meeting a core and mandated capability providing:

- the core and mandated capability is still met either through a replacement service or by rationalising service duplication
- the decision does not conflict with the practice’s choice of Foundation Solution
- for non-Foundation Capabilities as part of the determination of the replacement service the practice has been consulted

The CCG may de-commission a service meeting an enhanced capability providing the risks to and impact on practices and patient services has been identified and affected practices consulted. Where a replacement service for an enhanced digital capability is to be commissioned practice consultation will have taken place as part of the process.

The CCG may de-commission a GP IT enabling service providing:

- any core and mandated enabling requirements are still met either through a replacement service or by rationalising service duplication
- practices are advised of any service delivery changes and Appendix 1 of the CCG Practice Agreement is updated as necessary

5. Funding

Detailed guidance on current funding arrangements and allocations is provided in Primary care SDF and GP IT funding guidance 2021/22. Further published guidance will where applicable supersede funding guidance in this document.

5.1 Key Actions:

- core and mandated GP IT Enabling Requirements (See Appendix A) are mandatory for local investment
- investment for GP IT should be maintained and enhanced to support local plans to address the sustainability and quality of general practice, as outlined in the NHS Planning Guidance
- investment in Enhanced Requirements should be commissioner led, and in consultation with general practices. It will align closely with plans for any local digital strategy and ICS which underpin the integration and transformation of care locally
- CCGs are accountable for any financial risks associated with over-spending as part of their overall resource limit
- clear financial protocols must be established and agreed between commissioners and delivery organisations to ensure CCGs remain in compliance with their financial obligations
- CCGs and their GP IT Delivery Partners must follow all necessary financial guidance in relation to provision of GP IT services, including NHS England financial guidance. Where the commissioned GP IT Delivery Partner is not an NHS England body or a CCG they will be required contractually to support the CCG in its compliance with NHS England financial guidance in all matters relevant to GP IT services provided for example procurement support services
- allocation of GP IT funding to CCGs is to support the provision of services, as outlined in this Operating Model, to general practices. If individual practices do not wish to receive such services from the CCG the CCG has no obligation to provide alternatives or to offer direct funding to the practice in lieu of such service provision

5.2 Revenue Funds

5.2.1 Core GP IT Funding

GP IT revenue funding is included in CCG core baseline allocations. Priority must be given to funding the core and mandated digital requirements described in this Operating Model, for both practices and additional roles associated with PCNs, with any remaining funds used to support the wider transformation of digital primary care.

5.2.2 GP IT Infrastructure and Resilience

Additional revenue funding is allocated direct to CCGs to support infrastructure and resilience dealing with specific technology upgrade programmes which are key to providing safe, robust and secure IT services prioritising replacing some of the non-strategic temporary remote working solutions such as Remote Desktop Protocol systems, deployed during the Covid-19 pandemic but not appropriate as long term solutions. Instead, alternatives such as Virtual Desktop Infrastructure should be considered, while also allowing systems to apply flexibility

5.2.3 GP IT Futures Framework

The GP IT Futures Framework as part of the Digital Care Services (DCS) Catalogue is supported by a notional allocation of revenue funds held by NHS Digital to each CCG. These funds are based on registered patient capitations.
In using these funds, the CCG:

- will procure Foundation Solutions to meet the Foundation Capabilities through the GP IT Futures Framework as first call on the funds
- will only use the funds to procure solutions through the GP IT Futures Framework
- may use remaining funds to procure remaining core and mandated Essential Clinical System Capabilities (see Appendix A) available through the GP IT Futures Framework
- may use any remaining funds to procure solutions to meet enhanced clinical capabilities through the GP IT Futures Framework for use by their practices
- NHS Digital holds a smaller amount of funding for GP IT Futures Framework to manage central activities such as standards payments

CCGs can also use local funds and baseline GP IT revenue funds to procure enhanced capabilities directly through the GP IT Futures Framework.
Individual practices are also able to procure any accredited solutions directly through the GP IT Futures Framework using their practice funds.

Assurance

Through the GP IT Futures Framework reporting capability NHS Digital will, for each CCG:

- identify by each CCG that all core and mandated (essential clinical system) capabilities have been procured by the CCG for all its practices
- identify that the total in year spend by the CCG flagged on the catalogue as centrally funded is within the value of the GP IT Futures notional allocation for the CCG

In the event that assurance (i) above is not met NHS Digital will raise an escalation with NHS England who will investigate to confirm there is no breach of NHS GP Contract obligations.
Individual practices can refer to Appendix 1 – Summary of Services Table within the CCG-Practice Agreement to confirm services the CCG has procured for the practice.
Directions on coding and monitoring arrangements for CCG allocations is given in Primary care SDF and GP IT funding guidance 2021/22.

5.2.4 Online Consultation Systems

The programme supports the rollout and uptake of online consultations in general practice and ensures that software systems are in place to support this. From 1st April 2021 onwards, CCGs are expected to have a local contract(s) in place for online consultation and for video consultation systems. Accredited solutions should be selected, and these can be sourced through the new Digital Care Services DFOCVC Framework or Health Systems Support Framework (HSSF).

5.2.5 Digital First Primary Care

The Digital First programme fund launched in 2019 is a five-year revenue stream with a focus on the use of digital and online tools to improve access to the core elements of primary care services. This will support:

- CCGs to embed and build on the digital transformation advances made in primary care as part of the pandemic response
- all practices to deliver the core digital offer set out in the GP Contract and to increase use of digital tools by staff and patients, including through digital inclusion initiatives
- all staff to work remotely
- implementation in all PCNs and practices to streamline digital pathways to increase usability for patients, embed triage and support at-scale working
- Digital First Accelerator projects that either test a new digital innovation or enable deployment of a tested solution in a new area or context, to solve performance or clinical priority issues. They must have the potential to be scalable across the system or regional footprint and to be sustainable over time

5.3 Capital Funds

5.3.1 BAU GP IT Capital

NHS England capital funding for GP IT will continue to be available for CCGs to access from NHS England Regional teams. Regional teams have delegated authority to set GP IT capital allocations for CCGs/health systems. This funding is designated to deliver, as first priority, systematic refresh of the GP IT estate for both practices and additional roles associated with PCNs, in line with the requirements of the GP IT Operating Model. Any remaining funds should be invested in technology advances that will improve the overall experience for staff and patients, as well as the security and cost-effectiveness of general practice and PCN IT infrastructure. Priority should be given to maintaining the GP IT estate necessary to support the core and mandated digital capabilities described in this Operating Model and compliance with the current local warranted environment specification (WES). Associated deployment costs for example installation, disposal, software licences should be considered within the capital bid. Depreciation costs arising from GP IT capital will continue to be funded centrally by NHS England.

Other revenue consequences arising from the growth of the combined GP and PCN IT estate will need to be included within CCG GP IT revenue plans. Practices need to discuss this with the CCG at an appropriate early stage.

5.3.2 Estates and Technology Transformation Fund (ETTF) Capital

ETTF is a multi-million pound investment (revenue and capital funding) in general practice facilities and technology across England. ETTF programme capital will continue to be available through Regional Teams to support both business as usual (BAU) GP and PCN IT investments and transformational estate schemes. It is expected this fund will continue to be available until 31st March 2022. CCGs will be responsible for communicating with their practices the detail of such investments and how these are expected to support general practice. Depreciation costs arising from ETTF capital will continue to be funded centrally by NHS England. Any other revenue consequences arising from the growth of the GP IT estate will need to be included within CCG GP IT revenue plans.

5.3.3 Microsoft Office 365 for the NHS Licencing

£41.1m of central capital funding was allocated in 2020/21 to regions on a fair share basis and accessible by CCGs via PID submission to regional teams available to pay for licensing of Microsoft systems across Primary Care. No further central funding is allocated for N365 licences any further requirements up until April 2023 should be supported from GPIT capital funds. Participating CCGs must fully implement all elements of **Microsoft Office 365** licences for general practices by no later than 13 October 2021 in accordance with the Microsoft Office 365 for the NHS Participation Agreement. The agreement will then run until 30 April 2023.

CCGs responsible for procuring Microsoft Office 365 for the NHS licences for general practices and the migration away from Office 2010 will have considered a desktop installed version of Office 365 for those general practice users who require integration between the practice clinical system and Microsoft Word.

Compatibilities vary with each GP clinical system and the CCG should check with the relevant foundation supplier.

Other software applications in use by the practice may also rely on integration with MS Word, CCGs should therefore consider their entire estate as they plan their Microsoft 365 migrations. CCGs or practices (depending on who holds the licence) should check requirements with the relevant system supplier.

For practice staff and organisations who only use MS Word as a “standalone” application (without integration) CCGs may have considered the cheaper restricted E3 licence.

CCGs should start planning for the impact on Office application use in practices after 30 April 2023 when the current NHS participation Agreement ends. These plans should reflect NHS policy and guidance as it becomes available.

5.4 Time limited funding initiatives

To enable specified programmes additional allocations of non-recurrent funds will continue to be released to CCGs to support such programmes. These funds should be used to support the identified programme. Assurances will be secured through the relevant programme generally based on deployment and capability outcomes. CCGs should take into consideration financial impacts of any new systems or infrastructure deployed and the continuity in provision once the time limited funding ceases. Any decision to enhance the CCG allocations to support any recurring costs after the transition period will be made on a programme by programme basis.

5.5 Direct Funding

CCGs have delegated responsibility to provide by (either directly or by commissioning) digital services for their practices as defined in this Operating Model. CCGs should not offer GP IT funds directly to general practices to enable them to provide or commission these services, unless advised otherwise for a specified GP IT purpose in this document for example reimbursement to practices for clinical system training. Where a CCG considers direct funding to practices for any such specified service, whether funded in advance or by reimbursement against an approved claim, the following requirements should be adhered to:

- CCG compliance with its SFIs
- compliance with NHS England financial guidance
- compliance with other standards for example cyber and data security, clinical safety, GP Connect Products
- how value for money is assured when procurement is disaggregated. The CCG remains responsible for compliance with the standards in this Operating Model
- that other practices, not receiving direct funding for GP IT from the CCG, are not disadvantaged
- GP IT Funding is not awarded directly to another party acting on behalf of the practice (for example sub-contracted), unless that party has been commissioned by the CCG to provide GP IT Services following appropriate procurement process

5.6 Other sources

The designated funding allocations above are made to ensure CCGs are able to provide, as a minimum, the core and mandated digital requirements required by general practice as defined in this Operating Model. Any funding surplus to meeting this requirement should be used to provide the locally prioritised enhanced digital requirements. CCGs should also consider the use of any other locally available funding

sources to support enhanced digital capabilities which reflect the local digital roadmap for service improvement and transformation in all local care settings.

5.7 Continuity and Digitisation of GP Records

Using the learnings from the pilot projects for digitisation of paper records, the strategy for the digitisation of Lloyd George records is under review to ensure that the most effective delivery model is implemented to meet the GP contractual commitment to digitise GP patient records at the point of care by March 2022.

5.8 Out of scope

CCGs are expected to ensure that the commissioning and procurement of digital services locally does not duplicate existing funding sources or provision. General practice business requirements should not be funded using CCG allocations.
The General Practice Global Sum is out of scope. It is used to directly fund GP Contracts and will include services and utilities such as those listed in this document as General Practice Business Requirements.

Dispensing practices (approximately 1,000) operating under NHSEI Standard Contract arrangements for pharmaceutical dispensing regulations require software and digital infrastructure to operate the dispensing function. These services are outside the scope for the receipt of GP IT digital services under this Operating Model. Dispensing practices are in scope for the GMS/PMS/APMS contracts to provide essential services.

Table 2: Funding sources and application supporting Digital Primary Care

Funding	Type	Purpose
Core GP IT Revenue	Revenue	To provide/commission GP and PCN IT services with 1st priority on core and mandated GP IT Enabling Requirements.
GP IT Infrastructure and Resilience	Revenue	Additional funding direct to CCGs to support infrastructure and resilience dealing with specific technology upgrade programmes which are key to providing safe, robust and secure IT services for example replacing some temporary remote working solutions deployed during the pandemic.
GP IT Futures Framework	Revenue Notional Allocation	To call off accredited solutions from GP IT Futures Framework with priority for Foundation and core and mandated capabilities
GP Online Consultations	Revenue	To support the rollout and uptake of online consultations in general practice.
Digital First Primary Care	Revenue	A five-year revenue stream with a focus on the use of digital and online tools to improve access to the core elements of primary care services including remote access for GP staff
BAU GP IT Capital	Capital	GP and PCN IT infrastructure/equipment priority to support Core and Mandated Requirements
ETTF Capital	Capital	To support both Business As Usual GP and PCN IT investments and transformational estate schemes.

6. Commissioning, Procurement and Contract Management

CCGs should exercise best practice and comply with NHS England financial guidance and local Standing Financial Instructions (SFIs) in the commissioning, procurement and contract management of GP digital services. These activities will ensure:

- value for money
- compliance with procurement legislation and internal SFIs

CCGs will ensure procurements are compliant with the standards described in this Operating Model including:

- data protection regulations and cyber security controls
- clinical safety standards and medical device safety standards
- information standards
- interoperability standards
- clinical terminology standards

CCGs must ensure, as a Core and Mandated Requirement, that they and their practices have access to competent procurement advice for any digital services and equipment being procured under this Operating Model (Appendix A).

Practices vary considerably in size, resources and inhouse technical capabilities. CCGs need to ensure consistent access to such services is available to all practices.

CCGs are encouraged to collaborate on procurements and make use of appropriate framework agreements such as Digital Care Services (DCS) Catalogue frameworks and Health Systems Support Framework (HSSF) (see Appendix C) to ensure best value for money, compliance with applicable standards and to reduce procurement workload. As ICS develop procurements should align with ICS digital strategies.

6.1 Procuring GP IT Enabling Requirements

CCGs are encouraged to use an applicable national framework (Appendix C) with underpinning standards for example HSSF to procure GP IT enabling services. Appendix E provides a specification template and supporting tools for CCGs. Without precluding providers offering innovative approaches CCGs should give consideration to the following:

- services where demand is likely to be linked to quantities supported (for example number of devices, users etc) and how incremental/organic growth can be accommodated
- for specialist (expert) services (for example training, data quality, project management, information governance etc) what will the available capacity be and how will it be managed
- how the framework can provide assurances against compliance with applicable standards

Where the GP IT enabling services cannot be provided through an appropriate framework such as HSSF then CCGs may commission GP IT enabling services from providers through other procurement routes – this includes private providers, local NHS Trusts, CCG shared services and other local consortia arrangements providing that the capabilities and standards described in this document are met.

Where CCGs support practice organisations which hold multiple contracts in geographically dispersed CCGs they 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

Neither the practices in question or the remaining practices in the CCG(s) should be disadvantaged by such an arrangement. (Note see also sub-contracting of services)

Whatever the procurement approach used the CCG as commissioner is responsible for commissioning services which:

- offer resilience
- ensure the Core and Mandated Requirements described in this document are provided to their practices
- meet all other requirements and standards in the Operating Model
- ensure the provider organisation meet the standards for GP IT Delivery Partner organisations described below including Data Security and Protection Toolkit (DSPT) and other certification requirements
- comply with any relevant legal and regulatory obligations for example as Data Processor. This should include any required Data Processing Agreements (DPA)
- ensure the CCG is able to meet its obligations under the CCG-Practice Agreement
- is governed either by a fixed term formal contract or fixed term formal NHS Service Level Agreement (SLA). Either to be supported by a robust specification which reflects the requirements to be met and the standards applicable
- comply to a service specification with robust Key Performance Indicators (KPIs) and standards which is used to inform the Support and Maintenance Levels Schedule in Appendix 2 of the CCG-Practice Agreement
- demonstrate value for money
- complies with the CCG's Standing Financial Instructions (SFIs)

All CCGs, regardless of procurement approach, are encouraged to make use of the GP IT specification commissioning support pack in Appendix E.

Some digital services will be procured through dedicated framework contracts as directed by national NHS programmes.

6.2 Direct provision of GP IT Enabling Requirements

Some CCGs may choose to provide all or part GP IT enabling services directly either as an individual CCG (in-house services), a CCG collaborative (in-house services) or as a CCG shared service. In such cases the CCG(s) must put in place robust arrangements which meet ALL the requirements listed above (6.1) and also

- ensure any necessary and appropriate steps are taken to manage any potential conflicts of interest for the CCG as both commissioner and provider

6.3 Organisational Standards for GP IT Delivery Partners

When commissioning GP IT enabling Services, the following mandatory organisational standards must be met by the provider:

- NHS Information Governance – to demonstrate compliance with all mandatory assertions in the NHS Data Security and Protection Toolkit (DSPT) for the relevant organisation type
- accreditation to Cyber Essentials Plus (CE+)
- the organisation will be accredited to ISO 22301 for Business Continuity Management OR will be compliant with the NHS England Business Continuity Management Framework

Organisational standards may apply to whole organisation and all services it provides internally and externally or may be defined in more detail, for example within the Information Security Management System (ISMS) scope or Business Continuity Management System (BCMS) scope. Commissioners should seek assurance that any standards compliance or certification from a provider fully applies to the scope of the services being commissioned and to all providers delivering the services commissioned. Note: individual requirements have applicable standards assigned as required (see Appendix A).

The CCG **must** also obtain assurance, for example through a data processing agreement, that the provider organisation is able to meet its obligations as data processor required under the General Data Protection Regulation (GDPR) Compliance Guidelines.

These should be regarded as minimum standards for the organisation. Using an appropriate framework such as Health Systems Support Framework (HSSF) will provide assurances for compliance with such standards

.

6.4 Procuring Essential Clinical System Capabilities

Under the GP IT Futures Framework CCGs will use notional allocations of funds held by NHS Digital to procure solutions from the GP IT Futures Framework which meet the Essential Clinical System Capabilities for their practices. In exercising this responsibility CCGs must:

- ensure Essential Clinical System Capabilities are provisioned for all eligible practices

- ensure compliance with procurement legislation and internal Standing Financial Instructions (SFIs) (through utilising the GP IT Futures Framework)
- ensure value for money
- ensure practices are able to choose their preferred accredited Foundation Solution

6.5 Procuring GP IT Equipment

When procuring GP IT equipment using NHS capital funds CCGs will adhere to NHS England financial guidance, internal SFIs and procurement legislation. National framework contracts which offer the best value for money should be used where possible. CCGs have access to the NHSE/I National Commercial and Procurement Hub for advice and support in procurement of GP IT equipment using capital funds.

6.6 Practice Direct Procurement

Where practices commission, procure and contract manage digital services directly they should have access to specialist advice and support either through CCG commissioned GP IT services or, if applicable, through the NHSE/I National Commercial and Procurement Hub where such digital services and systems will interface with NHS provided systems or operate on NHS managed infrastructure. Practices procuring practice business support systems, local clinical systems and equipment enhancements are responsible for resourcing and managing their own procurement and contract management processes but should seek advice where NHS systems or managed infrastructure may be used, integrated or impacted and seek assurance that the systems do not represent a risk to other NHS IT systems. A local procurement checklist is provided in Appendix G which may help practices in these activities.

Any practice procured software, digital system or equipment which utilises NHS systems or managed infrastructure must be approved as described in CCG-Practice Agreement. Such approvals should not be unreasonably withheld. Software, browsers and operating systems not supported or maintained by the supplier must not be used on NHS managed infrastructure.

Where practices procure digital services directly, they remain responsible as contract holder, for the maintenance of that service which will include ensuring it remains supported by the supplier/developer. The security of systems and applications which are unsupported or unmaintained cannot be assured and must not be used on NHS managed infrastructure. Where a practice chooses to procure its own solution to a “core and mandated” requirement or capability defined in this document the CCG is not obliged to reimburse the practice for the cost of this service – see Direct Funding. Individual practices have direct access to appropriate frameworks such as Health Systems Support Framework (HSSF) and DCS Catalogue frameworks and are encouraged to use these to ensure value for money and compliance with applicable standards.

7 Assurance

7.1 Digital Primary Care Maturity Assurance Tool

The Digital Primary Care Maturity Assurance Tool (DPCMAT) holds annual data from April 2015 demonstrating trends and changes over this period and allowing the NHS to assess the effectiveness of the Operating Model. The DPCMAT will continue to be used in support of this Operating Model.
Data will be sourced annually from the following:

- NHS Digital – Organisation Data Service (ODS)
- General Practice annual e-Declaration (eDEC)
- CCG Annual GP IT Survey
- NHS DSPT– GP Submissions
- NHS Digital – Patient Online Management Information (POMI)

The updated DPCMAT indicators (from April 2021) are shown in Appendix D.
Where an indicator is relevant to a requirement described in this Operating Model the indicator(s) is shown assigned to that requirement (Appendix A). DPCMAT data is available through the Primary Care Indicators Dashboard (www.primarycareindicators.nhs.uk). This dashboard provides access to General Practice Indicators and the DPCMA data. GPs and CCGs can register for an account here

Local benefits include:

- supporting CCGs in the management or re-procurement of GP IT service provision
- provide assurance that CCGs are meeting the requirements of the GP IT Operating Model in the effective delivery of GP IT services
- demonstrate progress and identify areas for investment in GP IT services and digital innovation
- support Care Quality Commission (CQC) assessment by providing insight into the use of digital technology within the practice, to help meet patient need and improve delivery of clinical services
- demonstrate local progress against GP Contract digital requirements

7.2 NHS Data Security and Protection Toolkit (DSPT)

All practices must complete and submit an annual DSPT as a requirement under the CCG-Practice Agreement. This is the responsibility of the individual practice, but support should be available to practices in the form of technical advice and access to required data which the CCG or its commissioned GP IT provider may hold.

7.3 NHS Tracking Database

The NHS Tracking Database provided by NHS Digital was decommissioned on 1 April 2020. Updating the tracking database is no longer part of the National Digital Services implementation requirement. Services procured through the GP IT Futures Framework will now be selected and recorded through the Digital Care Services (DCS) Catalogue.

7.4 Use of Funding Allocations

Directions on coding and monitoring arrangements for CCGs is given in Primary care SDF and GP IT funding guidance 2021/22.

8 Addressing the Challenges

This updated Operating Model continues to address six contemporary challenges

8.1 Challenge 1: Keeping General Practice and Patients Safe

A strong emphasis on security and safety of digital technologies used in general practice

8.1.1 Risks to General Practice

General practices have a critical operational dependence on digital systems to operate routinely on a daily basis. Practices are at risk from:

- significant system failure which may severely disrupt or close Essential Services in a practice with almost immediate effect. Workarounds may be limited depending on the nature and extent of the system failure
- the loss of data (patient records) or loss of access to data, whether arising from failure of digital systems or of infrastructure will present high impact risks to the practice in (i) operational continuity (ii) patient safety (iii) corporate criminal liability (iv) potential regulatory action from the (Information Commissioner's Office (ICO) including fines
- errors, faults or algorithmic based outputs from embedded logic and knowledge bases in software which processes patient information may lead to clinically unsafe recommendations or decisions

8.1.2 Minimising risks

General practices as independent organisations have certain legal and regulatory responsibilities relevant to data protection and security and business continuity. Understanding these responsibilities at a senior level within practices and within CCGs and providing practices with access to specialist support and advice forms the foundation of minimising these risks.

The CCGs are required to provide practices with access to specialist advice to support practices discharge these responsibilities. This includes:

- information governance, including advice and support for the practice designated Data Protection Officer (DPO)
- Cyber Security management and oversight
- Clinical Safety Assurance advice and support
- digital systems procurement advice

These are complemented by the wide range of GP IT Enabling Requirements described in Appendix A which underpin a safe digital operating environment for practices.

8.1.3 Information Governance

As data controllers and public authorities general practices have specific regulatory, legal and contractual responsibilities and are lawfully required to designate a DPO. Practices will have access to an information governance support service providing specific areas of support including advice to the practice designated DPO on Data Protection and Information Governance matters. CCGs are required to provide a DPO service offering a named DPO to practices (which can be shared between practices). Individual practices are entitled to appoint an alternative DPO of their choice although CCGs are not expected to fund this if a DPO function has already been offered.

Individual practices must complete and submit the NHS GP DSPT as a requirement under the CCG-Practice Agreement.

8.1.4 Patient safety and medical devices

As a core and mandated GP IT Enabling Requirement CCGs should ensure they and their practices have access to a Clinical Safety Assurance Service when procuring and deploying clinical systems and system modules:

Where CCGs or individual practices procure clinical software from routes other than the Digital Care Services (DCS) catalogue steps should be taken by the procuring authority (namely CCG or General Practice) during procurement to ensure the supplier has applied DCB0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems in the development and manufacture of the software.

CCGs and individual practices should apply DCB0160: Clinical Risk Management: Its Application in the Deployment and Use of Health IT Systems when implementing clinical systems and should apply DCB0160 in the regular review of business and clinical process. This will ensure safety is not put at risk by operational work rounds. This is the responsibility of the procuring authority (i.e. CCG or General Practice).

All practices should register with the Medicines and Healthcare products Regulatory Agency (MHRA) Central Alerting System (CAS) for both email and mobile phone text alerts. This is a web-based national cascading system for issuing patient safety alerts, important public health messages and other safety critical information and guidance to the NHS and others.

Where CCGs or individual practices procure clinical software or medical devices which interact with the clinical software and patient record from routes other than the DCS Catalogue assurances should be sought that the supplier has applied if applicable to the product current medical device regulations: Medical Devices (Amendment etc.) (EU

Exit) Regulations 2020: and the Medicines and Medical Devices Act 2021. Users of such software and medical devices should follow manufacturer's instruction for use (IFU). Any change of use needs to be properly assured with the manufacturer's knowledge/permission as any "off label" use will mean that the user has taken on the responsibilities/liabilities of the manufacturer/developer.

The Digital Technology Assurance Criteria (DTAC) will be helpful in securing these assurances.

8.1.5 Continuity of General Practice Records

The following areas identified as risks to the continuity of patient records continue to be worked on by NHS England, NHS Digital and relevant suppliers.

Issue: The transfer of records between systems can result in record integrity and continuity issues.
Action: NHS England and NHS Digital will continue working with system suppliers to address and resolve this.

Issue: Where general practices close or patients move out of NHS general practice care (or cross Home Nations borders within the UK) record continuity and integrity issues can arise.
Action: NHS England and NHS Digital will continue to work with the professional bodies to address and resolve this whilst ensuring compliance with data controller responsibilities.

Issue: The persistence of paper patient records in general practice can result in record continuity and integrity issues and is resource intensive
Action: NHS England will continue to work with stakeholders and professional bodies to develop national standards leading to the commissioning of approved digitisation services. CCGs are advised to defer further commissioning of GP records digitisation until such standards and national guidance become available.

8.1.6 Locally procured digital systems and technologies

Systems and technologies procured locally, for example by practices or PCNs, continue to represent a security and safety risk within the GP IT estate. These may include diagnostic equipment which use desktop computers or which interface with the clinical systems.

The functionality available from such systems is often invaluable to the operation and efficiency of a busy general practice.

To support practices, make safe procurements and utilise digital systems and technologies with confidence this Operating Model puts in place the following:

- practices, CCGs and GP IT delivery providers should meet the capabilities and standards described in this Operating Model including those related to hardware, infrastructure and procurement. CCGs and practices will have access to specialist advice on procurement of digital services and systems:

- CCGs, practices and PCNs should make full use of the DCS Catalogue and other applicable Frameworks (see Appendix C) to procure solutions which meet necessary standards
- a simple checklist for CCGs and practices considering local procurement where a framework is not applicable has been provided in this Operating Model (Appendix E). This includes utilising the Digital Technology Assessment Criteria (DTAC)
- software, browsers and operating systems not supported or maintained by the supplier must not be used on NHS managed infrastructure
- the contract holder (namely original purchaser) is responsible for ensuring systems, applications and hardware remain supported (by the original supplier or their agent)
- practices as data controllers should ensure where applicable that responsibilities of the digital service supplier as data processor are contractually recognised and the agreed data flows are documented

Note: This does not include personal devices and applications owned by practice staff (see Remote Access and Bring Your Own Device (BYOD)).

8.1.7 Remote Access

Remote access to practice clinical systems and Managed GP IT Infrastructure is required to support mobile and remote working for practice staff during normal business operations and as a key part of practice business continuity plans offering resilience and flexibility. A remote access service is now a core and mandated service which must be offered to practices. Remote access services offered to practices should have the capability of supporting at least 60% of normal operational capacity.

Remote access solutions must not be used which bypass or otherwise reduce the effectiveness of security measures, including authentication using NHS Smartcard (or an approved alternative/replacement) or the NHS Care Identity Service 2, service, within the GP IT Futures Framework solutions, National Digital Services or the Managed GP IT Infrastructure.

Operating a GP clinical system without the proper use of an NHS Smartcard, or an approved alternative which supports secure authentication and an ‘advanced electronic signature’, may compromise the legal status of e-prescribing. Those signing a prescription need to be able to demonstrate that they were in sole control of the signing capability at the point of signing. Once approved (through NHS Digital) alternative solutions to NHS Smartcards can be integrated by suppliers into the Accredited Foundation Clinical Systems.

Approved remote access solutions include:

- issuing of an NHS managed laptop (or other endpoint) and means of secure VPN access

or:

- use of a secure Virtual Desktop Infrastructure (VDI) solution

Remote access to practice clinical systems will be more effective if remote access to practice telephony systems is also available to staff for example by using an advanced voice over internet protocol (VoIP) telephony solution.

Remote access to practice business systems is a practice responsibility but any solution must comply with standards in this document if the Managed GP IT Infrastructure is used or accessed in any way.

8.18 High Severity Cyber Incident Management, Business Continuity and Disaster Recovery

All parties namely individual practices, CCGs, GP IT Delivery Partners, NHS England and NHS Digital have a responsibility to:

- take measures including technical, planning and organisational policies and operating procedures to minimise the risk of cyber incidents
- identify, report, manage and mitigate high severity cyber incidents whenever they occur

Responsibilities and accountabilities are summarised in Appendix B

In the event of a national cyber incident being formally declared (for example by the NHS Digital Data Security Centre) all parties will fully cooperate and support the actions required by the Emergency Preparedness, Resilience and Response (EPRR), NHS Digital, NHS England, or any other party with delegated authority. This may include providing urgent out of hours contacts and communication routes as well as access to practice premises and digital systems and equipment outside normal working hours.

The CCG and its commissioned GP IT Delivery Partners will ensure full cooperation in 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.

High Severity Service Incidents (HSSI) initiated by third parties (for example providers of clinical systems, infrastructure services, national digital systems) will be reported to the NHS Digital Service Desk. Higher severity incidents (levels 1 and 2) and incidents identified as a Crisis will be coordinated by and managed by the NHS Digital Service Bridge, in conjunction with the third party.

8.1.9 Data Breaches

As data controllers and public authorities, general practices have specific regulatory, legal and contractual responsibilities but they do need to be supported with access to specialist services who can provide expert advice and guidance in the event of a data breach.

As data controllers and public authorities general practices are required in accordance with GDPR Article 33 (refer to Recitals 85, 86, 87 and 88), to report personal data security breaches where there is a risk to the rights and freedoms of individuals to the Information Commissioner's Office (ICO) without undue delay and where feasible within 72 (actual) hours. To Note:

- NHS Digital have written guidance on reporting data breaches. This can be accessed through the Data Security and Protection Toolkit (DSPT)
- data breaches may occur without loss of data or loss of access to data, and therefore without a serious business continuity risk
- data breaches must be assessed and if applicable reported by the practice (as data controller) through the incident reporting tool within the DSPT and if applicable to the ICO (see above)
- CCGs, GP IT providers and practices must be aware of the legal responsibilities for data processors and data controllers.
- All parties namely individual practices, CCGs, GP IT providers, NHS England and NHS Digital will have responsibilities to identify, report, manage and mitigate data breaches and near misses whenever they occur. See Appendix B.

8.1.10 Patient Safety Incidents

All NHS funded organisations in England have a role to play in reporting and responding appropriately to patient safety incidents in to support improvement in patient safety. Patient safety incidents which meet the definition of a Serious Incident (SI) as described by the Serious Incident Framework should continue to be reported by the CCG (or by the GP IT Provider where they have direct access) to the Strategic Executive Information System (StEIS) or any successor reporting system. General Practices can report patient safety incident using the General Practice Patient Safety Incident Report Form.

Any adverse Medical Device incident should be reported by healthcare professionals or patients via the MHRA Yellow Card System.

NHS England operates the EPRR framework providing strategic national response to meet incidents or emergencies that could affect health or patient care.

8.1.11 Loss of access to patient records

The total loss of access to patient records may represent a patient safety and information governance incident. This may be due to a number of possible causes for example host system failure, network failure, power failure, premises disruption, system configuration fault denying permissions. Each practice will maintain a Business Continuity Plan (BCP) approved by the CCG which will include as well as response to threats to data security a response to loss of access to patient records. This should be activated as necessary.

As more systems become securely hosted externally and fewer are located within individual practice premises the role of a practice Disaster Recovery (DR) Plan becomes less relevant, although business continuity planning remains essential. Assurances are required however that third parties, providing infrastructure and/or data processing services have robust DR Plans.

8.1.12 Digital infrastructure, equipment and systems performance

The end user's experience of digital systems can be variable and subject to a number of factors including, but not limited to:

- network bandwidth, latency and contention
- hosted system performance
- local equipment and infrastructure age, specification, concurrent applications and configuration
- external threats

Where the digital system performance for the practice is impacted to the extent that it obstructs ongoing efficient and effective access to the digital patient record and its supporting capabilities then the practice should consider whether this represents a patient safety issue in which case they should escalate to the CCG requesting that it is processed as a High Severity Incident. The CCG should lead the resolution using methodologies applicable to potentially complex, multi-factor and multiple party problem solving.

8.1.13 Business Continuity Plans

Practices are required to maintain a business continuity plan (BCP) which should include loss of access to relevant IT services which the practice requires to maintain Essential Services. These should be reviewed and updated as necessary to reflect the lessons learned from the 2020-21 Covid-19 Response. CCGs must review all practice BCPs by 31st July 2022.

8.2 Challenge 2: Supporting general practice deliver their contracted services

IT infrastructure provided to a standard which allows the practice to efficiently and effectively use the capabilities identified in this Operating Model

Under the terms of the CCG-Practice Agreement practices are eligible to receive NHS funded services to meet the digital capabilities described in this Operating Model. Where a CCG-Practice Agreement is in place the CCG will offer these services as described in this Operating Model to the practice. This provides a single reference point identifying practices receiving GP Digital Services as well as formalising the responsibilities of the respective parties in providing and using these services.
The arrangements to address the previous challenge are a pre-requisite to the NHS being able to meet this challenge.

A number of requirements are defined as core and mandated. These require solutions to be provided (by the NHS) and to be used (by the practice) in order to meet the CCG-Practice Agreement obligations.

Clinical systems are defined through clinical digital capabilities. A number of these capabilities are categorised as core and mandated and referred to in this document as Essential Clinical System Capabilities.

These include six Foundation Capabilities which must be met using a Foundation Solution which is:

- accredited through the GP IT Futures Framework
- funded by the NHS for eligible practices with a signed CCG-Practice Agreement
- chosen by the individual practice from the GP IT Futures Framework
- procured through the GP IT Futures Framework

For those Essential Clinical System Capabilities which are not Foundation Capabilities solutions will be provided which:

- are funded by the NHS for eligible practices with a signed CCG-Practice Agreement
- must meet any standards referenced in this Operating Model, using the Digital Care Services (DCS) Catalogue or other applicable framework contract (see Appendix C)
- are selected by the commissioning CCG in collaboration with local practices

Note: Certain non-Foundation Capabilities may be provided as an embedded part of the Foundation Solution at the individual supplier's discretion. CCGs should determine with their practices which non-Foundation Capabilities are still required once Foundation Solutions have been selected. Additional solutions for these capabilities may still be available and may be procured as enhanced items if they offer a greater level of functionality and more appropriately meet local needs.

All capabilities in the DCS Catalogue have relevant standards assigned. System suppliers must meet these standards with their solutions to be "onboarded" to the catalogue. These standards can be accessed through the GP IT Futures Framework and include critical areas such as SNOMED CT, interoperability, clinical safety and cyber security.

Details on the funding arrangements for GP IT Futures Framework are given in section 5.

All digital capabilities where defined have standards attributed to these capabilities.

The CCG-Practice agreement requires that:

- practices have annual IT reviews with their CCG (or a party delegated on the CCG's behalf)
- there is an agreed escalation process which can be accessed where there are unresolved system or service performance issues
- there is an agreed dispute resolution process

From 31 March 2021 local hosting of GP clinical systems is no longer supported. Where legacy local clinical system servers are still in place CCGs and practices must work with the system suppliers and the GP IT Futures Framework to replace these with accredited hosted clinical systems by 31st August 2022. For details on how such legacy servers should be supported until then refer to the previous Operating Model.

8.2.1 Infrastructure

IT infrastructure should be provided to a standard which allows the practice to efficiently and effectively operate the capabilities provided locally to practices through this Operating Model. The cost of providing an enhanced capability therefore should include any associated IT infrastructure necessary to operate the capability. IT infrastructure cost should include any required operating system and software licencing costs.

The CCG is required to maintain a local warranted environment specification (WES). This should ensure hardware specifications meet the above requirements and should include the locally agreed infrastructure lifecycle to facilitate a systematic refresh and replacement programme.

GP IT capital and other sources of non-recurrent funds can be used to provide and refresh the necessary IT infrastructure.

IT infrastructure requirements created through the expansion and development of the GP Estate should be factored into the business planning process for the estate development. Growth of workforce and practice activity should also be allowed for. Appropriate NHS capital sources such as Estates and Technology Transformation Fund (ETTF) whilst available may be used to support these developments.

Individual practice IT reviews should include discussions on possible practice service and estate developments which may increase demands on the existing IT infrastructure. IT hardware may also attract recurrent costs which are likely to align with the volume of the IT hardware estate for example operating system and anti-virus licences, GP IT support contracts. Whenever possible GP IT Support contracts should include a tolerance which allows for organic growth of the GP IT estate without the requirement to renegotiate support costs.

8.3 Challenge 3: Enabling service improvement, transformation and digital innovation

Digital Technology to improve efficiency and enable transformation

Supporting GPs, PCNs and CCGs locally prioritise and invest in technologies which improve practice efficiency and enable local service transformation. Those capabilities described in this Operating Model as Core and Mandatory must be first priority to provide through the use of local allocations of funds as these capabilities are essential for general practice contractors to meet their GP contract obligations.

There are a number of digital capabilities described in this Operating Model as enhanced which enable general practice service improvement, efficiency and transformed care. This does not mean these capabilities are of less importance. Local investment in the right digital enablers for service improvement can improve patient outcomes and experience within a stable and efficient service.

Digital technologies and systems when commissioned for practices should whenever possible be accompanied by the availability of regular utilisation data.

8.3.1 Supporting the commitment to deliver a Net Zero NHS

The Delivering a 'Net Zero' NHS report published in October 2020 sets out ambitions to respond to climate change and improve the health of the nation, by becoming the world's first 'net zero carbon' national healthcare system. Two clear targets have been set, with short-term ambitions:

- for the emissions we control directly (the NHS Carbon Footprint), net zero by 2040, with an ambition to reach an 80% reduction by 2028 to 2032
- for the emissions we can influence (our NHS Carbon Footprint Plus), net zero by 2045, with an ambition to reach an 80% reduction by 2036 to 2039

NHSE/I will published an updated Green Plan Guidance document in 2021, detailing the framework and approach to help guide the creation and updating of these plans.

This Operating Model supports this commitment. The NHS Net Zero report includes a number of early priorities for carbon reduction, including for primary care services:

- use digital technology to reduce carbon emissions in general practice including:
  - reducing staff and patient travel with digital consultations and monitoring
  - rationalising estate requirements/usage (approximately 9,000 buildings)
  - continuing progress to a paper free environment for patient records and transactions
  - increased use of digital tools for peer-to-peer communications
- invest in and deploy GP IT infrastructure which minimises energy usage including (i) power saving on IT devices (ii) optimizing equipment life cycle (for example with Virtual Desktop Indicator (VDI)) to reduce manufacturing energy costs
- ensure adherence to policy advice which will be issued to ensure NHS data centres and companies providing these services as part of the Managed GP IT Infrastructure minimise their environmental impact and support the drive to reach Net Zero

As the NHS progresses along a net zero trajectory specific targets and requirements will develop which future Operating Model releases will reflect.

8.4 Challenge 4: Supporting new models of care and contracts

Support for the PCN DES and Integrated Care Systems

The CCG-Practice Agreement provides clarity on eligibility and assurance to both parties on the requirements for the provision of and use of digital services provided to general practices under this Operating Model.

8.4.1 Primary Care Networks (PCN)

The five-year framework for GP contract reform to implement The NHS Long Term Plan introduced PCNs through a Direct Enhanced Service (DES). PCN Staff as part of the contracted delivery will be supported under this Operating Model. It is expected that the PCN staff will continue to use the Foundation Digital Capabilities for general practice provided under the GP IT Futures Framework although new (enhanced) capabilities may develop as these services become established. GP IT Enabling Requirements will support PCN staff in the same way as existing practice staff. PCN IT requirements should be treated and managed in alignment with the management of GP IT services. Funding for PCN staff IT needs are now incorporated within core GP IT revenue and GP IT business as usual capital funding. Where PCN services are provided through a commissioned third party provider the requirements for sub-contracting of services by practices must be met.

8.4.2 Sub-contracting of services by practices

Practices will be eligible for receipt of NHS funded digital services as described in this Operating Model where they hold a GP Contract and have signed a CCG-Practice Agreement. Some practices may choose to sub-contract certain services to specialist providers, providing the conditions for sub-contracting of clinical matters under the GP Contract are met. Examples include:

- GP Federations and similar collaborative organisational arrangements set up as discrete organisational forms to provide services to general practice contractors
- specialist private providers contracted to deliver online digital services to the practice
- PCN services provided by a third party organisation

Note: this does not apply to a contract for services with a healthcare professional for the provision of clinical services personally by that professional.

In all cases it is the practice as the contractor and not the sub-contracted provider who is eligible to receive NHS GP digital services and the CCG is not obliged to provide such services to the sub-contracted provider. GP IT funds are not directly available to sub-contracted providers. Sub-contracting of services may however enable practices to innovate and achieve significant efficiencies.

The practice may inform the CCG that its sub-contracted provider requires access to use certain services provided to the practice under this Operating Model. The CCG may agree, not to be unreasonably withheld, to provide this access. In doing so the CCG should secure assurance that the cost of providing the services to this practice is proportionate to other similar GP Contracts they support (based on a cost per registered patient basis) and that controls are in place to ensure compliance with relevant standards as required in this Operating Model including those relating to patient safety, data quality, information governance and cyber security.

Where the sub-contracted provider uses digital systems to provide services to the practice, whether these are provided by the CCG, the practice or the provider directly, the practice must take reasonable steps (contractually if possible) to ensure relevant standards as described in this Operating Model are applied particularly in respect of patient safety, data quality, information governance and cyber security.

The sub-contracted provider may use their own digital systems and IT infrastructure providing:

- the practice as GP Contract holder complies with the CCG-Practice Agreement and with its GP Contract obligations, including use of an accredited clinical records system and use of certain National Digital Services
- no digital system or IT equipment owned or managed by the sub-contracted provider is connected to the Managed GP IT Infrastructure in the practice without explicit approval from the CCG
- the systems and infrastructure meet the standards required in this Operating Model. Use of the Digital Care Services (DCS) Catalogue and other applicable frameworks (see Appendix C), is recommended

Appropriate data processing agreements which comply with GDPR (article 28) must also be in place between the practice as Controller and the sub-contracted provider as Processor.

The GP contract gives clear direction on restrictions on advertising and hosting private GP services. These restrictions apply to the use of digital services provided by the NHS to practices under this Operating Model.

Where a provider is a sub-contractor for a number of individual general practices with these practices commissioned by different CCGs and the relevant CCGs have agreed with their practices to support this provider (as described above) with access to the practice digital services, the CCGs involved are advised to consider, if appropriate, a collaborative approach (for example through a lead CCG) to ensure efficiency and effectiveness in the service and avoid duplication of funding. CCGs must ensure in such circumstances that other practices, for which the CCG has IT responsibilities, are not disadvantaged.

8.5 Challenge 5: Supporting general practice meet patients' digital expectations

Focus on the GP Contract patient facing digital commitments

8.5.1 Patient Facing Digital Capabilities

Practices are required to offer a number of patient facing digital capabilities:

- repeat prescription requesting
- appointment requesting
- viewing patient record
- update patient record
- update patient details

- online consultations (patient-practice)
- video consultations (patient-practice)
- two way secure written (text) communications (patient-practice)

These capabilities, which are core and mandated under this Operating Model, will be available through either accredited solutions from the Digital Care Services (DCS) Catalogue (including the GP IT Futures and DFOCVC Frameworks) or the NHS App and other accredited solutions. Foundation Solution suppliers may choose to embed these capabilities in their Foundation Solution. Additional solutions to meet these capabilities may also be commissioned centrally and made available directly to practice patients subject to accredited interoperability with the practice choice of Foundation Solution.

GP online and video consultation capabilities are now a core and mandated capability (to align with the GP Contract).

Additional Patient Facing digital capabilities may be provided for practices as Enhanced Services to meet local needs.

Practices are encouraged to use Advanced Telephony Services, a significant benefit of which is an improved patient experience particularly during peak demand periods for telephone access. A template specification to assist practices (and supporting CCGs) to procure advanced telephony services is attached to Appendix E.

8.6 Challenge 6: Building on success and learning lessons

Recognising and building on success of GP Systems, GPSOC Framework and previous Operating Models.

In updating the Operating Model NHS England has, with the support of the profession, considered the following:

- The GP Systems of Choice (GPSoC) Framework, the previous Operating Models and their preceding arrangements have, with strong clinical engagement and contractual levers, been successful in developing highly digitised general practice with a large percentage of paper free processes. We must build on this success.
- the GP Contract continues to make a number of obligations and recommendations regarding digital services on the NHS and GP contractors
- general practice leads the NHS in the adoption of patient facing digital systems

The approach taken has therefore been to:

- continue to retain much of the preceding Operating Model principles and approach – streamlining and enhancing to make it easier to use, more comprehensive and more relevant.

- utilise standards to ensure the benefits of consistency from a single national framework are retained
- retain and build on functional capability-based requirements categorised by digital maturity and “must do” or “enhanced” provision.
- build on existing key controls (contracts, agreements, standards, directives, guidance, assurance)
- reflect on and adapt to significant national events and changes and trends in service improvement and transformation

8.6.1 Covid-19 Pandemic Response Lessons Learned

Just as the previous Operating Model incorporated lessons learned from the Wannacry global cyber incident in 2017, this Operating Model takes account of the significant lessons learned from the Covid-19 response during 2020-21. To date these include

- the need for greater resilience in supporting flexible working practices in particular secure remote and home working
- the success of alternative to face-to-face channels for triage and consultation including online, telephone, video. An RCGP snapshot survey (July 2020) indicated an increase in telephone and video consultations during this period and a recognition from respondents of the efficiency benefits of telephone, video and digital triage and consultation:
  - a capability to rapidly scale up any patient/public communication channel as determined by circumstances (for example text messaging).
  - using technology to manage peaks in demand on practices, for example using online solutions and advanced telephony
  - a capability to rapidly exploit national patient facing services such as NHS App and NHS login
  - the value of wider clinical access to appropriate content in the primary care patient record through the enhanced Summary Care Record (with additional information) and the use of GP Connect Products is now recognised and evidenced
  - a requirement for effective tracking of NHS IT assets when supporting remote, outreach and home working

9. Transition Arrangements and Timescales

The following describes the significant transition arrangements arising from the release of version 5 of the Operating Model. More detailed transition actions are given against individual capabilities documented in Appendix A.

Topic	Transition Action	Timescale
Changes to GP IT Enabling Requirements	Where the requirements have changed since the previous Operating Model (2019 V4). CCGs should agree a plan with their commissioned GP IT Delivery Partner for these changes to be effective in the services provided within the NHS financial year during which the Operating Model is published, unless otherwise specified against that individual requirement for example where there is an urgency or time pressure for the change to be effective.	Within Financial Year of Operating Model Publication
Resilience and practice Business Continuity Plans.	CCGs must review all practice BCPs with particular reference to Covid-19 lessons learned	By 31 July 2022
GP Telephony	GP Telephony remains a practice business responsibility. CCGs should encourage, practices to migrate to an Advanced GP Telephony solution and provide technical advice, for example on network infrastructure.	From April 2021
Remote Working	CCGs must review all supported remote working solutions, with particular reference to temporary arrangements deployed during the Covid-19 Response period. Any temporary arrangements which do not meet the standards described in this Operating Model must be decommissioned by 31 August 2022	By 31 August 2022
Local Clinical Servers	Local Hosting of GP Clinical Systems is not supported after 31 March 2021. CCGs must ensure any legacy/residual clinical system servers for local hosting are identified and decommissioned by 31 August 2022.	By 31 August 2022
Microsoft Office 365 for the NHS	Participating CCGS must fully implement all elements of Microsoft Office 365 for the NHS required for general practices by no later than 13 October 2021 in accordance with the Microsoft Office 365 for the NHS Participation Agreement. The agreement will then run until 30 April 2023.	By 13 October 2021
Microsoft Office 365 for the NHS	CCGs should start planning for the impact on Office application use in practices after 30 April 2023 when the current NHS participation Agreement ends. These plans should reflect NHS policy and guidance as it becomes available.	By 31 July 2022
Cyber Essentials	Commissioned GP IT provider organisation(s) will be accredited to Cyber Essentials Plus (CE+)	

Online and Video Consultation Systems	CCGs are expected to have local contracts in place for online consultation systems and video consultation systems.	By 1st April 2021
SMS and Prescribing	Where SMS (or other digital messaging) is used to replace paper tokens for non-nominated prescriptions these must comply with the approved digital token definition SMS (or other digital messaging) will also support secure written communications between patients, carers and the practice	By 1st April 2021
NHS Smartcards	Deprecation of old NHS Smartcards: To remove all series, 3, 4, 5 and 6 NHS Smartcards	By March 2023
PCN Enhanced Access	CCGs will work with PCNs and practices in the development of their proposed Enhanced Access Plans. This should include identifying areas in the existing digital infrastructure and systems (including telephony) which will require development and/or investment.	By 31 July 2022

APPENDIX A – Schedule of GP Digital Requirements and Capabilities

Essential Clinical System Capabilities – Foundation Capabilities

Six clinical digital capabilities enabled through software (and data) solutions which under the GP Contract are necessary to deliver primary care services and must be accredited through the GP IT Futures Framework. These are sourced through the GP IT Futures Framework.

For these capabilities, where a signed CCG-Practice Agreement is in place

- the solutions are funded by the NHS for GP Contract holders
- the solution must be accredited through the GP IT Futures Framework
- the Foundation Solutions for those capabilities described as GP IT Futures Foundation Capabilities will be determined by individual practice from the accredited systems available through the GP IT Futures Framework

Note: Non-Foundation Capabilities may be provided as an embedded part of the procured Foundation Solution at the supplier's discretion. CCGs should determine which non-Foundation Capabilities are still required once the Foundation Solutions have been procured. Additional solutions for these capabilities may still be available and may be selected as enhanced items if they offer a greater level of functionality and more appropriately meet local needs.

Foundation Capabilities available through GP IT Futures Framework

Capability	Description
GP Referral Management	Supports recording, reviewing, sending, and reporting of patient referrals. Enables referral information to be included in the Patient Record.
Prescribing	Supports the effective and safe prescribing of medical products and appliances to Patients. Information to support prescribing will be available.
Recording Consultations	Supports the standardised recording of consultations and other General Practice activities.
Patient Information Maintenance	Supports the registration of patients and the maintenance of all patient personal information. Supports the organisation and presentation of a comprehensive Patient Record. Also supports the management of related persons and configuring access to citizen services.
GP Resource Management	Supports the management and reporting of Practice information, resources, staff members and related

	organisations. Also enables management of staff member availability and inactivity.
Appointments management – GP	Supports the administration, scheduling, resourcing and reporting of appointments.

Essential Clinical System Capabilities – Non-Foundation Capabilities

Clinical digital capabilities enabled through software (and data) solutions which are necessary to deliver primary care services under the GP Contract or as otherwise nationally mandated in addition to the six Foundation Capabilities.
These are sourced through the Digital Care Services (DCS) Catalogue or an applicable Framework (see table below and Appendix C).

For these capabilities, where a signed CCG-Practice Agreement is in place:

- the solutions are funded by the NHS for GP Contract holders
- solutions will be determined by the commissioning CCG in collaboration with local practices from systems offered on frameworks in the DCS Catalogue or other applicable frameworks
- non-Foundation Capabilities may be provided as an embedded part of the procured Foundation Solution at the supplier's discretion. CCGs should determine which non-Foundation Capabilities are still required once the Foundation Solutions have been procured. Additional solutions for these capabilities may still be available and may be selected as enhanced items if they offer a greater level of functionality and more appropriately meet local need.

Accredited solutions are not contractually mandated for non-Foundation Capabilities but compliance with any standards attributed to the capability in this document should be considered essential.

Non-Foundation Capabilities available through Applicable Frameworks

Capability	Description	Applicable Framework(s)
Digital Diagnostics	Supports electronic requesting with other healthcare organisations. Test results can be received, reviewed and stored against the patient record. NB: this is additional to the pathology messaging already	GP IT Futures or other applicable framework

	available through Foundation Capabilities.	
Document Management	Supports the secure management and classification of all forms unstructured electronic documents including those created by scanning paper documents. Also enables processing of documents and matching documents with patients.	GP IT Futures or other applicable framework
GP Extracts Verification	Aggregated data is extracted from practice Clinical Systems via the General Practice Extraction Service (GPES) and sent to the Calculating Quality Reporting Service (CQRS). Calculations performed by the CQRS determine how much money a general practice should be paid for National Services. The data extracted in this process is based on information recorded in individual patient records. The GP Extracts Verification Capability provides practices with reports and search tools to establish which patients will be or have/have not been included in these payment extracts and calculations. These reports and tools will ultimately support data quality investigations and improvements.	GP IT Futures or other applicable framework
Scanning	Support the conversion of paper documentation into digital format preserving the document quality and structure. Note: Requires as an enabler compatible scanning hardware.	GP IT Futures or other applicable framework

Communication Management (patient-practice)	Supports the delivery and management of (two way written) communications between patients and practice staff. Note: May require as an enabler electronic messaging for direct patient communication (for example SMS) or NHS Mail.	GP IT Futures or other applicable framework
Online-consultations (patient-practice)	Enables patients to access support from health and care professionals, across a range of settings online without the need for a face to face encounter. Includes triage and consultations. Note: This may also fulfil the above requirement for communications.	DFOCVC framework
Video consultations (patient-practice)	Enables patients to access support from health and care professionals, across a range of settings using video conferencing. Includes triage and consultations.	DFOCVC framework

Patient Facing Capabilities

These must be available to patients through accredited solutions from the GP IT Futures Framework and through the NHS App. Foundation Solution suppliers may choose to embed these capabilities in their Foundation Solution.
Additional accredited solutions to meet these capabilities may also be commissioned centrally and made available directly to practice patients or commissioned locally.

Capability	Description
Appointments Management	Enables patients to manage their appointments online. Supports the use of Appointment slots that have been configured in the GP appointments management system
Prescription Ordering	Enables patients to request medication online and to manage their preferred and nominated pharmacy.
View Record	Enables patients to view their patient record online. Includes viewing of full record, clinical and administrative documents and pathology and radiology test results by patients and patient proxy.
Update Details	Enables patients to use an online method to inform their practice of a change of address, contact details or of their demographic information, including ethnicity
Update Record	Shared record access, including patients being able to add to their record

These capabilities are in addition to the online and video consultation and the two way secure communication capabilities described previously.

National Digital Services

Digital services and systems commissioned and provided nationally and available at no local cost to all NHS commissioned providers (where functionally appropriate). These are standard solutions with no element of local choice, the rationale for a national solution being based on a requirement for standardisation and consistency. Local alternatives should not be provided or used.

Responsibilities:

- NHS Digital commissions and provides a number of National Digital Services.
- CCGs will ensure availability of enablers namely infrastructure, equipment, training and deployment support for practices.
- alternatives including local solutions should not be used and should not be funded by CCGs. In particular local solutions which do not meet the same security, safety and data quality standards must not be supported.
- through the CCG-Practice Agreement practices are required to comply with the supplier's end-user terms and conditions accepted by the contract holder (for example NHS Digital).
- practices will use either as discrete systems or integrated with clinical systems as appropriate

Accredited clinical system developers will integrate with these as specified through the Digital Care Services (DCS) Catalogue.

Service	Description	Notes
Personal Demographics Service (PDS)	The Personal Demographic Service (PDS) holds the demographic details of users of health and care services in England, including name, address and NHS number. It is used to confirm the identity of patients, link care records, support communications with patients and support management of NHS Services.	Accessed through accredited Clinical System Capabilities.
Care Identity Service – (CIS)	CIS is a national electronic system that supports the identity verification of users, registering and issuing of NHS Smartcards and authentication when using national services such as PDS or SCR. Registration Authorities use the service to manage	Through NHS Spine Portal using Registration Authority issued NHS Smartcards.

	identities, Role-based access control (RBAC) and smartcard or other authenticator access to services.	
NHS Care Identity Service 2 – (CIS2)	The evolution of the Care Identity Service. It will support international standards for authentication and access (including authentication over the internet and new authenticator types). Users will be able to undertake self-service registration to aid new user onboarding journeys. CIS2 is a national electronic system that supports the identity verification of users, registering and issuing of NHS Smartcards and other authenticators Registration Authorities use the service to manage identities, RBAC and smartcard or other authenticator access to services.	Through NHS Spine Portal using Registration Authority issued NHS Smartcards.
Summary Care Record (SCR)	An electronic record created from GP medical records. It can be seen and used by authorised staff in other areas of the health and care system involved in the patient's direct care. There is a minimum core data set (medications, allergies and adverse reactions) but with patient consent, an enhanced SCR can now be created automatically to include additional patient data (for example significant medical history, immunisations, etc.).	Accessed through accredited Clinical System Capabilities.
GP2GP	This service allows patient electronic health records to be transferred directly, securely, and quickly between their old and new practices when they change GPs. This improves patient care by making full and detailed medical records	Accessed through accredited Clinical System Capabilities.

	available to practices, for a new patient's first and later consultations and significantly reduces the need to print records.	
Electronic Prescribing Service (EPS)	Enables the electronic transmission of prescriptions to community pharmacies.	Accessed through accredited Clinical System Capabilities.
NHS Mail	NHS Mail is the secure email service approved by the Department of Health and Social Care for sharing patient identifiable and sensitive information. NHS Mail, messaging, and sharing can be accessed by any organisation commissioned to deliver NHS healthcare or related activities. Instant messaging and presence are part of core functionality.	Directly by individual practice staff members through the NHS Mail portal or MS Outlook configured to access NHS Mail.
NHS E-Referral Service (e-RS)	The e-RS combines electronic booking with a choice of place, date and time for first hospital or clinic appointments. Patients can choose their initial hospital or clinic appointment, book it in the GP surgery at the point of referral, or later at home on the phone or online.	Accessed through accredited Clinical System Capabilities or directly.
Calculating Quality Reporting Service (CQRS) and GP Extraction Service (GPES)	The General Practice Extraction Service (GPES) collects information for a wide range of purposes, including providing GP payments. It works with the CQRS and GP clinical systems as part of the GP Collections service.	Accessed through accredited Clinical System Capabilities.
Spine	The spine allows information to be stored and shared securely through national services such as the EPS, SCR and the eRS. This is done through integrated clinical system or through the spine portal. The Spine supports high number of registered users and can handle large volume messaging rates with fast response times.	Accessed through accredited Clinical System Capabilities.

Message Exchange for Social and Health Care (MESH)	The service supports both clinical and business encrypted data flows in supplier applications via a central MESH server located within the Spine Core Messaging Service.	Accessed through accredited Clinical System Capabilities.
GP Connect Products (delivered by Direct Care APIs Programme)	GP Connect products are a series of APIs which allow authorised clinical staff to share and view GP practice clinical information and data between IT systems, quickly and efficiently.	Accessed through GP IT Futures accredited clinical system capabilities and other third-party clinical systems
Interface Mechanism (IM1) Pairing	Pairing integration is the process that allows suppliers to integrate their system with any principal GP clinical system through an interface mechanism.	Accessed through GP IT Futures accredited clinical system capabilities and other third-party clinical systems
NHS App	The NHS App provides a simple and secure way for people to access a range of NHS services on their smartphone or tablet including: symptom checking urgent help (NHS 111) book and manage GP appointments order repeat prescriptions. view their medical record register as an organ donor. choice on use of their data by NHS a gateway to access new digital services as available.	Directly by patient. If their GP practice is connected, patients can register and verify their identity. The NHS App is available to the public on Google Play and Apple app stores.
NHS Login	NHS login, a single, easy to use system for verifying the identity of people who request access to digital health records and services including NHS App.	Directly by patient. Most people aged 16 or over will be able to verify their identity and register through NHS login.
Data Security and Protection Toolkit (DSPT)	The DSPT is an online self-assessment tool that all organisations must use if they have access to NHS patient data and systems. It replaced the previous Information Governance (IG) toolkit. An online self-assessment tool	Directly by individual practices.

	that enables practices to measure and publish their performance against the National Data Guardian's (NDG) ten data security standards.	
Data Security Awareness Training	The topics covered are: • introduction to data security awareness • introduction to the law • data security - protecting information • breaches and incidents	Directly online by individual practice staff members through e-learning for healthcare.

GP IT Enabling Requirements

Digital technologies and services necessary to support (ie enable the use of) National Digital Services, Foundation Solutions and other solutions selected to meet the Essential Clinical System Capabilities as needed to deliver the primary care services under the GP Contract or as otherwise nationally mandated. Under the CCG-Practice Agreement these are funded by NHS for eligible contractors.

Unless funded nationally, meeting these enabling requirements will be the first call on GP IT revenue funding within CCG primary care allocations, or for IT equipment and infrastructure assets on GP IT Capital funds. The scope of the enabling requirements required is determined by the solutions selected to meet the Essential Clinical System Capabilities and the National Digital Services.

Locally commissioned enabling requirements will be extended to include the support necessary to enable those Enhanced Requirements commissioned.

As commissioner the CCG is responsible for selecting these enabling requirements but is expected to work with local practices in doing this.

Accredited solutions are not contractually mandated but compliance with any standards attributed to the capability in this document should be considered essential. The use of an applicable national framework with underpinning standards such as Health Services Support Framework (HSSF) (see Appendix C) will assist CCGs in that compliance.

Effective Commissioning of GP IT

Requirement	The commissioning of GP IT services by the CCG to meet GP IT Enabling Requirements. This is an internal CCG function, although CCGs may share or collaborate on this work.
Specialist Support Services	The CCG-Practice Agreement: • must be signed with all practices • must be reviewed in the event of significant changes to either party for example organisation merger • appendix 1 schedules require review not less than every 12 months • references (for example as links) to be provided to data processing agreements in appendix 1 schedules GP IT commissioned (enabling) services: • must meet required organisational standards • must be procured to required standards (for example SFIs) • should be subject to regular service review of performance and suitability for requirements of local general practice

	CCGs will have a budgeted plan for annual investment meeting the Core and Mandated Requirements and the Enhanced Requirements for GP IT – this should include GP IT enabling services, infrastructure and equipment.
Practice Responsibilities	To sign and comply with the CCG-Practice Agreement
Applicable Standards	Where GP IT services are commissioned and contracted, there will be: • robust and clear service specifications demonstrating alignment with this schedule of requirements • formal SLAs in place • identified and agreed KPIs • regular performance reviews • issue management and escalation arrangements agreed and clearly documented • formal complaints management procedure • a communication plan regarding the services provided through this Operating Model for all practices • a Data Processing Agreement (DPA) where required • compliance with the organisational standards referenced in this document The use of a suitable framework with underpinning standards such as Health Services Support Framework (HSSF) (see Appendix C) is recommended. As required under the CCG-Practice Agreement: • carry out practice IT reviews • where local IT and system performance issues should be identified, individual practices can request an additional service and infrastructure review
Applicable Guidance	CCGs are advised to use the GP IT Specification Commissioning Support Pack in the procurement of GP IT services and in the ongoing review of GP IT services with current GP IT Delivery Partners.
Other Controls	Where CCGs choose to provide some or all of these GP IT Enabling Requirements internally, whether solely, as a CCG consortium or as a local shared service, CCGs must enable sufficient arrangements and safeguards to ensure the services provided meet the range and standards described in this Operating Model.
Assurance	DPCMAT: IND20.0, IND21.1, IND24.0, IND150.1, IND150.2, IND155.0, IND157.0, IND174.1

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 must have clear and agreed priority incident categories, with minimum response and target fix times to ensure the safe and effective operation of GP digital services. • All calls are prioritised to the agreed standard, in conjunction with the person reporting the incident. A minimum standard should be agreed for percentage of incidents resolved on first contact or within an agreed timeframe from call logging.

	• 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 through the Summary of Services (Appendix 1) in the CCG-Practice Agreement. • Where 3rd party support is not available for required incident or problem management for example 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 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 GP IT Delivery Partner'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
Applicable Guidance	• Recommendation: The local SLA is based upon an agreed managed IT device volume
Assurance	DPCMAT: IND28.0, IND26.0, IND90.1

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	All disposal must be carried out by authorised contracted specialist IT hardware disposal organisations (meeting standards listed below). Develop and maintain a local IT equipment reuse and disposal policy.
Systems and applications	Software, browsers and operating systems not supported or maintained by the supplier must not be used on NHS owned GP IT equipment.
Practice Responsibilities	To provide consumables for example 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 are met for example air-conditioning, 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.
Applicable Standards	• Waste Electrical and Electronic Equipment (WEEE) Regulations (2013). • NDG standard 8

	• A local IT equipment re-use and disposal policy is required.
Other Controls	• General Data Protection Regulation (GDPR) • Data Protection Act 2018
Assurance	DPCMAT: IND36.0, IND38.0

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: • allocation and control of available 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 Windows 10 and Advanced 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 and browser compliant with the local WES. Specific software requirements: • software, browsers and operating systems not supported or maintained by the supplier must not be used on NHS owned or managed IT equipment • anti-virus software for example ATP • encryption software • effective patch and upgrade management for operating systems • 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
Applicable Guidance	Respond to an NHS cyber alert service (formerly Care CERT)
Assurance	DPCMAT: IND37.1
Timescales	Participating CCGs must fully implement all elements of Microsoft Office 365 for the NHS licencing for general practices by no later than 13 October 2021 in accordance with the Microsoft Office 365 for the NHS Participation Agreement. The agreement will then run until 30 April 2023. CCGs should start planning for the impact on Office application use in practices after 30 April 2023 when the current NHS participation Agreement ends. These plans should reflect NHS policy and guidance as it becomes available.

Registration Authority

Requirement	A Registration Authority is a function, usually within an NHS organisation, that carries out the identity checks of prospective NHS 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 the Registration Authority function will continue to support issuance of approved alternatives. Given the standards basis of these authenticators it is likely that they will place a greater emphasis on the user behaviour when using the authenticator, ie users will need to closely manage how they use their authenticator and log out of sessions when leaving a PC unattended. Ensure general practices are aware of their obligations under the Care Record Guarantee to protect patient data, and not leave sessions unattended.
Transactional Support Services	Availability: Operational Support Hours: • unlocking of NHS 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 service 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 and 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 NHS 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 for software to access national systems for example Identity Agent, CIS, CIS2 • 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 • support the new Self Service Registration process – allowing new users to self-register in their own time saving clinical and RA time • utilise the new improved User Registration Service. This will aide workflow, integration with other services and improved RA reporting and capabilities
Systems and applications	Identity Agent. CIS CIS2
Practice Responsibilities	• practices are responsible for determining which practice staff and other organisation staff can access practice data and system functions, and the (system) role of that staff member, through the Registration Authority process • practice 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 • ensure practice staff are aware of their obligations under the Care Record Guarantee to protect patient data, and not leave sessions unattended. As new authentication technology arrives for use, particularly with new market entrants there will need to be a re-emphasis on training and awareness of how to use new authenticators and the risks when users don't manage sessions appropriately
Applicable Standards	• National Registration Authority Policy • NDG Standard 4

	• Only accredited providers can provide this service
Applicable Guidance	• Registration Authority Operations and Process Guidance • Registration authority governance

NHS Mail Administration and Support

Requirement	The local administration of NHS Mail accounts. NHS Mail is provided to all practices as a National Digital Service.
Out of Scope	National NHS Mail Service Desk. Support for email solutions other than NHS Mail.
Transactional Support Services	Availability - Standard Service Hours: • creation and 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
Practice Responsibilities	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 practice staff member leaves the practice. Practices will have at least one securely managed and frequently monitored (at least once daily) NHS Mail account to receive clinical documentation. Practices should ensure practice staff follow NHS Mail Acceptable use Policy and advice on cyber security in their use of NHS Mail e.g. phishing, 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.
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)

Essential Infrastructure

Requirement	The provision, maintenance and technical support of the necessary infrastructure to deliver core and mandated GP IT services
Out of Scope	HSCN-GP WiFi-GP
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 and 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 Digital Care Services (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 cloud hosting services, 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 Recovery Point Objective (RPO) • where practices choose to use VoIP telephony CCGs should provide advice and technical support regarding the use of practice network infrastructure and if applicable HSCN connections. Individual practices remain responsible for the cost of their telephony services including any additional infrastructure costs
Practice Responsibilities	See General Practice Business Requirements Appropriate use of the infrastructure in compliance with the CCG-Practice Agreement.
Applicable Standards	• the GP IT Delivery Partner and any subsidiary service or infrastructure provider will operate to any prevailing NHS security standards, including the Data Security and Protection Toolkit or equivalent industry standard • tier 3 data centre
Applicable Guidance	• NHS and social care data: off-shoring and the use of public cloud services guidance – NHS Digital • NHSE/I Green Plan Guidance document • GP Advanced Telephony Specification Commissioning Support Pack
Other Controls	• HSCN connection agreements
Assurance	DPCMAT: IND39.2

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 (HSCN Consumer Network Service Provider) • break / Fix incident and problem resolution
Specialist Support Services	Availability: Standard Service Hours • commissioning of HSCN services for practices • NHS Digital provides a central service coordination function to monitor CN-SP and network performance and coordinate response to high severity service issues.
Infrastructure	• HSCN is the essential underlying network infrastructure that underpins the use of digital technology in the NHS • networking services: Management and support for provision of HSCN connectivity and interim legacy Transition Network services, including connections to main and branch practice sites as per national entitlement • the HSCN 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 and filters 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 to the NHS Digital Data Security Centre • 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 for example 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 for example 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 and rely on HSCN for backup telecoms connectivity
Practice Responsibilities	Ensure their practice is covered by an HSCN Connection Agreement signed on their behalf by the appropriate CCG.
Applicable Standards	• HSCN consumer handbook • the standards for HSCN suppliers known as Consumer Network Service Providers (CN-SPs) o HSCN Compliance Operating Model o HSCN Mandatory Supplemental Terms
Applicable Guidance	• HSCN compliance • HSCN overlays • HSCN Connectivity Options • HSCN Technical Guidance Further information: hscnenquiries@nhsdigital.nhs.uk • GP Advanced Telephony Specification Commissioning Support Pack

Other Controls	• HSCN customer Connection Agreements • Consumer Network Service Providers (CN-SP) Compliance documents required by NHS Digital • Local contracts between commissioners such as CCGs and CN-SPs • If shared, local arrangements with partners (e.g. support and any associated funding)
Service Availability	99.95% minimum availability (as per ISO 27001)
Assurance	Suppliers of HSCN services (Consumer Network Service Providers, CN-SP) are assured and accredited by NHS Digital as being compliant with HSCN standards. The CN-SP has to demonstrate that the network solution provided to the consumer is correctly configured and allows the appropriate routing and to the agreed HSCN end points and supplies the agreed capacity to the HSCN Consumer. It is important that access to any national and local applications used by a site are identified and tested as part of migration.

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 Managed GP IT 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 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. Such equipment should be available subject to availability of funds, and reasonable and fair practice use. Equipment required specifically for diagnostic or treatment purposes for example 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 devices (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 for example 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 Managed GP IT 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 which identifies and replaces hardware subject to availability of funds where it has reached its service life. • GP IT Equipment would be expected to be funded through NHS Capital funds, although CCGs are free to use other appropriate funding sources • 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 • the refresh service will include assessment, procurement, rollout, asset tracking and secure disposal (see above) • 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 (for example with Virtual

	Desktop Infrastructure (VDI)) to reduce manufacturing energy costs
Systems and applications	• software, browsers and operating systems not supported or maintained by the supplier must not be used on NHS managed 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)
Practice Responsibilities	• to provide consumables e.g. for printers and other operating requirements to equipment manufacturer's standard or to any standard specified in the local Warranted Environment Specification • software, browsers and operating systems not supported or maintained by the supplier must not be used on NHS managed infrastructure • to ensure the physical security, protecting against loss, theft or damage and power supplies for NHS Owned IT equipment on practice premises
Applicable Standards	• NDG Standard 8. • Information Security Management: NHS Code of Practice • NHS Digital: Data Security Standard 9: IT Protection • Spine WES
Applicable Guidance	• Respond to an NHS cyber alert service (formerly Care CERT) • NHSE/I Green Plan Guidance document • Recommendation: A local SLA should be based upon an agreed desktop estate volume
Assurance	DPCMAT: IND14.0, IND15.0, IND34.0, IND58.0

WiFi-GP

Requirement	Secure, stable, and reliable WiFi access for practice 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. Practice 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 and 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: • a secure, stable, and reliable WiFi capability within practices • 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 Solutions and NHS national systems There is compliance with NHS data security and protection requirements, including appropriate content filtering.
Systems and applications	• software, browsers and operating systems not supported or maintained by the supplier or unsupported devices must not be used to access the “corporate” WiFi-GP network in the practice • a WiFi landing page
Applicable Standards	• technical Policies and Guidance • locally agreed Acceptable Use Policies must be in place which should cover all the wireless network services provided, including Guest and Bring Your Own Device arrangements
Applicable Guidance	• technical Policies and Guidance
Other Controls	• local contracts with commissioners such as CCGs

Assurance	DPCMAT: IND171.0

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 for example email. This includes any necessary mobile and remote access IT infrastructure. The options for remote access are described below. To support resilience and business continuity requirements the service(s) provided should be available to support at least 60% of normal operational capacity working remotely
Out of Scope	• any remote access solutions not part of the Managed GP IT Infrastructure • internet connectivity for example 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 and 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 Managed GP IT Devices are provided: • the use of mobile computing systems is controlled, monitored and audited to ensure their correct operation and to prevent unauthorised access, supporting Data Security Protection Toolkit (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: **Option 1** A Managed GP IT Device (for example laptop or desktop or other endpoint) with all software necessary for the role (as native application or in a Virtual Desktop Infrastructure (VDI) service) together with a means of secure VPN access and a smartcard reader. Where Managed GP IT Devices are 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 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 **Option 2** Using staff personal devices (also known as “Bring Your Own Device” – BYOD) Where personal devices/BYOD are used • a virtual desktop infrastructure (VDI) service will be provided allowing access to the Foundation Solution and other Essential Clinical System Capabilities as necessary

	with a means of secure VPN access and a smartcard reader • NHS applications approved for use over the public internet (for example 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 • 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 • a BYOD policy must be in place which includes cyber and data security, software licencing and ownership, data storage, support, data and security breaches, loss of device, and termination. 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 provided within the Digital Care Services (DCS) Catalogue Solutions, the National Digital Services and the Managed GP IT Infrastructure (including authentication using NHS Smartcard or any approved alternative/replacement). 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: • client software installed on the personal device or; • desktop sharing software (ie Remote Desktop Protocol (RDP) or equivalent) to remotely access a host device for example 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 infrastructure.

Practice Responsibilities	• compliance with NHS and local information security standards and policies • follow NHSE 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 • ensure remote digital access to patient details and online, telephone or video consultations take place in a confidential environment. Access to the digital equipment used for these functions is controlled • Health and Safety (including DSE, PAT and WTD) Regulations include remote and home working (see Practice Business Requirements)
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 • Using online consultations in primary care: implementation toolkit • Working safely with display screen equipment
Applicable Guidance	Recommendation: The local SLA is based upon an agreed mobile estate volume and/or number of remote access users.
Assurance	DPCMAT: IND33.4, IND33.5, IND33.6, IND33.7, IND33.8, IND33.9

Electronic messaging for direct patient communication

Requirement	Electronic messaging (SMS or equivalent) for direct patient communication. The ability for practices to communicate short messages to patients 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 test results Can support two-way secure electronic written (text) communication between patients and practices
Out of Scope	The use of electronic messaging for requirements other than above e.g. local surveys, is discretionary.
Transactional Support Services	Vendor via local helpdesk.
Systems and applications	Provision of electronic messaging functionality ie SMS messaging or equivalent, for direct 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 (see below) for electronic messaging. This may be provided as a shared activity across multiple practices.
Practice Responsibilities	Where electronic messaging is used to support the processing of Special Category (Sensitive) Data including two-way communications between patients and the practice a DPIA should be completed and regularly reviewed.
Other Controls	• 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

Assurance	DPCMAT: IND9.1

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 GP IT Equipment and Practice Managed GP IT Equipment which is not connected to the Managed GP IT Infrastructure e.g. 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 and laptops within the managed GP IT estate • provide practices with a facility to notify the GP IT Delivery Partner when practice 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 The CCG will ensure there is an accurate and contemporaneous record of the following: • IT hardware inventory and assets • software and software licences installed on devices within the managed IT estate • information systems namely applications and data • 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 for example 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.

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 and 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 Digital Care Services (DCS) Catalogue Solutions will be managed nationally, although these should be referenced as third party services in plans produced under this requirement.
Transactional Support Services	Availability - High Severity Incident Support: • GP IT support must include access for out of hours High Severity 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 • 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 immediately 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) all 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 premises, digital systems and equipment • the CCG and its commissioned GP IT Delivery Partner(s) will ensure full cooperation in 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
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 DSPT 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 for practice staff and operate a process to archive and disable these. Provide practices with a facility to notify the GP IT Delivery Partner when practice 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).

	CCGs must ensure there are appropriate governance arrangements for example policies, audits etc to provide assurance on the following: • administration access rights for Active Directory configuration and services relevant to the managed 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 management • administration access rights for Office 365 should align to those for Active Directory • administration Access rights for network configuration and equipment (for example 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 management • generic (ie not assigned to an individual) administrator accounts must not be used **Business continuity and Disaster Recovery Plans:** • CCGs must ensure organisations providing GP IT services are contractually required to 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 should 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 and 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:** • CCGs shall ensure business continuity plans are in place for all practices and are reviewed and approved as required under the CCG-Practice Agreement

- advice and guidance to support the development of the digital element of practice BC plans, will be 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 CCGs must 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

CCGs will ensure the commissioned GP IT Delivery Partner(s) 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:

- CCGs must ensure their commissioned GP IT Delivery Partner(s) have allocated senior level (e.g. director or equivalent) responsibility for cyber and data security within their organisation
- CCGs, as responsible commissioners of GP IT services, should have board level awareness of cyber security, including undertaking nationally recommended cyber security training
- eligible organisations are encouraged to make use of NHS Digital's Cyber Security Support Model services.

	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	• systems provided through Digital Care Services (DCS) Catalogue Frameworks have their own contracted service level specifications • National Digital Services have their own contracted service level specifications • 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 (for example NHS Smartcards). NCSC provides guidance on password managers
Practice Responsibilities	• 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 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 and 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 and guidance to support the development of the digital element of practice BCPs, will be available to practices when required • although fewer systems are now located within individual practice premises Business Continuity planning remains critical. 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
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 • GP IT enabling services must only be commissioned from organisations compliant with the following standards: o NHS Information Governance – to demonstrate satisfactory compliance as defined in the NHS Data Security and Protection Toolkit for the relevant organisation type. o accreditation to Cyber Essentials Plus (CE+). o accreditation to ISO 22301 for Business Continuity Management OR compliance with the NHS England Business Continuity Management Framework • and registered for: o NHS Digital Cyber Alert Service and High severity Cyber Alerts
Other Controls	• General Data Protection Regulation (GDPR) • Data Protection Act 2018 • Primary Medical Care Policy and Guidance Manual
Applicable Guidance	• National Cyber Security Centre (NCSC) password manager guidance • National Cyber Security Centre (NCSC) password manager applications guidance
Assurance	• DPCMAT: IND2.0, IND181.0, IND182.0, IND183.1, IND176.0

Information Governance Support

Requirement	Information governance support, guidance and advice to support practice compliance with common-law duty of confidence, records management, information security, Data Security and Protection Toolkit (DSPT), Data Protection Act 2018, GDPR 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 suppliers of GP digital services as data processor(s) • local CCG commissioned GP IT Delivery Partner as data processor AND as specialist support service to practice • local health and social care providers where data has been shared as data processors • any digital services supplier commissioned locally by the practice jointly or through a federation – as data processor CCGs will ensure practices are supported with: • 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 Data Security Protection Toolkit (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 CCGs will require commissioned GP IT Delivery Partners as data processors: • 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 personal data breaches in line with NHS guidance (using the incident reporting tool within the DSPT) and GDPR (article 33) 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 (DSPT) 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 GP IT Delivery Partner(s). **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 practice 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 **DPO Function** Availability of a named DPO, in addition to DPO support and advice for practices to designate as their Data Protection Officer. Practices may choose to make their own DPO arrangements, but CCGs are not expected to fund these if a DPO service has been offered by the CCG. **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 practice 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, Data Protection Impact Assessment (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

	• deployment of 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. **Data Processing Activities** 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 in accordance with the digital services acquired and will be regularly reviewed. **Supporting local procurement** • The use of the Digital Technology Assurance Criteria (DTAC) may be helpful in local procurement activities
Practice Responsibilities	Individual practices as contractors are responsible for: • report personal data breaches in line with NHS guidance (using the incident reporting tool within the DSPT) and GDPR (Article 33) where required, without undue delay and where feasible within 72 (actual) hours • managing data breaches and data breach near misses • communication of a “high risk” breach to individual patients as required under GDPR • 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 practice • 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 although CCGs are not expected to fund this if these services have already been offered • 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 • FOIA compliance • 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 practice staff to use workarounds which compromise data security • understand and comply with GDPR and Data Protection Act 2018 • mandatory compliance with the National Data Opt-Out policy Individual practices are responsible for sourcing any legal advice required to support these activities.

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 and comply with:
	  o Records Management Code of Practice 2020
	  o Code of practice on confidential information
	  o Information security management NHS code of practice
	• 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 Information Governance Resources • Patient Online Services in Primary Care - Good Practice Guidance on Identity Verification • Digital Technology Assurance Criteria (DTAC)
Other Controls	• General Data Protection Regulation (GDPR) • Data Protection Act 2018
Assurance	• DPCMAT: IND158.0

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 responding to patient 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 practice Foundation Solution 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 Foundation Solution

	• decommissioning clinical systems for example when merging or closing practices • deploying new digital 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. **Supporting Local Procurement** The use of the Digital Technology Assurance Criteria (DTAC) may be helpful in local procurement activities
Practice Responsibilities	Practices must report patient safety incidents in line with national guidance using the General Practice Patient Safety Incident Report Form provided by NHS Improvement. Practices as independent contractors are responsible for sourcing any legal advice they may require supporting any of these activities.
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) • GP IT Delivery Partner 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	https://digital.nhs.uk/binaries/content/assets/legacy/word/f/p/clincal_safety_guidance1.docxIntroductory guide to the new MDR and IVDR (MHRA) Digital Technology Assurance Criteria (DTAC)
Assurance	DPCMAT: IND11.0

Digital Services Procurement Support

Requirement	Supporting CCGs and practices with specialist procurement and technical advice on procuring services described in the Operating Model, including advice on the procurement of capabilities through the Digital Care Services (DCS) Catalogue.
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 digital procurement projects • advice on procurement of GP IT enabling services 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 regarding reporting data breaches and near misses o accessing where applicable, the National Commercial and Procurement Hub to support CCG procurement • CCGs must ensure that any procurement activity in support of GP IT, when delegated to GP IT Delivery Partner(s), does not create conflicts of interest or potential procurement challenge. **DCS Catalogue procurement support:** • supporting mini-competition work for the procurement by CCGs from the DCS Catalogue • meeting practice capabilities within nominated CCG funding allocations whilst ensuring excellent value for money **Non-DCS Catalogue procurement support:** • support Practices and CCGs purchasing non-DCS Catalogue clinical systems and digital technologies which include hosting patient identifiable information secure

	assurance against the standards below including the Digital Technology Assurance Criteria (DTAC) • Utilise as appropriate the Procurement Checklist provided in the document
Other Controls	Procurement legislation.
Applicable Standards	• NHS England Financial Guidance • NDG Standard 10
Applicable Guidance	• Digital Technology Assurance Criteria (DTAC)

Digital Services Contract Support

Requirement	Facilitating CCG GP IT delivery with support for contract and supplier management and technical support. Solutions procured through Digital Care Services (DCS) Catalogue Frameworks 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 • to meet CCG responsibilities 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 • ensure local DCS Catalogue contracts are current and accurate • manage local payments ensuring that all charges incurred are current and accurate, including payments for additional software to enhance the functionality of the clinical system • inform 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 DCS Catalogue 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

GP Estate 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 GP 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, enhanced GP IT services and local digital strategy • CCGs must ensure that any of the above activities, when delegated to IT delivery partner(s), does not create conflicts of interest or potential procurement challenge 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	Practices should engage with CCGs at an early stage of planning any premises development or expansion which will impact on GP IT provision.

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 Foundation Solutions to meet core and mandated capabilities • National Digital Services And will include training requirements arising from: • practice staff turnover • refresher training • new system functionality The CCG shall review the practice training plan and may request changes to the plan in line with local priorities and plans for the deployment of services. The CCG shall 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, Digital Care Services (DCS) Catalogue 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

Practice Responsibilities	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, either using the services provided under this requirement or at practice cost through another source, 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 practice staff to be trained and the training to be provided by the CCG within a six months period or as agreed by both parties. Practices shall make their staff available for training in line with any timetable agreed with the CCG or its Supplier(s). Practices 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 practice 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 basic IT skills, business administration systems and office systems is the responsibility of the practice.
Applicable Standards	NHS IT Skills Pathway GP IT Futures Framework Training Standard
Applicable Guidance	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).
Assurance	DPCMAT: IND7.0

Data Quality Support

Requirement	Data quality training, advice and guidance.
Specialist Support Services	Availability -Standard Service Hours. Comprehensive data quality advice and guidance service is 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 and 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 practice 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.
Practice Responsibilities	Individual practices are responsible for the quality of their patient records and the application and use of clinical terminology.
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
Assurance	DPCMAT: IND30.0

Project and Change Management

Requirement	GP IT services include formal P3M (Project, Programme and Portfolio Management) methodologies which are recognised and used in the deployment of GP IT Futures Foundation Solutions, local implementation of national solutions and major GP IT infrastructure changes or upgrades.
Specialist Support Services	Availability: Standard Service Hours The CCG will ensure skilled project and programme management resources are available, to deliver the planned programme of work, both nationally and locally driven. This may be provisioned within current SLA support arrangements, or could be procured on an 'as required' basis. 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 end to end project management of DCS Catalogue 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	• GP IT Futures Data Migration Standard • GP IT Futures Training Standard GP IT Delivery Partner staff should be appropriately trained and qualified to recognised industry standards such as APMG (equivalent level recognised industry standards) in:

	• project management – for example Prince II Practitioner • programme management – for example Managing Successful Programmes Practitioner • change management – for example Change Management Practitioner
Assurance	DPCMAT: IND32.0

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 leadership for the development of local digital strategy including the development of GP IT services • develop a patient and practice facing 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 IT requirements are represented in any relevant local, regional or national forum
Specialist Support Services	This is a direct CCGs responsibility. CCGs may wish to commission specialist skills and resources to assist in developing their digital strategy.
Assurance	• DPCMAT: IND12.0, IND153.0

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 record of local status of system deployments, changes and updates and update the national tracking database or it's replacement • local deployment programme for national systems implementation within practices, including benefits realisation, stakeholder engagement, business change support

Enhanced Requirements

These are GP digital requirements which are agreed locally to support local strategic initiatives and commissioning strategies to improve service delivery. They should support the ICS and CCG local digital strategy and where possible, strategic rather than tactical solutions should be developed.

Enhanced Requirements include:

1. **Productive Digital Capabilities -**digital technologies, systems and support services which enable and improve efficiency and effectiveness of practice contracted services including primary care at scale.

2. **Transformational Digital Capabilities** -digital technologies, systems and support services which enable transformed care, often extending beyond the practice and its core GP Contract function. These may enable new models of care, service integration, wider GP functions, and models.

   Where the practice is represented within an ICS, any decision to commission enhanced transformational requirements remains the responsibility of the CCG who has delegated responsibility for GP IT but would also be expected as local commissioner to work closely with the ICS.

   CCGs may use local GP IT funds, subject to CCG Standing Financial Instructions (SFIs) and any other financial restrictions, and with the agreement of local practices to support to support community wide transformation digital initiatives which involve GP IT. GP IT funds should not be considered the sole source of funding in such cases and must not be at the expense of providing the Core and Mandated Requirements to practices.

3. **Additional GP Contract digital capabilities** - required to deliver those elements of a GP Contract additional to providing Essential Services, for example a PMS or APMS contractor providing walk in services, minor injuries, GP out of hours etc.

4. **GP IT Enabling Requirements –** any extension of the core and mandated GP IT Enabling Requirements necessary to support and enable those Enhanced Requirements commissioned locally.

Accredited solutions are not contractually mandated but compliance with any standards attributed to the capability in this document should be considered essential. CCGs are strongly advised to use the Digital Care Services (DCS) Catalogue, Health Services Support Framework (HSSF) or other applicable frameworks listed in Appendix C offering accredited solutions.

If GP IT Futures notional CCG funds are used then the solutions can only be sourced through the GP IT Futures Framework.

Provision of Enhanced Requirements through commissioner GP IT funding is secondary to funding Core and Mandated Requirements, but they should not be seen as less

important as they underpin service improvement transformation in the locality. Compliance with CCG SFIs will require demonstration of value for money and product quality and safety.

As commissioner the CCG is responsible for selecting the solutions and services to meet Enhanced Requirements, but in doing so the CCG should collaborate with local practices.

Where Enhanced Capabilities are required which cannot be procured as an accredited solution local procurement or other frameworks may be used but solutions must still meet any standards attributed to the capability as defined in this Operating Model. The application of the procurement checklist in Appendix G and the Digital Technology Assessment Criteria (DTAC) will support this.

Listed below are some examples of enhanced capabilities which at local discretion may be provided.

Capability	**Description**
Additional Patient Management Capabilities	Additional capabilities for patient management as available through Digital Care Services (DCS) catalogue and Health Services Support Framework (HSSF)
Patient Facing Digital Services (local)	Locally commissioned patient facing digital services, where these capabilities are not provided through the NHS App, the DCS Catalogue or HSSF **Applicable Standards** • designing and Assessing Digital Heath Services - Digital Assessment Criteria • Patient Online Services in Primary Care - Good Practice Guidance on Identity Verification • Licence for Digital Interoperability Platform • FHIR standard for interoperability • 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
GP Hubs and GP Collaborative enablement	Digital enablers required to support GP collaborative and at scale operations including, but not restricted to: • practices working collaboratively • practice co-location to share resources • Hubs to share resources and improve patient access **Tracking DPCMAT**: IND 57.1, IND 57.2, IND 57.4, IND57.5

Practice Efficiency and Service Quality Enablers	• Patient arrival and kiosk systems, patient touch screens • display screens (for example large TV screens and Jayex Boards), projectors, multi-function devices, webcams • chronic disease management, drug monitoring, anticoagulation management • digital order communications and results reporting for laboratory, imaging and diagnostic tests • advanced appointment management • advanced document management • dictation • data entry e-forms • client software and integration for third party patient management systems for example Hospital Patient Administration System (PAS), Hospital radiology viewers **Tracking DPCMAT:** IND46.1, IND46.2, IND46.3, IND48.2, IND48.3, IND48.4
Additional GP Contract Digital Capabilities	Additional digital requirements needed to support those elements of a GP Contract additional to providing Essential Services – including but not limited to: • Community Provider Services • Population Management • Urgent Care Services • Walk in centres • Minor Injury Units • GP Out of Hours • Homeless primary care services • Referral Management Services
CQRS Support	CQRS training, advice and guidance for practices. Note: CQRS provides support for calculating approximately 12-14% of General Practice incentive-based payments (for example QOF). The service is business critical to general practice and to NHS England, as one of the primary mechanisms in place to support the GP Contract and to ensure that NHS England can meet its legal obligation to pay general practices. Calculating Quality Reporting Service (CQRS) advice and guidance service is available to all general practices, to include review, report management and remedial action planning, particularly around exception reporting, to ensure appropriate data quality within GP sites to enable effective Quality and Outcomes (QOF) reporting

	CQRS uses an Internet based payment calculation system: Management and support for provision payment calculation system services, supporting QOF and Enhanced Service payments
GP Data Quality Accreditation Service	A structured data quality accreditation programme is available for practices to ensure continuous review and improvement. Formal data accreditation support programme that includes: • Data quality baseline/audit review • Development and delivery of a general practice data quality improvement plan with practice(s) and • A formal rolling data accreditation programme for general practices that will underpin key work streams to support paper free / 2020 vision. **Applicable Standards and Guidance** • SNOMED Clinical Terms (CT) in General Practice / Standards Change Notice SCCI0034 Amd 35/2016 • Data Security and Protection Toolkit (DSPT) (data quality assertions) • Records Management Code of Practice 2020
BYOD	Provision for practice staff to use their personally owned devices for work related purposes (also known as Bring Your Own Device – BYOD) Because personal devices are not part of the Managed GP IT Infrastructure, they are assumed to be insecure. Where this service is offered the standards and requirements described under the Remote Access capability above will apply.
Enhanced Infrastructure	Infrastructure requirements which enable enhanced digital capabilities, or which support a more efficient, effective or secure means of GP IT provision in the locality. Networking Services: • management and support for provision of additional HSCN services • where Community of Interest Networks (COINs) are a feature of local digital primary care infrastructure, the use of GP IT allocated funds, to support these, needs to consider the following: o Where the COIN is used to support GP IT there is a clear requirement for this in addition to HSCN connectivity. o Where the COIN is shared between providers, the costs need to be appropriately proportioned. o Where the COIN is used to support GP IT, the network must have sufficient bandwidth, low latency and low contention ratio to support the necessary services.

	N.B. The cost of COINs which are cross care settings should be shared with those care settings. Local network services, including equipment, cabling and local COIN. Enhanced or alternative architectures including (but not limited to): • Virtual Desktop Infrastructure (VDI) • Citrix Access Gateway (CAG) • Smartcard/Remote Secure Access Token authentication • Single sign on **Applicable Guidance:** Where centralised infrastructure (for example but not limited to network infrastructure and virtual desktop infrastructure) is deployed particular attention should be given such that the security, end user performance and resilience of Digital Care Services (DCS) Catalogue solutions and National Digital Services is not compromised.
Advanced Telephony	An advanced cloud based Voice over Internet Protocol (VoIP) telephony solution offered to practices as a managed service (for example part of a community wide initiative). The solution will: • support resilience and flexibility including remote working, home working, hub working and alternative locations (namely for business continuity response) • support general practice manage large workload and demand including growth in telephone consultations • provide overall value for money • support local and national planning with better information on telephony based patient interactions • support the convergence of GP telephony and general IT/digital services ensuring that general practice can benefit from the latest and most innovative technologies. Individual practices remain responsible for telephony recurring operating costs, capital and revenue consequences including pro rata costs of shared/managed systems. Where possible HSCN connections to practice premises should be utilised to support the advanced telephony solution. See HSCN Requirement. The practice may choose, at their expense, to install and use a dedicated broadband connection in preference to HSCN. The capabilities required and applicable standards are described in the specification included in Appendix F.

	Tracking DPCMAT: IND193.0, IND193.1, IND193.2, IND193.3, IND193.4

General Practice Business Requirements

Digital systems, technologies and services necessary to run the internal practice business and organisational governance namely:

- general practice business support systems
- general practice legal and regulatory obligations
- general practice websites
- dispensing Practices
- general Practice Operating Costs
- general Practice Buildings and Estate

Notes:

1. Although out of scope for commissioning and provision responsibilities these may be indirectly linked through the use of common infrastructure, standards, assurance, interoperability and security. In such cases practices are required to comply with any relevant technical and security standards.
2. The infrastructure and general support required to operate these services (namely desktops, printers, network connectivity) can at the discretion of the CCG be funded and provided through “enhanced GP IT Enabling Requirements” where this allows the practice to operate more efficiently.
3. Where there are elements of the requirements described below which are not solely a practice responsibility these are descried as “Exemptions”

The ‘Global Sum’ within the GP Contract makes provision for practice expenses including practice staff costs and general running costs of the practice (stationery, telephone, heating and lighting, repairs and maintenance).

CCGs have an obligation to ensure services already NHS funded, directly or indirectly, are not also funded as an enhanced GP IT service. Any changes to existing funded arrangements should be discussed with the practices and transition arrangements agreed.

Where there is a demonstrable benefit in incorporating elements of GP business support services for example advanced telephony as part of broader efficiency release and improved patient care initiatives, GP contributions are to be considered as part of local funding provision/business case arrangements. These services should routinely be assumed to be out of scope, unless local business cases can demonstrate patient benefit, in which case, when considering funding any of these services, CCGs should take account of whether this service is already funded via alternative routes for example global sum GP Contract.

General practice business support systems

Requirement	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. GP IT funds must not be spent purchasing or supporting Systems not directly related to patient care. N.B. The 'Global Sum' within the GP Contract makes provision for practice expenses including practice staff costs and general running costs of the practice (stationery, telephone, heating and lighting, repairs and maintenance). Practice estate infrastructure.
Exemption	Where practices commission, procure and contract manage digital services directly they should have access to specialist advice and support where such services and systems will interface with NHS provided systems or operate on Managed GP IT Infrastructure. Although practices procuring business support systems are responsible for resourcing and managing their own procurement and any ongoing contract management they may seek advice where NHS systems or infrastructure may be integrated or impacted. NHS owned equipment should be insured against loss or theft by the owners of the equipment.
Services	Production of practice staff ID cards for new employees and changes to existing employees (name, role etc.). Practice Intranet – hosting, maintenance and development Insurance against loss or damage of practice owned IT equipment. Insurance against consequential losses, harm or damage arising from the failure of digital systems or equipment used by the practice to deliver their contractual obligations With evolving primary care delivery models, local service/support arrangements may develop that incorporate aspects of service provision that would traditionally have been considered GP business support functions to be directly funded by the practice under GP Contract arrangements. Equipment which only supports the practice as a business for example photocopiers. (note faxes must not be used by practices for the processing/communication of patient identifiable information). The infrastructure and general support required to operate these services (namely desktops, printers, network connectivity) can at the discretion of the CCG be funded and provided as "enhanced" services where this allows the practice to operate more efficiently subject to practice compliance with any local technical and security policies and change control procedures. Systems that only support the practice as a business for example. Payroll, HR systems, billing systems and associated hardware. Email systems other than NHS Mail

General practice legal and regulatory obligations

Requirement	Legal and regulatory obligations for example assigning a DPO, Caldicott Guardian, serious incident reporting etc. Practice compliance with: • Data Protection legislation. • Health and Safety legislation. • Freedom of Information legislation • NHS DSPT
Exemption	CCGs are required to offer General practices a DPO service which the practice can then designate as their named DPO. Practices are still entitled to select an alternative DPO of their choice although CCGs are not expected to fund this if a DPO function has already been offered. Where a CCG (or a GP IT Delivery Partner) has information necessary for the practice to comply with its legal and regulatory obligations (above) the CCG should make reasonable efforts to provide this to the practice.
Services	• Software to support redaction when processing patient record documentation for patients or third parties for example SAR, legal and insurance reports (refer to procurement checklist) • Health and Safety regulation compliance, including PAT and DSE requirements, associated with the practice premises buildings and estate and where staff are working at home or remotely (regardless of equipment ownership).

Dispensing general practices

Requirement	Digital capabilities required to support the dispensing operations in practices which hold a dispensing contract.
Exemption	Digital capabilities required to support the personal administration of medications within practices for example vaccinations.
Services	The infrastructure and general support required to operate these services (ie desktops, printers, network connectivity) can at the discretion of the CCG be funded and provided as “enhanced” services where this allows the practice to operate more efficiently.
Applicable Standards, Guidance and Controls	EPS Dispensing Systems Compliance Specification.

General practice websites

Requirement	General Practice websites including: • domain registration • hosting of website • maintenance of website and • design
Exemption	Online patient facing digital capabilities as defined in Core and Mandated Requirements. Note the practice website must provide a link for the public/patients to these online services.
Services	Responsive service to resolve performance and access issues and to implement necessary changes as required to fulfil the practice GP Contract obligations. Website design and maintenance. Website hosting requirements. Integration (links) with GP online services. The core digital offer which all practices must provide to patients should include: • an up to date accessible online presence, such as a website, that, amongst other key information, links to online consultation system and other online services prominently • signposting to a validated symptom checker and self-care health information (for example nhs.uk) via the practice's online presence and other communications
Applicable Standards, Guidance and Controls	GMS Regulations require that where General practices have a website specifically defined information and access to patient online services will be published on the website. The GP Contract framework requires all practices to have an up-to- date and informative online presence, with key information being available as standardised metadata for other platforms to use (for example the Access to Service Information (A2SI) Directory of Services Standard). The GMS Regulations also place restrictions on the advertising and hosting of private GP services including through practice websites. W3C Website Accessibility Initiative: https://www.w3.org/WAI/ Equality Act 2010 (EQA). Equality and Human Rights Commission: Statutory Code of Practice for "Services, public functions and associations" under the EQA (the Code). The Privacy and Electronic Communications Regulations (PECR)

	General Data Protection Regulation (GDPR) Data Protection Act 2018

General Practice Operating Costs

Requirement	Examples include: • digital system consumables (printer paper, printer ink/cartridges) • power utility charges • telephony operating costs, call charges, equipment costs and implementation costs (or agreed pro rata costs of shared systems or managed service costs) • backup media for any local servers (practice premises based) • practice billing systems including card readers and cashless payment systems
Applicable Standards, Guidance and Controls	Where specified in the local Warranted Environment Specification (WES) or otherwise where specified by the equipment manufacturer and digital system consumables purchased or used by the practice in the operation of the Managed GP IT Infrastructure must meet these specifications.

General Practice Buildings and Estate

Requirement	Building and estate including environment to house securely any practice-based IT equipment. Environmental requirements as required for any practice-based IT equipment for example physical security, fire suppression and air conditioning/cooling equipment. Health and Safety regulation compliance associated with the buildings and estate including DSE and PAT requirements for IT equipment operated by staff on practice premises (regardless of equipment ownership). Building Security. Power supply for IT Equipment (including cabling and outlets).
Applicable Standards, Guidance and Controls	https://www.england.nhs.uk/publication/using-online-consultations-in-primary-care-implementation-toolkit/ Working safely with display screen equipment https://www.hse.gov.uk/msd/dse/

APPENDIX B – Responsibilities and accountabilities

General Responsibilities	General	Financial	Cyber and Data Security
NHS England	Set national strategic direction. Provide strategic leadership for local commissioners. Maintains Primary Care (GP) Digital Services Operating Model. Delegates GP IT responsibility to CCGs. GP IT assurance. CCG Assurance.	Issues NHS England Financial Guidelines Funding Allocation	Strategic direction for cyber and data security CCG Assurance
NHS England Regional Teams	Oversight of CCG GP IT Accountabilities and review with the CCGs CCG-Practice Agreement assurance and escalation point	The Regional Director of Finance and Head of Digital Technology provide CCGs with advice and confirm support for capital submissions which meet required criteria.	Escalation point for High Severity Incident management.
DHSC	Contracting Authority for Digital Care Services (DCS) Catalogue Frameworks	Contracting Authority for DCS Catalogue Frameworks	
NHS Digital	DCS Catalogue and Frameworks Standards Assurance process for DCS Catalogue	Compliance with Standing Financial Instructions	Operate Data Security Centre. Data Security Protection Toolkit (DSPT) provision and management.

	Assurance, accreditation management. Commissions National Digital Services.		
Nationally Commissioned Providers	Provide digital services to agreed contract, service specifications and standards.		DSPT completion CE + Data processor responsibilities.
CCGs (or successor organisation)	Delegated responsibility for commissioning GP IT Enabling Services for all practices with whom they have a signed CCG-Practice Agreement. CCG-Practice Agreement compliance Local Digital Strategy Leadership. Securing high quality services and VFM. Robust and relevant service specification reflecting end user requirements and local strategic needs (intelligent commissioner role). Collaboratively works with practices as “end - users”.	GP IT Futures management of nominal funding allocations. Compliance with CCG Standing Financial Instructions and procurement legislation. Confirmed support from CCG Chief Finance Officer (CFO) for capital bids. Financial coding as directed in Primary care SDF and GP IT funding guidance 2021/22.	Commission GP IT enabling services to include cyber security and information governance – providing advice and support on data breach and cyber incident management Assurance of cyber security responsibilities of all providers including GP IT Delivery Partners. Data processor responsibilities, directly or through NHS commissioned suppliers, on behalf of GP data controllers.

Locally Commissioned Providers	Provide local digital services to agreed contract, service specifications and standards.	Compliance with any CCG Financial protocols in procurement activities on behalf of CCG. Declare any conflicts of interest or potential procurement challenges arising from commissioned work with CCG.	DSPT completion. CE + Data processor responsibilities. Registration for NHS Cyber Security Alert Service.
General Practice Contractors	GP Contract compliance. Individual organisational responsibilities including legal, regulatory and contractual obligations. CCG-Practice Agreement compliance.		Data Controller GDPR responsibilities, e.g. appointment of DPO. DSPT submission. Register (generic practice) email and mobile phone number for urgent text and email alerts with MHRA CAS

Core and Mandated Requirements **Responsibilities**	**Essential Clinical System Capabilities available through Digital Care Services (DCS) Catalogue**	**National Digital Services**	**GP IT Enabling Requirements**
NHS England	Operating Model determines core and mandated capabilities. Step In Services in exceptional circumstances as described in the GP IT Futures Framework Data Processing Deed		Operating Model determines Core and Mandated Requirements. Directs CCGs to commission and provide. Assurance.
NHS England Regional Teams	Assuring CCGs meet responsibilities listed below		
DHSC	Contracting Authority Digital Care Services (DCS) Catalogue Step In Services in exceptional circumstances as described in the Data Processing Deed		
NHS Digital	DCS Catalogue and Frameworks Standards Assurance process for DCS catalogue Service management and Performance Step In Services in exceptional circumstances as described in the	Commissions National Digital Services Publish system utilisation data.	

	Data Processing Deed		
Nationally Commissioned Providers	Onboarding to Digital Care Services (DCS) Catalogue Service provision to required standards.	Provide contracted services.	
CCGs (or successor organisation)	Order through call off agreements using DCS Catalogue Management of GP IT Futures nominal funding allocations. Contract management and accountability. 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. CCGs may not delegate GP IT Futures Framework call off agreements. Choice of non-Foundation Solutions from DCS catalogue (in collaboration with practices)	Support deployment. No local choice Alternative (local arrangement) systems should not be offered and should not be funded by CCGs. CCGs will ensure availability of access, infrastructure, training and deployment support for practices.	Commissions local commissioner choice of solution. CCGs **may not** delegate HSCN access agreements. Service reviews with individual practices

Locally Commissioned Providers	n/a	n/a	Provide contracted services.
General Practice Contractors	Choice of Foundation Solution from GP IT Futures Framework.	Mandated use if applicable to the organisation /practice. No local choice.	See practice responsibilities for individual capability.

Enhanced Requirements **Responsibilities**	**Capabilities sourced through Digital Care Services (DCS) Catalogue**	**Capabilities sourced through non-DCS Catalogue**	**GP IT Enabling Requirements**
NHS England	Operating Model determines enhanced capabilities (non-exclusive list). Step In Services in exceptional circumstances as described in the Data Processing Deed	Operating Model determines enhanced capabilities (non-exclusive list).	Operating Model determines enhanced GP IT Enabling Requirements (non-exclusive list).
NHS England Regional Teams			
DHSC	Contracting Authority for GP IT Futures Framework Step In Services in exceptional circumstances as described in the Data Processing Deed		
NHS Digital	DCS Catalogue Frameworks Product assurance to catalogue standards. Service management and performance Step In Services in exceptional circumstances as described in the Data Processing Deed		
Nationally Commissioned Providers	Onboarding to DCS Catalogue		

	Service provision to required standards.		
CCGs (or successor organisation)	Order through call off agreements using DCS Catalogue Management of GP IT Futures nominal funding allocations. Contract management and accountability. CCGs **may not** delegate DCS Catalogue Framework call off agreements. Choice of solutions from DCS Catalogue in collaboration with practices	Local procurement to relevant standard and organisational SFIs.	Local procurement to relevant standard and organisational SFIs.
Locally Commissioned Providers		Service provision to required standards.	Service provision to required standards.
General Practice Contractors	No mandated practice choice although practices can also purchase directly from DCS Catalogue	No mandated practice choice but practices can also purchase directly from supplier.	No mandated practice choice.

Other Responsibilities	General Practice Business Requirements
NHS England	Operating Model determines Practice responsibilities.
CCGs (or successor organisation)	CCG may at it's discretion provide infrastructure and support through the GP IT Enabling Requirements.
General Practice Contractors	Funds, procures, implements, contract manages. Complies with standards where appropriate to ensure security, confidentiality, and protection of NHS digital assets and services.

APPENDIX C – Applicable National Frameworks

Frameworks will vary in the extent of standards assurance offered. This should be considered in the selection and use of any framework.

The NHS England and NHS Improvement-funded 'Commercial and Procurement Hub' is available to support primary care customers with all aspects of procurement, including buying via the Digital Care Services (DCS) Catalogue.

Digital Care Services Catalogue

The default route for the procurement of digital products for general practice and PCNs is via the DCS Catalogue.

The GP IT Futures Framework	This replaced the GPSoC Framework for the provision of accredited general practice clinical systems and sits under the DCS Catalogue. An accredited clinical system is necessary to fulfil the GP Contract requirements for clinical record systems. Available central funding is allocated (on fair shares basis) to all CCGs but held centrally. CCGs may call off clinical systems for their practices against their centrally held allocation.
Managed by	NHS Digital
Relevant Services	• GP IT Foundation Systems (accredited) • Patient Facing Services
Further Information	Digital Care Services Catalogue Portal GFP IT Futures Framework Data processing deed

Digital First Online Consultation and Video Consultation (DFOCVC) Framework	A new framework under the DCS Catalogue for procurement of GP Online Consultation and Video Consultation Systems replacing the procurement of these systems through the GP IT Futures Framework and the DPS Framework for Online Consultation.
Managed by	NHS Digital
Relevant Services	Access for commissioners to buy nationally assured online consultation and video consultation products for general practice, with the intention that this framework will include all products currently in use. This new arrangement will bring together the requirements for these systems into a single set of consistent requirements and standards. Online consultations and video consultations will be treated as separate capabilities and suppliers will be able to offer one or the other or both.
Further Information	Digital Care Services Catalogue Portal

	Procurement Framework for online consultations and video consultations

Health Systems Support Framework (HSSF)

Health Systems Support Framework (HSSF)	The Framework focuses particularly on services that can support the move to integrated models of care based on intelligence-led population health management. This includes new digital and technological advances that help clinicians and managers understand a population's health and how it can best be managed. The Lead Provider Framework (LPF) is no longer available and the Health Services Support Framework (HSSF) will provide an alternative route to market for GP IT enabling services described in this Operating Model. CCGs, individual general practices and ICS can access this framework.
Managed by	NHS England
Relevant Services	• ICT infrastructure support and strategic ICT services, including primary care IT support and cyber security • patient empowerment and activation (including remote technology including consultations, supported self-management, social prescribing and personal health records) • shared or integrated care records • transformation and change support (including development of service change and reconfiguration) • system-optimisation (including patient pathway optimisation, care model design and patient flow) Workforce development (including eRostering, Temporary Staffing, Job Planning Solutions and Digital Staff Passports)
Further Information:	Health Systems Support Framework

Health and Social Care Network (HSCN)

HSCN Access Services DPS	Access to the HSCN for data sharing. Including support for transition and implementation.
Managed by	NHS Digital
Relevant Services	This agreement provides access to the HSCN for health, social care, and related organisations. The HSCN is a data network that enables health and social care services to access and share information reliably, flexibly and efficiently. The agreement includes support for transition and implementation. The framework uses a Dynamic Purchasing System (DPS) which helps customers find relevant suppliers through a filtering system.
Further Information	HSCN Remote Access to HSCN

G Cloud

G Cloud 12	Cloud computing services covering hosting, software and cloud support on a commodity based, pay-as-you go service. For use by the UK public sector
Managed by	Crown Commercial Service
Relevant Services	Lot 1: Cloud Hosting Lot 2: Cloud Software Lot 3: Cloud Support
Further Information	G Cloud 12

Cyber Security Services

Cyber Security Services Framework	This Cyber Security Services Framework is a new framework which offers a complete range of external support services to help NHS and wider public sector organisations manage cyber risks and recover in the event of a cyber security incident. Through design, delivery, testing, governance and assurance it enables service continuity in patient care by ensuring patient data is secured and critical services and systems remain available.
Managed by	NHS Shared Business Services (SBS) in partnership with NHS Digital and the National Cyber Security Centre (NCSC).
Relevant Services	Lot 1 Emergency Cyber Incident Management Lot 2 Cyber Consultancy Services Lot 3 Security Personnel
Further Information	Cyber Security Services Framework

Cyber Security Services 3	A dynamic purchasing system (DPS) that allows public sector buyers to buy an extensive variety of cyber security services from pre-qualified suppliers. Two distinct routes to finding pre-qualified suppliers who offer a range of cyber security services. The first route provides the buyer with suppliers who are assured by the National Cyber Security Centre (NCSC). Using this filter will ensure that your supplier has been assessed by NCSC, the National Technical Authority for cyber security in the UK. The second route provides the buyer with a set of suppliers who provide similar services to those under the NCSC assured route but without the assurance the National Technical Authority provides. It is the purchasing authority's responsibility to determine whether the service offered is fit for purpose. This may involve understanding what is assured by other accreditation bodies and how they are tested.
Managed by	Crown Commercial Service
Relevant Services	Lot 1 Cyber Security Services 3
Further Information	Cyber Security Services 3

Digital Workplace – Hardware

Digital Workplace: Hardware (Link 3) Framework	The Digital Workplace: Hardware (Link 3) Framework can be used by NHS and wider public sector organisations to purchase end user client devices for corporate and clinical situations. The framework replaces the Link 2: IT Hardware and Services Framework. The catalogue contains a core basket of goods with competitive fixed pricing for at least two years, enables new innovative methods of purchasing IT hardware such as Device as a Service (DaaS), finance leasing, and can be used to procure highly sustainable products.
Managed by	NHS Shared Business Services (NHS SBS) in partnership with NHS North of England Commercial Procurement Collaborative (NOE CPC).
Relevant Services	Commonly purchased IT category areas, with particular focus on end user computer products such as desktop PCs, laptop PCs, tablets, mobile devices, clinical displays, medical IT hardware, printers, scanners, peripherals and associated maintenance and deployment services. One-stop-shop for bundled solutions including access to Original Equipment Manufacturers (OEM) and Value-Added Resellers (VAR).
Further Information	Digital Workplace: Hardware Framework

APPENDIX D –Digital Primary Care Maturity Assurance Tool Indicators

Indicators linked to a Core and Mandated Requirement

INDICATOR (Short Description)	DATA GRANULARITY	DATA SOURCE
(IND2.0) GP IT provider business continuity and D.R. plans	CCG	CCG Questionnaire
(IND7.0) Training in clinical systems for practices	CCG	CCG Questionnaire
(IND8.1) General Practice DSPT completed	GP	DSPT Reports (NHS Digital)
(IND9.1) Secure electronic communications facility	CCG	CCG Questionnaire
(IND11.0) Formal Clinical Safety system for GPs provided	CCG	CCG Questionnaire
(IND12.0) Local GP IT strategy in place	CCG	CCG Questionnaire
(IND14.0) Local GP IT infrastructure and software investment plan	CCG	CCG Questionnaire
(IND15.0) CCG has budgeted plan for core GP IT	CCG	CCG Questionnaire
(IND20.0) Service Specification for GP IT commissioned services	CCG	CCG Questionnaire
(IND21.1) Signed CCG-practice agreement v2	GP	eDEC
(IND24.0) Annual formal review of GP IT services with each practice	CCG	CCG Questionnaire

(IND26.0) GP IT support for core GMS contracted hours	CCG	CCG Questionnaire
(IND28.0) GP IT support service desk has formal accreditation	CCG	CCG Questionnaire
(IND30.0) Data Quality Service	CCG	CCG Questionnaire
(IND32.0) Formal P3M (Project, Programme and Portfolio Management) services for GP IT available	CCG	CCG Questionnaire
(IND33.4) Remote working available using NHS managed laptops	GP	eDEC
(IND33.5) Remote working available using personal computers and Virtual Desktop Infrastructure (VDI) service	GP	eDEC
(IND33.6) Remote working available using personal computers and NHS network connection	GP	eDEC
(IND33.9) Remote working capability is available and can be used by at least 60% staff	CCG	CCG Questionnaire
(IND34.0) There is a refresh plan for GP IT infrastructure	CCG	CCG Questionnaire
(IND36.0) GP IT equipment recorded in accurate asset register.	CCG	CCG Questionnaire
(IND37.1) All software on managed equipment approved and asset managed	CCG	CCG Questionnaire
(IND38.0) All NHS GP IT equipment disposed of properly	CCG	CCG Questionnaire

(IND39.2) Secure resilient off-site/cloud based secure data storage all electronic practice PI data	CCG	CCG Questionnaire
(IND45.1) Practice System able to support patient online access to detailed (coded) record.	GP	POMI - NHS Digital
(IND48.2) Local A and E discharge letters/summaries received by practice electronically	GP	eDEC
(IND48.3) Local acute trust inpatient discharge letters/summaries received by practice electronically	GP	eDEC
(IND48.4) Local acute trust outpatient discharge letters/summaries received by practice electronically	GP	eDEC
(IND52.2) Practice system able to support patients book/cancel appointments online.	GP	POMI - NHS Digital
(IND60.2) Documented Business Continuity Plans	GP	eDEC
(IND86.0) CCG has an appointed Chief Clinical Information Officer (CCIO)	CCG	CCG Questionnaire
(IND88.5) The practice promotes and offers video consultations for Practice patients	GP	eDEC
(IND88.7) The practice promotes and offers online consultations for Practice patients	GP	eDEC
(IND90.1) IT support for PCN extended hours services	CCG	CCG Questionnaire
(IND92.1) Practice system able to support patient online ordering repeat prescriptions.	GP	POMI - NHS Digital

(IND150.1) CCG (or successor body) have clear standing financial protocols in place between commissioners and delivery organisations to ensure commissioners comply with their SFIs.	CCG	CCG Questionnaire
(IND150.2) CCG (or successor body) have clear coding, reporting, monitoring and review arrangements to ensure oversight of GPIT funding and expenditure, with clear escalation points agreed.	CCG	CCG Questionnaire
(IND152.0) Formal Governance and Accountability	CCG	CCG Questionnaire
(IND153.0) Commissioner ownership of strategic digital direction	CCG	CCG Questionnaire
(IND154.0) Clinical consideration of digital technologies in commissioning	CCG	CCG Questionnaire
(IND155.0) Digital **requirements** in commissioning service specifications	CCG	CCG Questionnaire
(IND156.0) Governance on mapping of digital enablers	CCG	CCG Questionnaire
(IND157.0) Effective and VFM GP IT procurement	CCG	CCG Questionnaire

(IND158.0) GP IT provider DSPT and IG compliance	CCG	CCG Questionnaire
(IND162.0) Benefits are explicitly defined, tracked and captured within individual projects.	CCG	CCG Questionnaire
(IND164.0) Risk management arrangements	CCG	CCG Questionnaire
(IND171.0) WiFi services for GP staff, Guests and Public use	CCG	CCG Questionnaire
(IND174.1) IT Support for PCNs	CCG	CCG Questionnaire
(IND176.0) GP IT Delivery Partner(s) and the GP work to remove, replace or mitigate and actively manage the risks of unsupported systems.	CCG	CCG Questionnaire
(IND181.0) Specialist support for GP Cyber incidents commissioned	CCG	CCG Questionnaire
(IND182.0) GP IT Delivery Partner on-site assessments	CCG	CCG Questionnaire

(IND183.1) GP IT provider certification	CCG	CCG Questionnaire
(IND192.0) The practice no longer uses a facsimile machine to send/receive patient information.	GP	eDEC
(IND 194.0) Effective backup strategy for all critical data	CCG	CCG Questionnaire
(IND 195.0) Security and protection where GP systems interoperates/integrates with the wider health and care system.	CCG	CCG Questionnaire
(IND 196.0) Shared Care Record is available	CCG	CCG Questionnaire

Indicators linked to an enhanced GP IT requirement

INDICATOR (Short Description)	**DATA GRANULARITY**	**DATA SOURCE**
(IND33.7) Remote working available using personal computers and RDP software	GP	eDEC
(IND33.8) Remote working available using another method	GP	eDEC
(IND45.2) At least 10% Patients registered for patient online access to detailed (coded) record.	GP	POMI - NHS Digital
(IND45.3) At least 20% Patients registered for patient online access to detailed (coded) record.	GP	POMI - NHS Digital
(IND45.4) At least 30% Patients registered for patient online access to detailed (coded) record.	GP	POMI - NHS Digital
(IND46.1) Practice routinely electronically orders common laboratory tests	GP	eDEC
(IND46.2) Practice routinely electronically orders common imaging and diagnostic tests	GP	eDEC

(IND46.3) Practice routinely receives electronically reports for imaging and diagnostic tests	GP	eDEC
(IND52.4) At least 20% Patients registered for patient online access appointment booking	GP	POMI - NHS Digital
(IND52.45 At least 30% Patients registered for patient online access appointment booking	GP	POMI - NHS Digital
(IND57.1) Where the practice works within a federation/collaboration it is able to use its clinical system to share records	GP	eDEC
(IND57.2) Where the practice works within a federation/collaboration it uses its clinical system to book appointments	GP	eDEC
(IND57.3) Where the practice works within a federation/collaboration it has integrated telephony systems across practices	GP	eDEC
(IND57.4) Where the practice works within a federation/collaboration it shares reporting on activity and coded clinical data	GP	eDEC
(IND57.5) Where the practice works within a federation/collaboration it shares morbidity registers across populations	GP	eDEC
(IND58.0) Local GP IT equipment specification supports concurrent use of Core and non-Core GP IT systems	CCG	CCG Questionnaire
(IND72.0) Consistent local data sharing and consent model agreed	CCG	CCG Questionnaire
(IND73.0) Auditable electronic records in local community	CCG	CCG Questionnaire
(IND84.1) Clinical staff from general practice can access their digital patient information systems from all provider and GP locations.	CCG	CCG Questionnaire

(IND84.2) Clinical staff from NHS commissioned providers can access their digital patient information systems from all GP locations.	CCG	CCG Questionnaire
(IND88.4) The practice promotes and offers email consultations for Practice patients	GP	eDEC
(IND88.6) The practice promotes and offers telephone consultations for Practice patients	GP	eDEC
(IND88.8) The practice promotes and offers email consultations for Nursing Homes	GP	eDEC
(IND88.9) The practice promotes and offers video consultations for Nursing Homes	GP	eDEC
(IND88.10) The practice promotes and offers telephone consultations for Nursing Homes	GP	eDEC
(IND88.11) The practice promotes and offers online consultations for Nursing Homes	GP	eDEC
(IND88.12) The practice promotes and offers email consultations for Residential Homes	GP	eDEC
(IND88.13) The practice promotes and offers video consultations for Residential Homes	GP	eDEC
(IND88.14) The practice promotes and offers telephone consultations for Residential Homes	GP	eDEC
(IND88.15) The practice promotes and offers online consultations for Residential Homes	GP	eDEC
(IND92.3) At least 20% Patients registered for patient online repeat prescription ordering.	GP	POMI - NHS Digital
(IND92.3) At least 30% Patients registered for patient online repeat prescription ordering.	GP	POMI - NHS Digital

(IND93.1) Other local health providers can electronically access practice records	GP	eDEC
(IND93.2) Local social care providers can electronically access practice records	GP	eDEC
(IND93.3) Practice can electronically access records from other local health providers	GP	eDEC
(IND93.4) Practice can electronically access records from local social care providers	GP	eDEC
(IND100.1) Patients can record their personal health data online and accessible by GP	GP	eDEC
(IND100.2) Patients and GPs can online collaboratively set goals and care outcomes	GP	eDEC
(IND159.0) Other provider DSPT compliance	CCG	CCG Questionnaire
(IND161.0) The CCG assures benefit realisation from local investment in digital technology.	CCG	CCG Questionnaire
(IND168.0) CQRS Service	CCG	CCG Questionnaire
(IND174.0) Governance for GP IT with STP/ACS/ACO models	CCG	CCG Questionnaire
(IND189.0) The practice have completely digitised all of its paper records (Lloyd George) and paper records are no longer kept on site or in storage.	GP	eDEC
(IND189.1) The practice uses off site storage for its patient records?	GP	eDEC
(IND193.0) The practice telephone system is cloud based	GP	eDEC
(IND193.1) The practice telephone system Integrates with the clinical system to make outgoing calls	GP	eDEC

(IND193.2) The practice telephone system can be accessed outside practice for outgoing calls	GP	eDEC
(IND193.3) The practice telephone system can manage peak demands	GP	eDEC
(IND193.4) The practice telephone system meets practice needs	GP	eDEC

APPENDIX E – Commissioning GP IT Enabling Services

A GP IT Specification Commissioning Support Pack has been developed to support ALL CCGs who are commissioning GP IT services. It is designed to assist CCGs with the subject specialist aspects of GP IT services and includes support for the development of the local specification, carrying out a robust discovery process and subject specific help with bidder engagement activity.

Where a contract for GP IT services is already in place and re-procurement is not scheduled in the near future CCGs are advised to utilise this support pack to review current service provision arrangements against the new Operating Model.

The pack consists of two separate documents:

- GP IT Specification Commissioning Support Pack v4.0.docx

- GP IT Data Capture Service Schedule v4.0.xlsm *
  (* note this is a macro enabled Excel spreadsheet)

APPENDIX F – Commissioning Advanced GP Telephony Services

A DRAFT Advanced (Cloud) GP Telephony Specification Commissioning Support Pack has been developed to support practices, PCNs and their supporting CCGs in commissioning advanced GP telephony systems namely VoIP cloud hosted systems with clinical system integration, remote access and peak demand management capabilities.

This includes guidance for procuring practices and a template specification. This guidance and template specification will be reviewed with each review of this Operating Model and more frequently if necessary.

At the present time (of publication) a specific procurement route for example a framework for Advanced GP Telephony Services is not available
Note the responsibility for selecting and funding GP telephony systems remains with the individual practice(s).

BT OpenReach and all Communication Service Providers (CSPs) will stop providing Public Switched Telephone Network (PSTN) and Integrated Services Digital Network (ISDN) services by 2025. Practices, and their supporting CCGs, should consider this factor in determining commissioning of future practice telephony systems.

This pack consists of one document:

- DRAFT Advanced (Cloud) GP Telephony Specification Commissioning Support Pack

APPENDIX G – Procurement Checklist

Applicable Frameworks such as those offered through the Digital Care Services (DCS) Catalogue or through Health Services Support Framework (HSSF) should be used wherever possible. Where practices, CCGs, PCNs and ICS cannot do this and therefore choose to procure clinical systems and digital technologies (the "product") which include hosting patient identifiable information through local arrangements steps must be taken to ensure that the product provider can offer the following assurances as applicable. The use of the Digital Technology Assessment Criteria (DTAC) may be helpful as indicated below.

Ref	Assurance Required	DTAC
1.1	Provide Information Governance assurances for their organisation via the NHS Data Security and Protection Toolkit.	Yes
1.2	Confirm that products to be procured are fully in scope of the supplier's Cyber Essentials + (CE+) certification.	Yes
1.3	Confirm that the manufacturer/developer of the product 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.	Yes
1.4	Confirm that where the product being procured is classified as a medical device the product complies with the medical device directives.	Yes
1.5	If the product uses a clinical decision support tool (namely utilising predefined algorithms and/or a knowledge base) for direct use by the patient or clinician, provide details on how these are checked for accuracy and provenance.	
1.6	If patients can directly access the product it complies with national guidance on citizen identity verification, including "Patient Online Services in Primary Care - Good Practice Guidance on Identity Verification" OR That the product uses NHS Login to verify identity and NHS Number	Yes
1.7	As data processor can and will comply with GDPR and DPA legislation. This will include agreement to and compliance with a Data Processing Agreement. The use of standardised terms and conditions such as NHS terms and conditions for provision of services: purchase order version is advised.	Yes
1.8	If data is hosted outside England provide: • assurance it complies with the requirements of UK Government IA policy in the overseas location • names of third countries or international organisations that personal data are transferred to • safeguards for exceptional transfers of personal data to third countries or international organisations	Yes

1.9	Describe how the product will support individual General Practice(s) discharge their legal responsibilities as data controller. In particular with the following: • data sharing between legal entities • respond to a Full Data Disclosure Subject Access Request (SAR) made by a patient under data protection legislation • a record access audit log automatically maintained in the system	
1.10	As data processor can support the practice (the data controller) in carrying out a Data Privacy Impact Assessment (DPIA).	
1.11	Give assurance it has a defined process for assessing third party products which form part of the product and evidence that any third-party products have been assessed against all relevant standards.	Yes
1.12	Provide details on any clinical coding system used for (history, diagnosis, symptoms, findings, diagnostic investigations and results, treatment, prescribed drugs).	
1.13	Confirm the product uses the NHS number as primary patient identifier	Yes
1.14	Describe how the support for the product will be provided during practice business hours.	Yes
1.15	Describe how the product will be maintained and upgraded (operationally, technically and contractually).	Yes
1.16	How the product integrates with the practice clinical system and what standards are used to integrate.	Yes
1.17	Provide processes to manage the following scenarios: • patients changing registered general practice • deceased registered patients • other patient identity management issues (name change, gender reassignment, legal protections) • termination of the service contract (to include but not be limited to repatriation of the patient identifiable data to the data controller) • on the Supplier (or a subcontractor) ceasing to trade • on the Supplier ceasing to use a subcontractor (e.g. clinician) in the delivery of the service • supporting patients to exercise rights of rectification, erasure (the right to be forgotten), restriction, data portability and, objection to processing as part of GDPR compliance • on practice merger and / or closure	

Practices, CCGs, PCNs and ICS purchasing GP IT hardware equipment where applicable are able to support the assurances required:

Ref	Assurance Required
2.1	Confirm that unsupported operating systems and internet browsers are not used on these devices.
2.2	Confirm that tablets and mobile devices are encrypted to NHS Security Standards.
2.3	Confirm that the equipment is compatible with the (local) Managed GP IT Infrastructure.

APPENDIX H – General Practice Quick Reference

The following may be helpful as quick reference links for **General Practices** wishing to understand where and how this document can assist them. The full document contains much more detail and should be consulted as appropriate.

About the Operating Model
Defining which organisations and services are in the scope of the Operating Model including PCNs.

The role of the CCG Practice Agreement (and data processing agreements).

What service availability (hours) a practice can expect and how are High Severity Incidents managed. Business Continuity Planning requirements.

Supporting practice sub-contracting of services and requests for direct funding.

A table summarising responsibilities and accountabilities.

Transition arrangements: a table showing what actions a CCG needs to take and the timescales to implement the new changes in the Operating Model.

Procuring Services
Accreditation, choice and selection of systems and services

Advice on practice direct procurements and a local procurement checklist

Support for GP Telephony procurement including a template specification

Using the NHS Digital Care Services Catalogue including the GP IT Futures Framework and the Online Consultation Video Consultation (DFOCVC) Framework

Requirements
How the digital requirements for general practice are classified for example what are the "must dos", what are locally determined and what are practice responsibilities. Details of each of these requirements is provided as:

- Core and mandated (Must do) requirements for – clinical systems, nationally provided digital services, patient facing systems, and locally commissioned GP IT Enabling services. The latter includes Commissioning GP IT, GP IT Service Desk, Equipment Asset Management, Software Licence Management, Registration Authority (smartcards), NHS Mail Administration, Essential Infrastructure (for example networking and data hosting), HSCN, WiFi, Desktop Infrastructure, Remote Access (incl home), Electronic Messaging (for example SMS), Controlled Digital Environment, Cyber Security, Information Governance, Clinical Safety Assurance, Procurement Support, Contract Support, Estates, Clinical System Training, Data Quality Support, Project Management, Local Digital Strategy, National Digital Services.
- Enhanced Requirements – locally determined subject to affordability. These are often enablers for efficiency and transformation.

- General Practice Business Systems – these are practices responsibility to choose, procure and fund. These include practice websites, telephony, dispensing practices (systems and IT), business systems for example payroll and accounting systems, estate related for example power, comms rooms, air conditioning, IT consumables, practice legal and regulatory responsibilities for example Health and Safety regulations compliance.

APPENDIX I – Glossary of Terms

Term	Description
ANM	Advanced Network Monitors
APMS	Alternative Provider Medical Services
ATP	MS Windows Defender Advanced Threat Protection
BC	Business Continuity
BCP	Business Continuity Plan
BMA	British Medical Association
BCMS	Business Continuity Management System
BYOD	Bring Your Own Device
CAS	Central Alerting System
CAS-T	CESG Assured Service Requirement for Telecommunications
CCG	Clinical Commissioning Group
CE +	Cyber Essentials Plus
CESG	UK National Technical Authority for Information Assurance now part of National Cyber Security Centre
CIS	Care Identity Service
CIS2	NHS Care Identity Service 2. (formerly known as NHS Identity)
CN-SP	Consumer Network Service Providers (of local HSCN services)
COIN	Community of Interest Network
CQRS	Calculating Quality Reporting Service
CRM	Customer Relationship management
CSP	Communication Service Providers
DCB0129	Clinical Risk Management: Its application in the manufacture of health software
DCB0160	Clinical Risk Management: Its application in the deployment and use of health IT systems
DES	Directed Enhanced Service
DFOCVC	Digital First Online Consultation and Video Consultation
DPA	Data Protection Act
DPIA	Data Privacy Impact Assessment
DPO	Data Protection Officer
DR	Disaster Recovery
DSE	Display Screen Equipment
DSPT	Data Security and Protection Toolkit
DTAC	Digital Technology Assessment Criteria
eDec	General Practice annual e-Declaration
EPRR	Emergency Preparedness, Resilience and Response

EPS	Electronic Prescription Service
e-RS	NHS e-Referral Service
ETTF	Estates and Technology Transformation Funds
FOIA	Freedom of Information Act
GDPR	General Data Protection Regulation
GMS	General Medical Services
GPC	General Practitioners Committee of the BMA
GP FV	General Practice Forward View
GP2GP	GP2GP Service
GPES	General Practice Extraction Service
GPSoC	GP Systems of Choice Framework
HSCN-GP	Health and Social Care Network for General Practice
HSSF	Health Systems Support Framework
ICB	Integrated Care Board
ICO	Information Commissioner's Office
ICS	Integrated Care Systems
IFU	Instructions For Use
IG	Information Governance
ISMS	Information Security Management System
ITIL	IT Infrastructure Library
IVDR	In-Vitro Diagnostic medical device Regulations
KPI	Key Performance Indicator
LA	Local Administrator
LMC	Local Medical Committee
MDR	EU Medical Devices Regulations
MESH	Message Exchange for Social and Health Care
MHRA	Medicines and Healthcare Products Regulatory Agency
NCSC	National Cyber Security Centre
NDG	National Data Guardian
ODS	Organisational Data Services
P3M	Project, Programme and Portfolio Management
PAT	Portable Appliance Testing
DPCMAT	Digital Primary Care Maturity Assurance Tool
PCN	Primary Care Network
PDS	Personal Demographics Service
PID Submission	Project Initiation Document Submission as required for capital funding bids
PMS	Personal Medical Services
Prince II	PRojects IN Controlled Environments 2nd edition

PSTN	Public Sector Telephone Network
QOF	Quality Outcomes Framework
QoS	Quality of Service
RA	Registration Authority
PBAC	Position Based Access Control
RCGP	Royal College of General Practitioners
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAR	Subject Access Requests
SCR	Summary Care Record
SFI	Standing Financial Instructions
SIRO	Senior Information Risk Owner
SLA	Service Level Agreement
SMS	Short Message Service
STP	Sustainability and Transformation Plan
STEIS	Strategic Executive Information System
VDI	Virtual Desktop Infrastructure
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WES	Warranted Environment Specification
WiFi-GP	WiFi-GP access for practice staff and patients in general practice
WTD	Working Time Directive