Securing Excellence in Primary Care (GP) Digital Services

The Primary Care (GP) Digital Services

NHS England
NHS Improvement

Securing Excellence in Primary Care (GP) Digital Services

The Primary Care GP Digital Services Operating Model 2019-21

Publishing approval number: 000303

Version number: 4

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 the Customer Contact Centre by telephone on 0300 311 22 33 or email england.contactus@nhs.net or write to NHS England and NHS Improvement, PO Box 16738, Redditch, B97 9PT

Contents

1 Foreword

Investment and Evolution

General practice is the heart of the NHS, and the NHS relies on it to survive and thrive. As a working GP, I am fully aware of the struggles facing general practice today, we have growing demand and fewer resources, both physical and financial. We need to consider alternative ways in which to work and deliver care for our patients. Ways that will allow us to ease pressure, whilst providing the best care possible to our patients.

The use of digital and technology are methods which have been used by many other industries to modernise the way they work. We in the NHS must look to fully take advantage of the latest technologies available. However, I recognise the importance of a resilient and effective infrastructure upon which these technologies can only be delivered. We cannot have practices being asked to offer video consultations when their present hardware and bandwidth do not allow them to consult effectively without frustration.

This operating model recognises the struggles faced in general practice and needs all CCGs to take full advantage of ensuring that investment is directed to areas of need. It includes the details of what would be expected for general practice for now and the future.

This new Primary Care Digital Operating Model (previously the GP IT Operating Model) covers the key policies, standards and operating procedures that CCGs are obliged to work with to fulfil their obligations under the delegated arrangements. The model is intended to ensure that general practices have access to safe, secure, effective and high performing IT systems and services that keep pace with the changing requirements to deliver care.

It is essential that executives and staff in CCGs that have responsibility for or are involved with the provision of GP IT services are fully aware of and familiar with the guidance in this model. It is no longer sufficient to simply provide just IT support; digital service delivery must be recognised as core provision to support new models of care.

The NHS Long Term plan and the new five year framework for GP contract reform place general practice at the core of Integrated Care Systems (ICS) and local Strategic Transformation Partnerships (STPs) with access to a *digital first* primary care offer for patients enabled by the widespread adoption of technology. This operating model will empower practices, Clinical Commissioning Groups (CCGs) and STPs to embrace such change through supporting the Primary Care Networks (PCN) and accelerating the adoption of patient facing digital services such as online consultations.

The potential of disruption to critical NHS services such as general practice from cyber security threats is ever present. There are high public expectations on data

security and clinical safety in our electronic patient record systems. Keeping general practice safe is a critical element of the Primary Care Digital Operating Model as practices continue to embed digital technology.

A new CCG Practice Agreement accompanies the release of this operating model. All CCGs and General Practices are required to sign this new agreement by December 2019 which provides clarity and assurance to both parties on the provision of digital services (Clinical Systems and IT services) to general practice.

Adoption of technologies requires more than just new digital solutions. True digital transformation will only be realised with strong clinical and digital leadership making sure that locally primary care is supported by robust and responsive local services and infrastructure.

We are grateful for the support of many colleagues in CCGs, GP Practices, CSUs and other parts of the NHS (BMA and RCGP) that have contributed to the development of this guidance.

Dr Masood Nazir

GP at Hall Green Health, Birmingham & Associate Chief Clinical Information Officer for Primary Care Digital Transformation, NHSX

2 Introduction

This document sets out the revised operating model for the provision of a 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 and 2016.

2.1 Purpose – what does this document do?

The operating model is a **commissioning framework** supporting the provision of digital obligations under the GP Contract:

1. Defining the digital requirements for general practice as clinical and business capabilities and the necessary IT enablers.
2. Attributing standards (and guidance) to these requirements to ensure quality, safety and compatibility.
3. 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 IT services to:

- Explain how the NHS will fulfil its obligations regarding GP Digital services and support under the GP contract.
- Inform general practice of what to expect in the provision of GP digital 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/citizen 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 trajectory planning and 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.

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;
- Governance arrangements, including roles and responsibilities;
- The leadership necessary to achieve excellence.

2.2 Definitions

The following definitions are used in this document

Term	Definition
Clinical System	The digital application used by the practice to store & manage its electronic patient records and provided through GPSoC Principal Clinical System OR GP IT Futures Foundation Solution AND any additional integrated or interfaced application
Core and Mandated GP IT Requirements	The requirements for digital systems, technologies and services necessary to deliver essential primary care services under the GP contract or as otherwise nationally mandated. Under GP contract obligations these are funded by NHS for GP contractors.
Essential Clinical System Capabilities	The patient management and clinical capabilities which are core and mandated requirements and are enabled through accredited software applications and data solutions available through the GP IT Futures Framework.
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	Any 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 and against clearly defined service level agreements and KPIs.
GP IT Futures Catalogue	The online catalogue provided under the GP IT Futures Digital Care Services Framework
GP IT Futures Framework	The GP IT Futures Digital Care Services Framework Contract
High Severity Incident	An incident defined or classified as severity level 1 or 2 in NHS Digital Severity Level Guidelines
High Severity Incident Support Hours	24 hours / day, 7 days a week.
Managed Device	Any individual IT devices which are 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	Digital services commissioned centrally by NHS and provided to, and used by all NHS commissioned providers as applicable
NHS Owned IT Equipment	IT equipment purchased by the NHS using NHS funds (capital or revenue).
Additional GP Contract Digital Capabilities	Required to deliver those elements of a GP contract additional to providing essential primary medical services to a registered patient list, e.g. a PMS or APMS contractor providing walk in services, minor injuries, GP out of hours etc. These are Enhanced Requirements.
Operating Model	The Primary Care (GP) Digital Services Operating Model as described in the document entitled Securing Excellence in Primary Care (GP) Digital Services: Version 4: 2019-21 published by NHS England, and in the publication of subsequent amendments and revisions
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 and 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 Devices	Any individual IT device which is part of the practice managed IT equipment
Practice Managed IT Equipment	Any IT equipment, including desktops, mobile equipment, multi-function copiers etc, regardless of ownership, which is managed by the practice or a contractor appointed by the practice and is not directly connected to the managed GP IT infrastructure
Practice Owned 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 and practice employees as well as health & social care professionals individually commissioned directly by the practice.
Shared Managed IT Infrastructure	Those components of the managed GP IT infrastructure which are shared by other organisations who are not recipients of this service.

Note: as the GP IT Futures Framework which replaces the GPSoC Framework will be available to provide services after an initial period in this operating model any

reference to GP IT Futures can up until the point where it is available be interpreted with the equivalent reference within the GPSoC Framework.

2.3 About the revised operating model

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

In revising the operating model NHS England has, with the support of the profession, considered the following:

- That both GPSoC Framework and the GP IT Operating Models and their preceding frameworks have, with strong clinical engagement and contractual levers, been successful in realising a highly digitised general practice estate with a large percentage of paper free processes.
- That the GP contract includes a number of significant requirements for digital services.
- That general practice leads the NHS in the adoption of patient facing digital systems.
- That we must not lose these hard-won gains in developing this new operating model to meet new world demands.

NHS England recognises a number of significant drivers and trends:

- The introduction of new models of care.
- 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, practice federations, multisite practices, and super-partnerships.
- The implications of extended general practice access.
- Introduction of fresh digital solutions, diversity and innovation.
- Delivering on the digital commitments made in the General Practice Forward View, the NHS 10 Year Long Term plan and the five year framework for GP

contract reform and the views of the profession raised in Saving General Practice.

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 2019 to March 2021.

This operating model mandates a number of digital requirements which must be provided by the NHS to meet its obligations under the GP contract. CCGs as local commissioners should not view this as defining the limits of local investment in digital solutions for general practice, but as the minimum essential 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 in turn need to utilise and embrace these digital tools making the necessary service changes to realise the benefits they can deliver.

This revision includes;

- An updated description of roles and responsibilities.
- A strong emphasis on ensuring the security and safety of digital services in general practice.
- Arrangements for the replacement for GPSoC Framework with the new GP IT Futures Framework.
- An updated definition of organisational and functional scope.
- A re-categorised schedule of requirements and capabilities underpinned by applicable standards. Includes addition of a “national digital services” category.
- Building on the role of CCGs as informed local commissioners of GP IT services.

The scope of the Operating Model has been reviewed to reflect the ambition stated in the preceding published version (2016) for a single Digital Primary Care Operating Model aligned to primary care commissioning, to provide a framework which ensures digital technology fully supports and enables new models of care. This operating model therefore has embedded the GP IT Futures Framework, nationally commissioned digital solutions and the new Primary Care Networks (PCNs).

A new CCG-Practice Agreement accompanies the release of this operating model. All CCGs and General Practices are required to sign this new agreement which will provide clarity and assurance to both parties on the requirements for the provision and use of digital services available to general practices under this operating model.

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 driver for this operating model. This in turn defines the organisational scope for the operating model as follows:

Organisations in scope

- General Practices contracted under the GP contract (this includes GMS contracts, PMS agreements and APMS contracts).
- Primary Care Network (PCN) services provided by GP contractors under the new Direct Enhanced Service (DES).

Stakeholders

- Primary stakeholder organisations including CCGs, General Practices, NHS England and NHS Improvement and NHS Digital.
- Secondary stakeholder organisations include commissioned GP IT delivery providers, GP IT Futures Framework accredited suppliers, other GP digital capability suppliers and GPC England, LMCs and others representing and supporting general practice nationally and locally.

Organisations out of scope

- Other primary care contractors.
- Providers contracted through the NHS Standard Contract.
- GP Federations and similar collaborative organisational forms, set up 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.

Services out of scope

- Services provided outside the GP contract by practices e.g. occupational health services.

2.5 Key Challenges

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

- **Keep general practice 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
  - Replacing GPSoC framework with GP IT Futures Framework embedded in this Operating Model.

- **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.

- **Support new models of care and contracts**
  - *Support for the new PCN DES & Integrated Care Systems.*

- **Support general practice meet patient's digital expectations**
  - Requirements to support new GP contract patient facing digital commitments.

- **Build on success**
  - Recognising and building on success of GP Systems, GPSoC Framework and previous operating models.

How the operating model addresses each of these challenges is described later in this document.

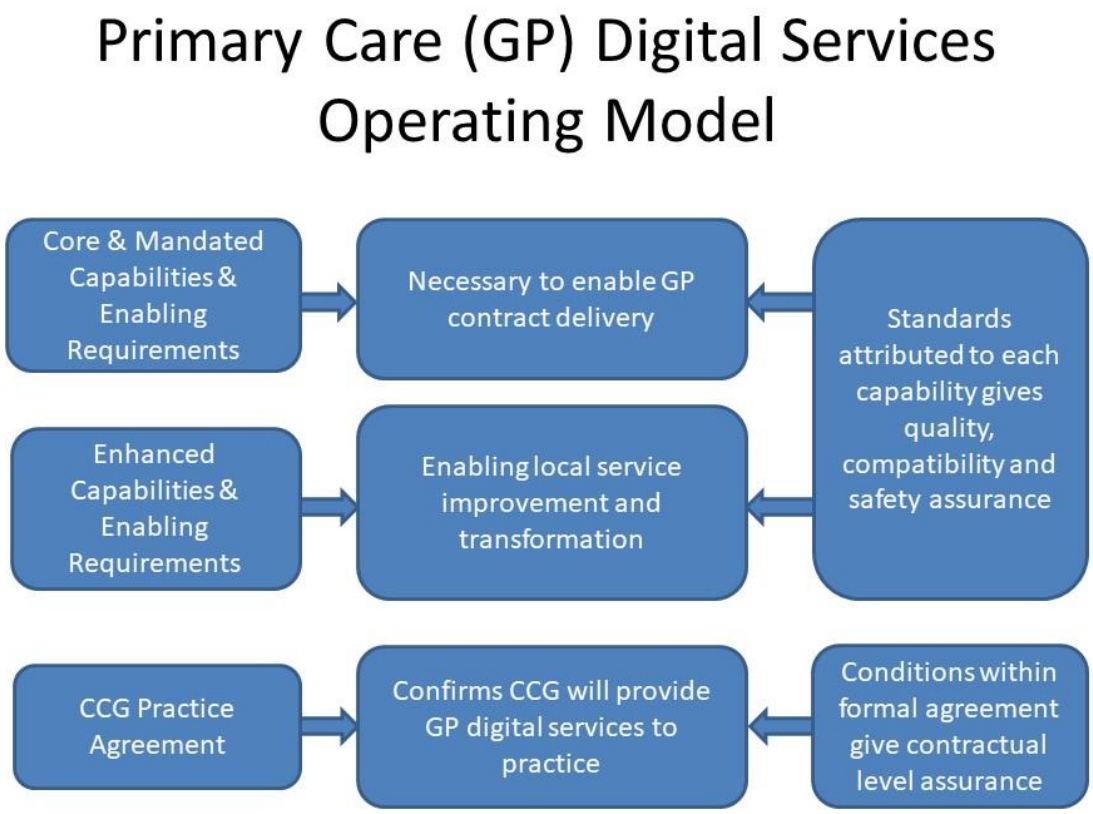
3 The CCG Practice Agreement

A new CCG Practice Agreement will be published in 2019.

All CCGs are required to sign this agreement with each general practice (ie holders of a General Medical Services (GMS) contract, Personal Medical Services (PMS) agreement or Alternative Provider Medical Services (APMS) contract offering Primary Care Essential Services to a registered patient list) within their area by 31st October 2019. This timescale aligns with the new GP IT Futures Framework. Any escalation on a failure to sign a CCG-Practice Agreement or a dispute on the terms of agreement must be raised with NHS England regional teams by 30th November 2019.

This agreement will provide clarity and assurance to both parties on the requirements for the provision and use of digital services available to general practices under this operating model. CCGs must therefore ensure a signed CCG-Practice agreement is in place before providing these services to a practice as shown in Figure1 below.

Figure 1: The CCG Practice Agreement and GP Digital Requirements



The Agreement

1. 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.
2. References the operating model as defining the scope of digital requirements to be provided and the applicable standards for those requirements.
3. References the Data Processing Deed, which sets out the data processing activities for the GP IT Futures Framework between the practice, NHS Digital, NHS England and the Secretary of State for Health and Social Care (at times acting as joint data controllers).
4. Requires CCGs to enter into data processing agreements for locally commissioned digital services for the practices.
5. Confirms that any national digital services have data processing terms under the national agreement.
6. Requires GPs who acquire independent digital services (outside of the GP IT Futures Framework, national digital services or local CCG commissioned

services) to enter into a data processing agreement with the supplier where personal data is being processed.
7. Describes how accreditation as required under the GP contract will be assured for solutions procured.
8. Defines categories for service availability.
9. Requires the practice as the “end user” organisation to comply with any terms and conditions of use of NHS commissioned systems made available to the practice.
10. Defines processes for the management of change requests, escalations and disputes relating to the delivery of services under the agreement.

The Agreement is supported by four schedules as appendices to the agreement which should be reviewed locally and subject to annual review in line with mandated national requirements and local priorities:

1. Appendix 1 - Summary of services.
2. Appendix 2 - Support and maintenance service levels.
3. Appendix 3 - Escalation procedure.
4. Appendix 4 – Business justification form.

Under the General Data Protection Regulation (GDPR) the practice must obtain assurance that data processing organisations providing services under this agreement (directly or indirectly) have “sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.”

In relation to the GP IT Futures Framework and national digital services data processing agreements and measures are already in place with which all parties must comply.

For locally commissioned digital services the CCG will ensure data processing agreements are entered into with the supplier which the practice can adopt.

If the practice puts its own arrangements into place with a third party which includes the processing of its data (e.g. a GP Federation organisation) then the individual practice must take necessary steps, including documentation, to give this assurance as this will fall outside the scope of the CCG-Practice agreement and this schedule.

Agreement Review

The agreement should be reviewed:

(i) when there is a significant change to the organisational form or status of either party e.g. merger of general practice(s), merger or Clinical Commissioning Group(s) (CCGs)

(ii) on request for review by either party

The agreement schedules should be reviewed;

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

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

Timescales

- NHS England to publish CCG-Practice Template Agreement by August 2019.
- CCGs to develop local Schedules i.e. Summary of services, Support and maintenance service levels and Escalation procedure for incorporation into CCG-Practice Agreements locally by 30th August 2019.
- CCGs and GPs to sign agreements August - October 2019.
- Note current CCG-Practice agreements remain in place until 31st December 2019 or until the practice and CCG sign the new agreement, whichever is the sooner.
- Unsigned agreements to be escalated to NHS England regional teams by 30th November 2019.

Assurance

The Primary Care Digital Maturity Assessment Tool (PC DMAT) will track CCG-Practice agreement sign up.

3.1 Accountabilities and Responsibilities

The CCG-Practice Agreement describes the responsibilities of the practice and the CCG for the provision and receipt of GP Digital Services.

Detailed accountabilities and responsibilities for parties involved in the operating model are given in Appendix B.

The 2018 Addendum to the GP IT Operating Model, Securing Excellence in GP IT Services 2016-18 (revision) v3 directed a change in responsibility for the commissioning/provision of Primary Care Enabling Services (i.e. Information Governance, Clinical Safety Assurance, Registration Authority and NHS Mail Local Administration) for general practice from NHS England regional teams to CCGs. This changed responsibility remains in this operating model.

4 Requirements and Capabilities

A set of digital requirements defined by the clinical or business capabilities needed to enable the practice to fulfil its obligations under the GP contract is described. These capabilities will require digital solutions to be procured and will require a set of GP IT enabling requirements to be met e.g. infrastructure, equipment, connectivity, support, training etc.

Requirements can be cross mapped to show dependencies and GP IT enabling requirements are scoped by those clinical system capabilities they need to support. 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 requirement is commissioned.

Responsibilities for fulfilling these requirements (e.g. 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 is provided in Appendix D to assist Clinical Commissioning Groups in this task.

4.1 Core & mandated requirements

The requirements for digital systems, technologies and services necessary to deliver the GP contracted service or as otherwise nationally mandated. Under GP contractual obligations these are funded by NHS 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 (when this replaces the current GPSoC Framework). To meet the six foundation capabilities practices will choose the best fit Foundation Solution(s) from those available in the catalogue. 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 – i.e. 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

The requirements for digital systems, technologies and services which may 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 & 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 GP IT Futures Framework.

4.2.2 Transformational digital capabilities - patient management and clinical capabilities which enable transformed care, often extending beyond the practice and its core GMS function and which can be enabled through software application and data solutions. Accredited solutions to meet these capabilities will be available through the GP IT Futures Framework.

4.2.3 Additional GP contract digital capabilities - Required to deliver those elements of a GP contract additional to providing essential primary medical services to a registered patient list, e.g. a PMS or 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 those enhanced capabilities above (4.2.1, 4.2.2, 4.2.3) commissioned locally.

In providing services to meet these enhanced requirements CCGs should have regard to the following points:

a. CCGs have an obligation to ensure requirements already met through NHS funded services or funded through other routes (e.g. GP global sum, provider baseline tariff) are not also funded as enhanced services.
b. A “capability” where met should be supported by the GP IT enabling requirements necessary to access and utilise that capability e.g. infrastructure, equipment, service desk, specialist support.
c. 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.

d. 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 & mandated requirements.
e. Many enhanced digital capabilities will be the enablers for service/business change which will realise significant benefits to the NHS 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 & regulatory responsibilities.
- Practice websites.
- Dispensing services.

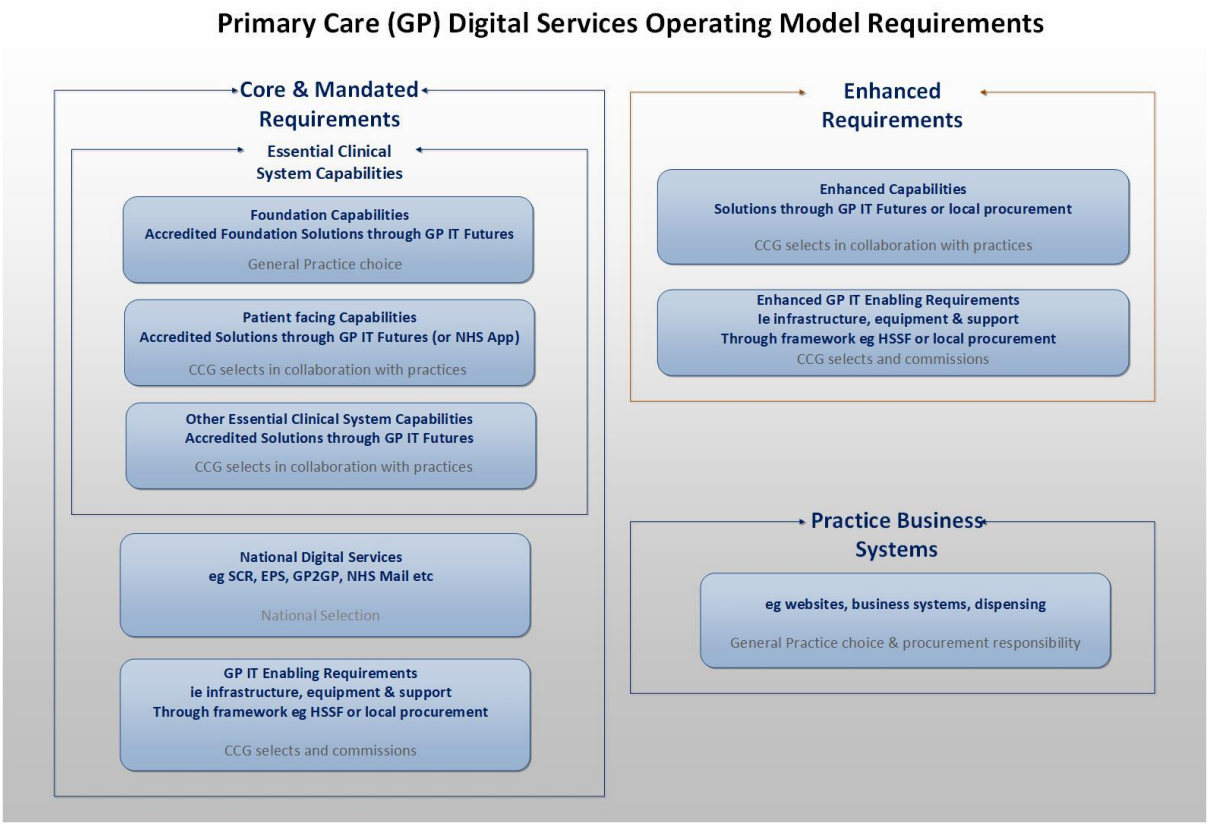
(i) Although out of scope for commissioning and provision responsibilities these may be indirectly linked through the use of common infrastructure, standards, assurance, interoperability and security. In such cases practices are required to comply with any relevant technical and security standards

(ii) The infrastructure and general support required to operate these services (i.e. 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.

(iii) Practices may also bid for financial support through non-recurrent or capital funds such as Estates and Technology Transformation Fund (ETTF) to support practice buildings and estate development projects.

(iv) 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.

Figure 2: Requirements and capabilities under this operating model.



Note: CCG collaboration with practices will include CCGs consulting with LMCs representing local practices

See Appendix A details.

4.4 Service Availability, Service levels and Incident management

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 extended hours but 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.
- Support high severity cyber incident management (through business continuity and disaster recovery planning).

The following are the minimum service availability requirements;

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.

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.

3. **Extended Operational Support Hours**
    - Responsibility for meeting the requirements of the extended hours access DES transferred from practices to PCNs as part of the PCN DES on 1 July 2019. As part of the GP IT enabling services to support PCNs under this model, CCGs must commission “Extended Operational Support Hours” to support these services. Practices and PCNs delivering services during these extended hours should have access to sufficient support services (GP IT enabling requirements) to ensure continuity of extended hours operations. These will apply to services delivering against requirements where “operational service hours” are required. The CCG will agree with practices, LMCs and PCNs locally to determine the scope of and any applicable restrictions to the “Extended Operational Support Hours” including:
        - Exceptions (e.g. public holidays).
        - Practice premises, practices and operational services supported.
        - Applications supported.

4. **High Severity Incident Support Hours**

- 24-hour 7-day access for high severity incident management & business continuity response based on a 48 (actual) hour Recovery Time Objectives (RTO) for essential practice activities.

- As part of the business continuity plans (BCPs) contractually required from GP IT delivery partners, a 24-hour 7-day access and response to a high severity cyber or data protection incident whether raised locally or nationally must be available. The business continuity plan and associated disaster recovery plans will address the mobilisation of resources necessary to manage the incident and meet the mandated Recovery Time Objectives (RTO).

- All practices should be able to log an incident or request at any hour or day using one of the following methods:
    - Telephone,
    - Email,
    - Web Portal (internet accessible),
    - App.

5. **Systems and Infrastructure Availability**

    - 24-hour 7-day availability for systems and infrastructure availability (with individual contracts defining % availability and support hours).
    - Examples include clinical systems (foundation solutions), NHS applications, Health & Social Care Network (HSCN), WIFI, Local Networks and GP Online Consultations.

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 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 & Selection of Solutions

General practices, which use computerised patient records, are required through the GP contract to use an accredited clinical system. The accreditation, currently determined through the GPSoC Framework will be determined by the inclusion of the required capability in the GP IT Futures Framework when it becomes available. Individual practices will be able to determine the most appropriate foundation solution from the accredited solution(s) in the catalogue 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 (eg patient facing services, online consultation systems, document management etc) 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 selection of accredited solutions is not contractually mandated although accreditation may be required if it is defined within any standard attributed to the capability. In all cases CCGS should only procure solutions which meet the standards referenced in this Operating Model and where authoritative accreditation is available e.g. the GP IT Futures Framework or the National Dynamic Purchasing System Framework (for online consultation solutions) then CCGs are strongly advised only to procure accredited solutions to meet these capabilities. If GP IT Futures notional CCG funds are used the solutions can only be sourced through the GP IT Futures Framework. Compliance with CCG SFIs will require demonstration of value for money and product quality & safety.

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

CCGs will be required [i] to provide a Data Protection Officer (DPO) function for all 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.

Table 1: Summary of Solution Selection and Mandatory Accreditation

Requirement	Identification & Choice of Solution	Mandatory Accreditation
National Digital Services	NHS Digital or NHS England	
GPSoC (Lot 1) Principal Clinical System	General Practice chooses clinical system	GPSoC Framework
GPSoC (Lot 1) Subsidiary Systems	Commissioning CCG in collaboration with practices	GPSoC Framework
GP IT Futures Foundation Capabilities	General Practice chooses foundation solution	GP IT Futures Framework
GP IT Futures core & mandated capabilities (not Foundation Capabilities)	Commissioning CCG in collaboration with practices	GP IT Futures Framework
GP IT Enabling Requirements	Commissioning CCG	See Operating Model
Enhanced Capabilities & Requirements	Commissioning CCG in collaboration with practices	
Practice Business Requirements	General Practice	

4.6 De-commissioning of services

The CCG may de-commission a service meeting core and mandated capabilities providing (i) the core and mandated capability is still met either through a replacement service or by rationalising service duplication (ii) the decision does not conflict with the practice's choice of foundation solution (iii) 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 enhanced capabilities providing the impact on practices 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 (i) any core and mandated enabling requirements are still met either through a replacement service or by rationalising service duplication (ii) practices are advised of any service delivery changes and appendix 1 of the CCG Practice Agreement is updated as necessary.

5 Funding

5.1 Key Actions

- Funding to support the delivery of GP IT services forms part of CCG revenue programme allocations.
- Core and mandated GP IT enabling requirements (See Appendix A) are mandatory for local investment.
- Investment in enhanced requirements should be commissioner led, in consultation with general practices and will align closely with local digital strategy, Sustainability and Transformation Partnerships (STP) and Primary Care Network (PCN) plans which underpin the integration and transformation of care locally.
- 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.
- CCG 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.
- 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 e.g. procurement support services.
- CCGs should start planning the impact of the new Primary Care Network DES and the associated digital requirements prior to the release of further clarification on IT funding to support the PCN DES.

5.2 GP IT Revenue

GP IT revenue funding forms part of CCG revenue programme allocations. Priority must be given to funding the core and mandated digital requirements described in this operating model, followed by funding enhanced requirements as required locally.

As directed in the 2018/19 Addendum to the GP IT Operating Model, Securing Excellence in GP IT Services 2016-18 (revision) v3 responsibility for the commissioning of Primary Care Enabling Services (i.e. Information Governance, Clinical Safety Assurance, Registration Authority and NHS Mail Local Administration) for general practice rests with CCGs and funding for this was included in the CCG baseline allocations from April 2018.

From April 2019 HSCN-GP, WiFi-GP and DPO provision will be funded by CCG from their baseline allocations.

Additional funding has been included in the core CCG allocation growth for 2019/20 for HSCN-GP, replacing previous in-year allocations.

5.3 Primary Care Network (PCN) DES

The new five-year framework for GP contract reform to implement The NHS Long Term Plan announced the introduction of Primary Care Networks (PCN) through a DES. 100% geographical coverage of the Network Contract DES is expected by July 2019 involving an additional 20,000+ staff by 2023/24.

It is expected that the PCN staff will use the practice GP IT Futures Foundation Solutions.

5.4 GP IT Futures Framework

The transition from GPSoC Framework to GP IT Futures Framework will be supported by a notional allocation of funds to each CCG. These funds, which will be held centrally, will be based on registered patient capitations.

In using these funds, the CCG:

1. May only use these funds to procure through the GP IT Futures Framework through the online catalogue.
2. Should procure Foundation Solutions to meet the Foundation Capabilities through the GP IT Futures Framework as first call on the funds, followed by the remaining core & mandated essential clinical system capabilities (see Appendix A) that may be met through the GP IT Futures Framework
3. May use any remaining funds to procure solutions to meet any enhanced clinical capabilities through the GP IT Futures Framework for use by their practices.
4. NHS Digital will hold 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 GP IT revenue funds to procure enhanced capabilities directly through the catalogue.

Individual practices can use practice funds to procure any other accredited solutions directly through the catalogue.

Assurance

Through the GP IT Futures Catalogue reporting capability NHS Digital will, for each CCG.

(i) Identify by each CCG that all core & mandated (essential clinical system) capabilities have been procured by the CCG for all its practices.
(ii) 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.

5.5 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 baseline funding allocations to support any recurring costs after the transition period will be made on a programme by programme basis.

5.6 GP IT Capital

NHS England capital funding for GP IT will continue to be available for CCGs to access from NHS England Regional teams. 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 e.g. installation, disposal, software licences should be considered within the capital bid.

Capital is available to support Business As Usual GP IT investments and IT to support transformational estate schemes under the ETTF programme. 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 GP IT 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.

5.7 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.

5.8 Out of scope

CCGs are expected to ensure that the commissioning and procurement of digital services locally does not duplicate existing funding sources or provisions. General practice business requirements should not be funded using these allocations.

The General Practice Global Sum is out of scope. The global sum is used to directly fund GP contracts and will include services and utilities such as the General Practice Business Requirements listed in Appendix A and practice telephony services. Investment and Evolution: a five-year framework for GP contract reform (published 2019) announced, in recognition of income loss and workload from subject access requests, £20 million of additional funding will be added to the global sum for the next three years (starting in 2019/20).

Dispensing practices (approximately 1,000) operating under pharmaceutical dispensing regulations require software and digital infrastructure to operate the dispensing function. These are currently outside the scope for the receipt of GP IT Digital services under this operating model.

Table 2: Funding sources and application supporting Digital Primary Care

Funding	Type	Purpose	How is this accessed locally	Timescale
GP IT Revenue	Recurrent Revenue	To provide/commission GP IT services with 1st priority on core & mandated GP IT enabling requirements From April 2019 includes HSCN-GP funding and WiFi-GP maintenance funding	Included in CCG baseline revenue allocations	Annual
GP IT Capital	Capital	GP IT infrastructure/equipment priority to support core & mandated requirements Capital bids through ETTF programme for infrastructure/equipment will support improvement & transformation	CCGs submit bids annually	Annual
General Practice Systems of Choice Framework		Provide GPSOC principal clinical systems to all practices (and limited subsidiary systems)	Held and managed nationally. CCGs call off national framework contract	Ends December 2019
GP IT Futures Digital Care Service Framework		To call off accredited solutions from GP IT Futures Framework with priority for Foundation and core & mandated capabilities	Notional allocation to each CCG to purchase (only) from GP IT Futures Framework	From January 2020
GP Online Consultations	Non-recurrent revenue	To provide online consultation solutions under GP FV	Allocation from established GPFV fund to STPs	From April 2019
Primary Care Networks	Recurrent Revenue & Capital	To provide IT services for PCNs	Revenue and capital digital/IT PCN funding arrangements to be confirmed during 2019	From July 2019

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 Standing Financial Instructions (SFIs).

CCGs should carry out procurement activities which ensure services procured are compliant with the standards described in this operating model. These activities should ensure services, where applicable, are compliant with;

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

CCGs must ensure, as a core & 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).

CCGs are encouraged to collaborate on procurements and make use of appropriate Framework Agreements to ensure best value for money and quality and to reduce procurement workload.

6.1 Procuring GP IT Enabling Requirements

CCGs are encouraged to use an appropriate and NHS approved framework e.g. Health Systems Support Framework (HSSF) to procure GP IT enabling services. With the end of Lead Provider Framework (LPF) contracts CCGs should ensure safe transition to other providers and contracts whilst maintaining or improving quality.

Without precluding providers from offering innovative approaches CCGs should give consideration to the following

(i) services where demand is linked to volumes (eg of devices, users etc) and how incremental/organic growth can be accommodated
(ii) specialist (expert) services (eg training, data quality, project management, information governance etc) what will the available capacity be and how will it be managed?

Further details are given in Appendix D: GP IT Specification Commissioning Support Pack

CCGs may procure GP IT enabling services from providers not on an approved framework – 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.

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 provider organisation meets 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 e.g. as Data Processor. This should include any required data Processing Agreements
- Ensure all the terms of the CCG-Practice agreement apply in full.
- Is governed either by a fixed term formal contract or fixed term formal NHS Service Level Agreement. 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.
- Provide demonstrable value of money.
- Complies with the CCG's Standing Financial Instructions.

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

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 and also;

- 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

The following organisational standards are required i.e. mandatory when commissioning GP IT Services;

- NHS Information Governance – to demonstrate compliance with all mandatory assertions in the NHS Data Security and Protection Toolkit (DSPT) for the relevant organisation type.
- Where the organisation is not accredited to ISO 27001 for Information Security Management it will by June 2021 achieve accreditation to Cyber Essentials Plus (CE+)

Organisational standards may apply to whole organisation and all services it provides internally and externally or may be defined in more detail e.g. within the Information Security Management System (ISMS) scope. Commissioners should seek assurance that any standard compliance or certification from a provider fully applies to the scope of the services being commissioned.

Note: individual requirements have applicable standards assigned as required (see Appendix A).

6.4 Procuring Essential Clinical System Capabilities

Under the GP IT Futures Framework (which replaces GPSoC Framework) CCGs will use notional allocations of funds to procure from the GP IT Futures Framework solutions 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 SFIs (through utilising the GP IT Futures Framework). This will require mini-procurement processes to take place within the catalogue capability options.
- Ensure value for money is secured.
- Ensure practices are able to choose their preferred foundation solution from the accredited catalogue.

6.5 Procuring GP IT Equipment

When procuring GP IT equipment using NHS capital funds (either Business As Usual or ETTF) CCGs will adhere to NHS England financial guidance, internal SFIs and procurement legislation. The National Commercial Procurement Hub framework contracts which offer the best value for money should be used wherever possible. CCGs have access to the National Commercial & Procurement Hub for advice and support in procurement of GP IT equipment using ETTF 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 National Commercial and Procurement Hub Framework where such services and systems will interface with NHS provided systems or operate on NHS managed infrastructure. Practices procuring practice business support systems and local clinical system & 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.

Any practice procured software, digital system or equipment which utilises NHS systems or managed infrastructure must be approved by the CCG (CCG-Practice agreement). Such approvals should not be unreasonably withheld.

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.

Software, browsers and operating systems not supported or maintained by the supplier must not be used on NHS managed infrastructure.

7 Assurance

7.1 Primary Care Digital Maturity Assurance Tool

The Primary Care Digital Maturity Assurance Tool (PCDMAT) now 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 PCDMAT will continue to be used in support of this operating model.

Data will be sourced annually from the following:

- NHS Digital – Organisation Data Sets (ODS).
- General Practice annual e-Declaration (eDEC).
- CCG Annual GP IT Survey.
- NHS DSPT– GP Submissions (formally GP Information Governance Toolkit).
- NHS Digital Patient Online data.

The PC DMAT indicators (from April 2019) are shown in Appendix C. These will continue to refer to GPSoC Framework as the GP IT Futures Framework will not be delivering clinical system capabilities during the indicator collection periods in 2019/20. Changes to the indicator set to reflect GP IT Futures Framework will be introduced for 2020/21.

Where an indicator is relevant to a requirement described in this operating model the indicator(s) is shown assigned to that requirement (appendix A).

The PCDMAT will move into the national Population Health Management Dashboard (PHMD) from 1st April 2019. This quality improvement dashboard has been developed to bring together a number of other national datasets to support an across system and population health view of health and care data and uses presentational formats which have been developed to support enablement of peer review and benchmarking. The PHMD dashboard includes presentation of measures and indicators at PCN and Integrated Care Systems (ICS) levels.

The inclusion of GPIT indicators to the PHMD provides an additional benefit opportunity for practices and commissioners to access and use both the GP IT indicators and the new and emerging PCN and ICS measures which are also available within.

From the 1st of April 2019 practice GP IT data collected through the General Practice Annual Electronic Declaration (eDEC) will move to new data collection systems and websites managed by NHS Digital.

Practices will need to obtain a new user account to be able to login to be able to view/edit and submit the eDEC.

7.2 Clinical Commissioning Group Assessment Framework

During 2019/20 NHS England will explore how the progress and quality of digital technology supporting general practice can be incorporated into the CCG Assurance Framework

8 Addressing the Challenges

This revision of the Operating Model builds on the successful approach of preceding versions but also looks to address six contemporary challenges

8.1 Challenge 1. Keeping General Practice Safe

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

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

(i) Significant system failure which may severely disrupt or close down essential practice operations with almost immediate effect. Workarounds may be limited depending on the nature and extent of the system failure.

(ii) The loss of data (patient records) or loss of access to data, whether arising from failure of digital systems or otherwise will present high impact risks to the practice in (i) operational continuity (ii) clinical safety (iii) corporate criminal liability (iv) potential regulatory action from the ICO including fines.

(iii) Errors, faults or algorithmic based outputs from embedded logic and knowledge bases in software which processes patient information may lead to clinically unsafe recommendations.

Minimising the risk

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 will form the foundation of minimising these risks.

The CCGs will 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 DPO
- Cyber Security management and oversight
- Clinical Safety 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.

Information Governance

As data controllers and “public authorities” general practices have specific regulatory, legal and contractual responsibilities but they need to be supported with access to specialist services who can provide expert advice and specific areas of support.

As data controllers and “public authorities” general practices are legally required to designate a DPO. Practices will have access to an information governance support service which will provide advice to the practice designated DPO on Data Protection and Information Governance matters. CCGs will commission a DPO service offering a named DPO to practices (which can be shared between practices). Funding has been made available in the CCG baseline to support this requirement. 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 also complete the NHS GP DSPT as a requirement under the new CCG-Practice Agreement. Practices are responsible for completing and submitting their own DSPT.

Clinical safety & medical devices

Previously Information Governance and Clinical Safety Assurance services were commissioned by NHS England Regional teams, from 1st April 2018 this commissioning responsibility for general practice moved to CCGs.

As a core & mandated GP IT enabling requirement CCGs should ensure they and their practices have access to a procurement support service. This in conjunction with the Clinical Safety Service should support CCGs and individual practice apply clinical safety standards when procuring clinical systems and system modules.

DCB0129 Clinical Risk Management: its Application in the Manufacture of Health IT Systems

1. Where CCGs or individual practices procure clinical software from routes other than GPSoC Framework or GP IT Futures Framework (which both include clinical safety DCB0129 as part of their assurance and accreditation process) steps should be taken by the procuring authority (i.e. CCG or General Practice) during procurement to ensure the supplier has applied DCB0129 in the development and manufacture of the software.

DCB0160 Clinical Risk Management: Its Application in the Deployment and Use of Health IT Systems

- CCGs and individual practices should apply DCB0160 in the deployment of new clinical systems and should apply DCB0160 in the regular review of business and clinical process (to 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).

The Medicines and Healthcare products Regulatory Agency (MHRA) also operates the Central Alerting System (CAS) which 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, including independent providers of health and social care.

From October 2019 there will be a contractual requirement for practices to:

- register a practice email address with the CAS team and to monitor the email account to act on CAS alerts which are received. All alerts issued to the account will have been vetted to ensure they are relevant to GP practices
- notify the CAS team if the email address changes to ensure continued receipt of alerts; and
- register mobile phone details with the CAS team, which will only be used as an emergency back-up to email for text alerts when e-mail systems are down.

It is advised that all practices complete this registration process as soon as possible, prior to the October 2019 deadline.

Medical Device Directives

Where CCGs or individual practices procure clinical software or medical devices which interact with the clinical software and patient record from routes other than GPSoC Framework or GP IT Futures Framework (which both include clinical safety & medical device regulation as part of their assurance and accreditation process) steps should be taken during procurement to ensure the supplier has applied EU Medical Devices Regulation (2017) if applicable to the product in the development and manufacture of the software or device.

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.

European Falsified Medicines Directive

The 'Safety Features' Delegated Regulation, part of the EU Falsified Medicines Directive (FMD), came into force in the UK on 9 February 2019. MHRA and the Department of Health & Social Care (DHSC) continue to work with stakeholders across the supply chain to support implementation to the required standard. General Practices as healthcare institutions are legally required to comply.

Additional software and hardware will be required to meet this new capability. This will apply to

- All practices (approximately 7,200) where medications are personally administered (e.g. vaccinations) – the software and the supporting GP IT enabling requirements are a core & mandated requirement. Designated GP IT funding sources ie GP IT Futures notional CCG allocations, GP IT Revenue and GP IT Capital can be used to support these requirements as appropriate.
- Dispensing practices (approximately 1,000) operating under pharmaceutical dispensing regulations will be required to meet this capability for the dispensing service. As this is part of the dispensing function provision of the software and enabling requirements are currently outside the scope of this Operating Model

Continuity of General Practice Records

The transfer of records between systems can result in record integrity and continuity issues.

> NHS England and NHS Digital will continue working with system suppliers to address and resolve this.

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.

> 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.

The persistence of paper patient records in general practice can result in record continuity and integrity issues and is resource intensive

> NHS England will continue to work with stakeholders and professional bodies to develop national standards leading to the commissioning of approved services. CCGs are advised to defer further commissioning of GP records digitisation until such standards and national guidance become available to support practices with the digitisation process.

Locally procured digital systems & technologies

Systems and technologies procured locally, e.g. by practices or federations, 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 provided to practices from such systems is often invaluable to the operation and efficiency of a busy general practice.

To support practices, make safe procurements and utilise such digital systems and technologies with confidence this operating model puts in place the following;

- Practices, CCGs and GP IT delivery providers should follow the (core and mandated) capabilities 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 GP federations (and other GP collaborations) should make full use of the GP IT Futures Framework to procure from an accredited catalogue.
- A simple checklist for CCGs and practices considering local procurement has been provided in the operating model (Appendix F).
- Software, browsers and operating systems not supported or maintained by the supplier must not be used on NHS managed infrastructure.
- The contract holder (e.g. 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.

NB This does not include personal devices and applications owned by practice staff. These should not be used on the managed GP IT Infrastructure or connected to practice clinical systems (unless the access is through a public access route e.g. public WIFI or patient online digital capabilities).

Remote Access

Remote access to practice clinical systems and managed GP IT Infrastructure is required to support mobile and remote working for practice staff. See Appendix A for further details. Remote access solutions must not be used which bypass or otherwise reduce the effectiveness of security measures, including smartcard access or the NHS Identity service within the GP IT Futures Framework solutions, the National Digital Services and the Managed GP IT Infrastructure. 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.

High Severity Incident Management

High Severity Cyber Incident Management, Business Continuity & Disaster Recovery

All parties i.e. individual practices, CCGs, GP IT delivery partners, NHS England and NHS Digital have responsibilities to:

(i) Take measures including technical, planning and organisational policies and operating procedures to minimise the risk of cyber incidents.
(ii) 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 (e.g. 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 initiated by third parties (e.g. 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.

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 & 88 for further detail). 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.

- NHS Digital have written guidance on reporting data breaches. This can be accessed on the DSP Toolkit
- 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 i.e. individual practices, CCGs, 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.

Clinical Safety Incidents

All NHS funded organisations in England have a role to play in reporting and managing high level clinical safety incidents. Clinical safety incidents which require to be reported as SIRIs should continue to be reported through the Strategic Executive Information System (STEIS) or any successor reporting system.

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

NHS Digital has issued a guide to logging clinical safety incidents and depending on the nature of the incident (e.g. scope, severity, risks/impact) and the mitigation/solution (e.g. root cause and fix delivery) may be escalated further

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

Loss of access to patient records

Management of a High Severity Total Loss of access to Patient Records Incident. This may be due to a number of possible causes e.g. 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 as well as response to threats to data security will also include 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 and control the role of a practice Disaster Recovery 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 Disaster Recovery Plans.

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 & infrastructure age, specification, concurrent applications and configuration
- external threats

Where the digital system performance for any user is impacted to the extent that it obstructs 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.

8.2 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

Replacing GPSoC framework with GP IT Futures Framework embedded in this Operating Model.

Under the terms of the GP contract 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 can provide these services under 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 (8.1 Challenge 1. Keeping General Practice Safe*)* 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 contract obligations. These core & mandated requirements include essential clinical system capabilities which must:

1. Be provided (funded) by the NHS for eligible practices with a signed CCG-Practice Agreement.

2. Be accredited (GPSoC Framework until December 2019, GP IT Futures Framework from January 2020).
3. Be available as foundation solutions to individual practices to choose from the accredited systems to meet the foundation capabilities.

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.

GP IT Futures Framework

Clinical systems, as provided through GPSoC Framework until December 2019, are now defined through clinical digital capabilities. A number of these capabilities, including six foundation capabilities, are categorised as core and mandated and referred to in this document as Essential Clinical System Capabilities. All practices must be provided with these capabilities through accredited solutions from the GP IT Futures Framework.

For these capabilities

1. The solutions are funded by the NHS for eligible practices with a signed CCG-Practice Agreement.
2. The solutions must be accredited (GPSoC Framework until December 2019, GP IT Futures Framework from January 2020).
3. Foundation Solutions which meet the Foundation Capabilities can be chosen by individual practices from the accredited systems offered in the catalogue.
4. Solutions for other capabilities should be called off by the commissioning CCG in collaboration with local practices from the accredited systems offered in the catalogue.
5. Certain non-foundation capabilities may be provided as an embedded part of the procured Foundation Solution at the individual Foundation 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 GP IT Futures 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 buying catalogue and include critical areas such as SNOMED CT, Interoperability, Clinical Safety and Security.

Up until the end of the GPSoC Framework (December 2019) these capabilities will be sourced through a local call off agreement from the GPSoC Framework Contract as a single deployment per practice of the GPSoC Principal Clinical System.

Foundation Solutions which meet these capabilities must be selected from the GP IT Futures Framework before the GPSoC Framework closes (January 2020).

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

Local (practice based) clinical system servers are **not recommended** under the new GP IT Futures Framework and will not be assured. Where existing clinical systems use local practice based clinical servers and these clinical systems are available on the new GP IT Futures Framework catalogue system suppliers **may** allow such clinical systems to be hosted locally subject to assurances on how the security and resilience risks of local hosting can be managed. After March 2021 however local practice based clinical system hosting will not be available.

- CCGs and Practices should work with their suppliers to migrate any local hosted solutions to accredited hosted solutions before March 2021.
- CCGs and Practices are recommended they do not deploy any new local hosted solutions.

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) 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 e.g. 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

Support for GPs and CCGs locally prioritise and invest in technologies which improve practice efficiency and 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. The development of Primary Care Networks will in many cases be the driver for primary care transformation and as such will offer local insight and intelligence on which of these digital capabilities are most needed by a locality and how they might be effectively delivered. This does not mean these capabilities are of less importance. Local investment in the right digital enablers for service improvement and transformed care is necessary to 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.

8.4 Challenge 4: Supporting new models of care and contracts

Support for the new PCN DES & Integrated Care Systems and the new GP contract.

Where GP Contractors are eligible for NHS digital services the new CCG-Practice Agreement will provide clarity and assurance to both parties on the requirements for the provision and use of digital services provided to practices under this operating model.

Primary Care Networks (PCN)

The new five-year framework for GP contract reform to implement The NHS Long Term Plan *announced the introduction of PCNs through a DES.* 100% geographical

coverage of the Network Contract DES is expected by July 2019 involving an additional 20,000+ staff by 2023/24. 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 and these services become established. GP IT enabling requirements will support PCN staff in the same way as existing practice staff.

Sub-contracting of services by practices.

Practices will be eligible for receipt of NHS Funded digital services as described in this operating model if they hold a GP contract. A signed CCG-Practice Agreement is also required by the CCG to provide services. 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 may include:

1. GP Federations and similar collaborative organisational arrangements set up as discrete organisational forms to provide services to general practice contractors.
2. Specialist private providers contracted to deliver online digital services to the practice.

Note: this does not apply to a contract for services with a health care 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.

The practice must contractually ensure relevant standards as described in this operating model are applied by the sub-contracted provider when using digital systems to provide services to the practice particularly in respect of clinical safety, data quality, information governance and cyber security. The use of the GP IT Futures Framework, from which the sub-contracted provider and practices can independently procure, is encouraged to ensure selected solutions meet the appropriate standards.

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

The new GP contract gives clear direction on restrictions on advertising and hosting private GP services, stating that from 2019 it will no longer be possible for any GP provider either directly or via proxy to advertise or host private paid-for GP services that fall within the scope of NHS-funded primary medical services. These restrictions apply to the use of digital services provided by the NHS to practices under this operating model.

The sub-contracted provider is not eligible to directly receive NHS funded digital services under this operating model and the CCG is not required to provide such services. GP IT Funds are not directly available to sub-contractors.

The practice may inform the CCG that its sub-contracted provider requires access to use certain NHS Digital Services provided to the practice under this operating model. The CCG may agree at its discretion, not to be unreasonably withheld, to provide the sub-contracted provider with this access providing the CCG is assured that the cost of providing digital services to this practice is proportionate to other similar GP contracts they support (based on a cost per registered patient basis) and that controls to ensure compliance with relevant standards as required in this operating model including those relating to clinical safety, data quality, information governance and cyber security are in place.

The origins of this Operating Model sit with the contractual obligation on the NHS to provide clinical systems and IT enabling services to general practice through the GP contract. New contracts may extend beyond offering Primary Care Essential Services to a registered patient list e.g. community services, urgent care, minor injuries etc. Although this may already be the case with some APMS contracts and GP Special Interests the possible scale of new contracts will require definitive guidance as these contracts develop.

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

Focus on the GP contract patient facing digital commitments

Patient facing Capabilities

Three citizen facing capabilities are necessary to support contractual requirements for practices to offer:

- Repeat prescription requesting
- Appointment requesting
- Viewing patient record

Under GPSoC Framework these capabilities are enabled through subsidiary modules under Lot 1 and are nationally funded. From December 2019 these capabilities, which are core & mandated under this operating model, will be available through accredited solutions from the GP IT Futures Framework. CCGs may use the GP IT Futures notional funding allocations to provide these capabilities. The NHS App once enabled for all practices with full functionality will offer an alternative, nationally funded solution, to deliver these capabilities.

The GP Online Consultations Systems Fund continues to be supported through the General Practice Forward View online consultation funding (£45m per annum over 3

years) and continue as an enhanced capability allowing local prioritisation to match individual practice readiness for this business change.

The new 5-year GP contract framework sets out a defined roadmap for citizen facing capabilities. These measures will become contractual requirements over time, subject to available IT infrastructure. NHS England and GPC England expect practices where feasible to make progress in 2019/20 towards meeting those requirements and CCGs should support practices in this development through this operating model.

- **From April 2019**
    - New practice registrants have full online access to prospective data, subject to safeguards for vulnerable groups and third party confidentiality and system functionality
    - **From July 2019**
        - all practices will ensure at least 25% of appointments are available for online booking
- **By April 2020**
    - all practices will be giving all patients access online to correspondence, as the system moves to digital by default (with patients required to opt-out rather than in)
    - all patients will have online access to their full record, including the ability to add their own information, subject to national negotiations, existing safeguards for vulnerable groups and third-party confidentiality and system functionality.
    - all practices will offer online consultations to patients. The online consultation fund established through GP Forward View will be provided to the system to stimulate the uptake and use of online consultation systems
      all practices will need to have an up-to-date and informative online presence
- **By April 2021**
  all patients will have the right to online and video consultation by April 2021

Electronic prescriptions and electronic repeat dispensing

- **From April 2019**
    - All practices will be offering and promoting electronic ordering of repeat prescriptions and using electronic repeat dispensing for all

patients for whom it is clinically appropriate, as a default from April 2019

- **During 2019/20**
    - Once EPS Phase 4 has been installed at a practice, practices must use electronic prescriptions if they are satisfied EPS is working properly and apart from some specific exemptions ie patient choice or clinical need.

8.6 Challenge 6: Building on success

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

In revising the operating model NHS England has, with the support of the profession, considered the following:

- That both GPSoC Framework and Operating Model and their preceding models and frameworks have, with strong clinical engagement and contractual levers, been successful in realising highly digitised general practice with a large percentage of paper free processes.
- That the GP contract continues to make a number of obligations and recommendations regarding digital services on the NHS and GP contractors
- That general practice leads the NHS in the adoption of patient facing digital systems
- That we must not lose these hard-won gains in developing a new approach to meet new world demands.

The approach taken has therefore been 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)

9 Transition Arrangements

The following describes the significant transition arrangements arising from the release of version 4 of the operating model. More detailed transition actions are given against individual capabilities documented in Appendix A.

1. **Implementation of new CCG-Practice Agreement**
    - Publication of the CCG-Practice Template Agreement by August 2019.
    - CCGs to develop local schedules for incorporation as appendices into CCG-Practice Agreements locally by 30th August 2019.
    - CCGs and GPs to sign agreements by 31st October 2019.
    - Current CCG-Practice agreements remain in place until the practice and CCG sign the new agreement.
      Unsigned agreements to be escalated to NHS England regional teams by 30th November 2019.

2. **Migration from GPSoC Framework to the new GP IT Futures Framework**
    - Capabilities will be available to be procured as soon as a solution has gone through compliance and is available on the GP IT Futures Framework – the earliest expected date for this will be July 2019.
    - CCGs will need to ensure that they have made necessary arrangements to ensure continuity of service on 1 January 2020.
    - CCGs will be notified of notional funding allocations to support GP IT Futures Framework from 1st January 2020 by September 2019.
    - Notional funding allocations will be notified in advance of the catalogue being open for buying. The funding is moving towards a per patient allocation formula, but transitional arrangements will be put in place to ensure that practices have the services they need under the new arrangements.

3. **Application of the Operating Model to Primary Care Networks**.

4. **Exit from LPF GP IT contracts. Re-procurement of GP IT Services.**

5. **Managing changes to GP IT Enabling requirements**
    - Where the requirements have changed since the previous operating model (2016 V3 & 2018 Addendum) 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 e.g. where there is an urgency or time pressure for the change to be effective.

6. **Primary Care Digital Maturity Assurance Tool**
    - From the 1st April 2019 the Primary Care Digital Maturity Assurance Tool (PC DMAT) will move into the Population Health Management Dashboard (PHMD) and practice GP IT data collected through the General Practice Annual Electronic Declaration (eDEC) will move to new data collection systems and websites managed by NHS Digital. From 1st April 2020 the PC DMAT indicator set will reflect the GP IT Futures Framework and not the GPSoC Framework.

7. **Cyber Security**
    - By 1st June 2021 GP IT Delivery Partners who are not accredited to ISO 27001 for Information Security Management must have achieved accreditation to Cyber Essentials Plus (CE+). CCGs should ensure, where necessary, these organisations are taking the required measures to meet this deadline.
    - By 14 January 2020 replace, remove or isolate Windows 7 operating systems on managed devices. Replacements through the Windows Managed Service must include Advanced Threat Protection (ATP). A custom support agreement (CSA) must be in place (at local cost) for any remaining use of Windows 7 after this date.

8. **Health & Social Care Network (HSCN)**
    - August 2020: All GP connections to HSCN to be completed

APPENDIX A – Schedule of GP Digital Requirements & Capabilities

Essential clinical system 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 are sourced through the GP IT Futures Framework using the online catalogue.

For these capabilities

- The solutions are funded by the NHS for GP Contract holders.
- A signed CCG-Practice Agreement is in place
- The solutions must be accredited through GPSoC Framework until end December 2019 and the GP IT Futures Framework from January 2020.
- Foundation Solutions for those capabilities described as GP IT Futures Foundation Capabilities will be determined by individual practices from the accredited systems offered in the GP IT Futures Catalogue.
- Solutions for other non-foundation capabilities will be determined by the commissioning CCG in collaboration with local practices from the accredited systems offered in the GP IT Futures Catalogue.
- 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.

Up until the end of the GPSoC Framework contract (December 2019) these capabilities will be sourced through a local call off agreement under the GPSoC Framework Contract as a single deployment per practice of the GPSoC Principal Clinical System.

Note: The Read v2 and CTV3 clinical terminologies are deprecated standards. All GP IT service providers must be aware that there are codes in patient records that are only accessible through SNOMED CT. All Specifications and systems should now utilise SNOMED CT rather than Read codes.

Solutions to meet these capabilities must be selected from the GP IT Futures Catalogue once it becomes available (January 2020).

These capabilities are listed in the table on the next page.

Capabilities available through GP IT Futures Framework

Capability	Description	Notes
GP Referral Management	Supports recording, reviewing, sending, and reporting of Patient Referrals. Enables Referral information to be included in the Patient Record.	Fulfilled through GP IT Futures Foundation Solution
Prescribing	Supports the effective and safe prescribing of medical products and appliances to Patients. Information to support prescribing will be available.	Fulfilled through GP IT Futures Foundation Solution
Recording Consultations	Supports the standardised recording of Consultations and other General Practice activities.	Fulfilled through GP IT Futures Foundation Solution
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.	Fulfilled through GP IT Futures Foundation Solution
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.	Fulfilled through GP IT Futures Foundation Solution
Appointments management – GP	Supports the administration, scheduling, resourcing and reporting of appointments.	Fulfilled through GP IT Futures Foundation Solution
Appointments Management – Citizen	Enables Citizens to manage their Appointments online. Supports the use of Appointment slots that have been configured in the GP	Citizen facing capabilities; Commissioning CCG collaborates with practices to determine an accredited solution from the GP IT Futures

	appointments management system	Catalogue (accessed directly or through the NHS App).
Prescription Ordering – Citizen	Enables Citizens to request medication online and manage nominated and preferred Pharmacies for Patients.	Citizen facing capabilities; Commissioning CCG collaborates with practices to determine an accredited solution from the GP IT Futures Catalogue (accessed directly or through the NHS App).
View Record – Citizen	Enables Citizens to view their Patient Record online. Includes viewing of full record, clinical & administrative documents and Pathology & Radiology test results by patients and patient proxy.	Citizen facing capabilities; Commissioning CCG collaborates with practices to determine an accredited solution from the GP IT Futures Catalogue (accessed directly or through the NHS App).
Communication Management	Supports the delivery and management of communications to Citizens and Practice staff.	Commissioning CCG collaborates with practices to determine an accredited solution from the GP IT Futures Catalogue Requires as an enabler electronic messaging for direct patient communication (i.e. SMS or equivalent).
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 available through foundation capabilities.	Commissioning CCG collaborates with practices to determine an accredited solution from the GP IT Futures Catalogue
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.	Commissioning CCG collaborates with practices to determine an accredited solution from the GP IT Futures Catalogue
GP Extracts Verification	Aggregated data is extracted from practices	Commissioning CCG collaborates with practices to

	Clinical Systems via the General Practice Extraction Service (GPES) and sent to the Calculating Quality Reporting Service (CQRS), both operated by NHS Digital. 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.	determine an accredited solution from the GP IT Futures Catalogue
Scanning	Support the conversion of paper documentation into digital format preserving the document quality and structure.	Commissioning CCG collaborates with practices to determine an accredited solution from the GP IT Futures Catalogue Requires as a GP IT enabling requirement compatible scanning hardware.
Medicines verification	To enable compliance with EU Falsified Medicines Directive (FMD) for Individually Dispensed medications e.g. vaccinations (excludes dispensing services).	Requires as a GP IT enabling requirement compatible scanning hardware.

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 i.e. infrastructure, equipment, training and deployment support for practices.
- Alternative (local arrangement) systems should not be used and should not be funded by CCGs.
- Through the CCG-Practice Agreement practices are required to comply with the supplier's end-user terms and conditions accepted by the contract holder (e.g. 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 GP IT Futures Framework.

These services are listed below.

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 – GP (CIS)	CIS is an electronic system for registering and issuing smartcards. Registration authorities use the service to control smartcard access for over 800,000 smartcards used to access NHS applications.	Through NHS Spine Portal using Registration Authority issued smartcards.
Summary Care Record	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	Accessed through accredited Clinical System Capabilities.

	patient's direct care. There is a minimum core data set (medications, allergies and adverse reactions) but with patient consent, an enriched SCR can now be created automatically to include additional patient data (e.g. significant medical history, immunisations, etc.).	
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 available to practices, for a new patient's first and later consultations and significantly reduces the need to print records.	Accessed through accredited Clinical System Capabilities.
Electronic Prescribing Service	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	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.
CQRS & GP Extraction Service (GPES)	The General Practice Extraction Service (GPES) collects information for a wide	Accessed through accredited Clinical System Capabilities.

	range of purposes, including providing GP payments. It works with the Calculating Quality Reporting Service (CQRS) and GP clinical systems as part of the GP Collections service.	
Spine	The spine allows information to be stored and shared securely through national services such as the Electronic Prescription Service, Summary Care Record and the e-Referral Service. 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 & Health Care (MESH)	The service supports both clinical and business data flows. It is made up of two elements, the MESH client software, which is predominately integrated into supplier provided applications installed at end-sites, and the central MESH server, which is located within the Spine Core Messaging Service. The MESH client allows secure transfer of data between the end site application and the central MESH server. The MESH client transfers data, over an encrypted link to the central MESH server. The central MESH server then stores this data until the intended recipient site connects to the service and with its MESH client downloads the data addressed to it over an encrypted link.	Accessed through accredited Clinical System Capabilities.
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	Directly by patient. If their GP practice is connected, patients can register and verify their identity. The NHS App

	People can: • check their symptoms using the health A-Z on the NHS website. • find out what to do when they need help urgently using NHS 111 online. • book and manage appointments at their practice. • order their repeat prescriptions. • securely view their practice medical record • register as an organ donor. • choose whether the NHS uses their data for research and planning. • Use the NHS App as the gateway for access new and innovative digital services as they become available All functions of the app should be fully available across England by 1 July 2019, after all practices are connected.	is available to the public on Google Play and Apple app stores.
NHS Login	The NHS App is the first major platform to use NHS login, a single, easy to use system for verifying the identity of people who request access to digital health records and services.	Directly by patient. Most people aged 16 or over will be able to verify their identity and register through NHS login.
Data Security & Protection Toolkit	The Data Security and Protection Toolkit 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 toolkit. An online self-assessment tool that enables practices to measure and publish their performance against the National Data Guardian's ten data security standards.	Directly by individual practices.

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.
National Commercial & Procurement Hub	The National Commercial and Procurement Hub support service commissioned by NHS England is able to provide expert advice and guidance to CCGs, practices and legally incorporated practice affiliations on specified areas of procurement. This includes support to CCGs, practices and legally incorporated practice affiliations procuring digital online consultation systems as part of the General Practice Forward View (GPFV) Online Consultation Systems programme and broader investment and procurement in digital solutions intended to transform general practice.	Directly by CCGs, practices and legally incorporated practice affiliations.

GP IT Enabling Requirements

Digital technologies and services necessary to support (ie enable) the National Digital Services and the solutions selected to meet the Essential Clinical System Capabilities (including the Foundation Solutions) needed to deliver the primary care services under the GP contract or as otherwise nationally mandated. Under GP contractual obligations 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 baseline 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.

- Effective Commissioning of GP IT,
- GP IT Support Service Desk,
- IT Equipment Asset Management,

- Software Licence Management,
- Registration Authority,
- NHS Mail Administration & Support,
- Essential Infrastructure,
- HSCN-GP,
- Desktop Infrastructure,
- Local Clinical Server,
- WiFi-GP,
- Remote access to the clinical system at the point of care,
- Electronic messaging for direct patient communication,
- Controlled Digital Environment,
- Cyber & Data Security,
- Information Governance Support,
- Clinical Safety Assurance,
- Digital Services Procurement Advisory Service,
- IT & Digital Services Contract Support,
- Estates Strategy,
- Clinical Systems Training and Optimisation,
- Data quality support & advice,
- Project and Change Management,
- Local Digital Strategy,
- National Digital Services Implementation.

Effective Commissioning of GP IT

Requirement	The commissioning of GP IT services by the CCG to meet GP IT enabling requirements. Note this is an internal CCG function, although CCGs may share or collaborate on this work.
Specialist Support Services	CCG-Practice Agreement • must be signed with all practices. • must be reviewed in the event of significant changes to either party eg organisation merger. • schedules require review not less than every 12 months. GP IT commissioned services • Must be commissioned to required standards (e.g. 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.
Practice Responsibilities	To sign and comply with the CCG-Practice Agreement
Dependencies with other capabilities	National Commercial & Procurement Hub

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 GP Digital Services for all practices. • A Data Processing Agreement where required
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 providers. • As described in the CCG-Practice Agreement in addition to individual practice annual service reviews, where local IT and system performance issues should be identified, individual practices can request an additional service & infrastructure review.
Other Controls	CCGs must maintain • Schedules as required in the CCG-Practice Agreement • Individual annual practice service reviews. 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	PC DMAT: • (IND20.0) GP IT services are commissioned and contracted with robust and clear service specifications • (IND21.1) All practices sign the CCG - practice agreement v2 • (IND24.0) The CCG has completed a formal review of IT Services with each Practice in the last 12 months. • (IND150.0) Clear standing financial protocols are in place between commissioners and delivery organisations to ensure commissioners comply with their SFIs. Clear reporting, monitoring and review arrangements established to ensure CCG oversight of GPIT funding and expenditure, with clear escalation points agreed. • (IND155.0) Service specifications for commissioning of clinical services, encompass core digital requirements, including, but not limited to data management and reporting, data security, data sharing, systems access, digital technology requirements

	• (IND157.0) CCG has contracted for GP IT enabling services ensuring value for money through effective use of national framework contract or other robust procurement in adherence with SFIs and procurement legislation.
Actions Required & Timescales	All practices and CCGs are required to sign the new CCG-Practice Agreement by 31st October 2019.

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 within the Summary of Services (Appendix 1) in the CCG-Practice Agreement.

	• Where 3rd party support is not available for required incident or problem management e.g. when outside 3rd party support hours the end user (practice) will be advised on timescales and any practical workarounds. The GP IT Service desk provider remains responsible for the incident until the 3rd party can take action to resolve. Availability: High Severity Incident Support Access must be available for out of hours high severity service incident alerting, logging and escalation in accordance with the approved business continuity and disaster recovery plans.
Specialist Support Services	Service Availability: Standard Service Hours; • SLA reporting.
Dependencies with other capabilities	Cyber Security.
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	PC DMAT: • (IND28.0) The GP IT support service desk has current formal accreditation through a recognised (NHS or other industry) scheme. • (IND26.0) CCG Commissioned GP IT support provides consistent support for core GP contract hours (0800 - 1830 Mon - Fri excluding Bank holidays)

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). To develop and maintain a local IT equipment reuse and disposal policy.
Systems and applications	All software and operating systems NHS owned GP IT equipment 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. 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 e.g. for printers and other operating requirements to any standard specified in the local Warranted Environment Specification or as otherwise specified by the manufacturer of the equipment. NHS owned GP IT equipment does not require to be individually insured under practice policies (content insurance) however the practice should take reasonable steps to ensure the physical security of the equipment, protecting against loss, theft or damage. To ensure environmental requirements (eg air-conditioning, fire suppression and power protection) 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.

Dependencies with other capabilities	Controlled Digital Environment General Practice Business Requirements.
Applicable Standards	• European Community directive 2012/19/EU, The Waste Electrical and Electronic Equipment Directive (WEEE Directive) • 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	PC DMAT: • (IND36.0) All NHS owned GP IT equipment is recorded in an accurate asset register. • (IND38.0) All NHS owned GP IT equipment is subjected to an approved IT reuse & disposal policy and procedures - using authorised contractors. This is fully integrated with the asset management system

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 & 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 W10 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 & browser compliant with local WES. Software, browsers and operating systems not supported or maintained by the supplier must not be used on NHS owned GP IT equipment • Anti-virus software, Encryption software and Effective patch and upgrade management for operating systems and anti-virus software must be in place • Microsoft Office will be provided on NHS owned devices.
Dependencies with other capabilities	Controlled Digital Environment General Practice Business Requirements.
Applicable Standards	• NDG standard 8
Applicable Guidance	• CareCERT Best Practice Guides
Assurance	PC DMAT: • (IND37.1) All software (including operating systems) used on managed GP IT infrastructure by the practice must be approved and recorded on a software asset & licence register which must confirm the software is appropriately and legally licenced for such use.

Registration Authority

Requirement	A Registration Authority is a function, usually within an NHS organisation, that carries out the identity checks of prospective smartcard users and assigns an appropriate access profile to the health professional's role as approved by the employing organisation. Smartcards are required to access NHS Spine information systems and registration authorities' roles and responsibilities are defined by NHS policy.
Transactional Support Services	Availability: Operational Support Hours • Unlocking of smartcards • Position Based Access Control (PBAC) configuration Availability: Standard Service Hours • Issuing of smartcards (including ID checks / printing etc). • Provide practices with a facility to notify the RA Services Provider when practice staff leave the practice organisation or no longer require RA access to the practice, and ensure access is removed within the agreed performance standards for user account management.
Specialist Support Services	Availability: Standard Service Hours • Registration Authority service including policing 'Access Policy' and the delivery and management of role-based or position-based access control and issuing of smartcards. • Training of practice RA managers and sponsors. • Support for software to support national systems for example.) Identity Agent, CIS. • Ensure adherence to access security policy. • Advise practice RA managers and RA sponsors of configuration of business functions, completion of documentation and use of RA systems (for example. reset PINs). • Involvement in national project roll out such as attendance at project boards to support project delivery. • Production of RA reports
Systems and applications	Identity Agent. CIS
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

Dependencies with other capabilities	Care Identity Service
Applicable Standards	• National Registration Authority Policy. • NDG Standard 4. • Only accredited suppliers can provide this service.
Applicable Guidance	• Registration Authority Operations and Process Guidance • Registration authority governance

NHS Mail Administration & Support

Requirement	The local administration of NHS Mail accounts.
Out of Scope	National NHS Mail Service Desk. Support for email solutions other than NHS Mail.
Transactional Support Services	Availability: Standard Service Hours • Creation & deletion of user and email accounts. • Password resets, account unlocking etc. • Setting up shared mail boxes and authorising 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 daily monitored NHS Mail account to receive clinical documentation. This will support (i) the GP contract requirement by April 2020 that practices will no longer use facsimile machines for either NHS or patient communications. (ii) the GP contract requirement from October 2019, practices will register a practice email address with MHRA CAS alert system and monitor the email account to act on received alerts where appropriate. 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.
Dependencies with other capabilities	NHS Mail Software License Management
Applicable Standards	• NDG Standard 4 • NHS Mail Acceptable Use Policy
Applicable Guidance	• NHS Mail Support Portal
Actions Required & Timescales	By April 2020: Practices will no longer use facsimile machines for either NHS or patient communications. To support this requirement practices will have at least one securely managed and daily monitored NHS Mail account to receive clinical documentation.

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	Provision, maintenance and technical support of the necessary infrastructure to deliver core & mandated GP IT capabilities, to include: • Network connectivity and access to core GP IT services at point of care, including main to branch site(s) connectivity. • Local network services, including equipment, structured cabling and support. • Interface between locally managed networks and HSCN-GP, nationally managed services (e.g. Windows Managed Services), Legacy N3 and community partner networks • File management, data storage and hosting services for core services. • Provide access to a secure, resilient off-site data storage facility for all practice data required for delivery of clinical services, other than that held in externally hosted applications such as clinical systems and NHS Mail, to a standard not less than tier 3 data centre. Examples include clinical documents e.g. multi-disciplinary Team discussions/clinical case reviews/referral management reviews, clinical protocols etc. • Maximum use should be made of best practice to reduce costs and increase efficiency such as server virtualisation and storage area networks. • All backups of shared data storage are configured and executed to support compliance with the data backup and recovery procedure to allow the agreed RPO (Recovery Point Objective).
Practice Responsibilities	See General Practice Business Requirements Appropriate use of the infrastructure in compliance with the CCG-Practice Agreement.
Dependencies with other capabilities	HSCN-GP. WiFi-GP. Enhanced Infrastructure. General Practice Business Requirements.
Applicable Standards	• Tier 3 data centre. • The GP IT delivery partner and any subsidiary service and infrastructure provider will operate to any prevailing NHS security standards, including the Data Security and Protection Toolkit or equivalent industry standard.

Applicable Guidance	• CareCERT Best Practice Guides • NHS Digital Good Practice Guides • NHS and social care data: off-shoring and the use of public cloud services guidance – NHS Digital • Health and social care cloud security - good practice guide – NHS Digital
Other Controls	• HSCN connection agreements.
Assurance	PC DMAT: • (IND39.0) All practices have secure data storage services available for any electronic patient identifiable and clinical data other than that stored in their GPSOC/GP IT Futures clinical systems and NHS Mail to a standard not less that tier 3 data centre. • (IND39.1) All practices have secure cloud-based data storage services available for any electronic patient identifiable and clinical data other than that stored in their GPSOC / GP IT Futures clinical systems and NHS Mail to a standard compliant with "NHS and social care data: off-shoring and the use of public cloud services guidance".

HSCN-GP

Requirement	All practice premises are required to migrate to Health and Social Care Network (HSCN) connectivity and terminate all legacy Transition Network services (previously known as N3) by the specific dates published by NHS Digital and no later than August 2020. 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. • Asymmetric Digital Subscriber Line (ADSL) services no longer to be procured for primary connectivity and existing ADSL primary connections to be upgraded to superfast broadband, preferably as Fibre to the Premises (FTTP) service or Fibre to the Cabinet (FTTC) service as a minimum, at the earliest opportunity - and no later than March 2020. • All future procurements for network connectivity to existing and new practice premises are required to obtain full-fibre connectivity either as Fibre to the Premises (FTTP) services or Ethernet leased-line services. • Practice premises should consolidate their network connectivity and use HSCN connectivity for both Internet and private network connectivity This will ensure all network connectivity is sufficiently robust, reliable, secure and value for money.
Out of Scope	Network overlays e.g. voice, video, WiFi-GP, remote access, site to site VPNs 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.
Practice Responsibilities	Ensure their practice is covered by an HSCN Connection Agreement signed on their behalf by the appropriate CCG.
Dependencies with other capabilities	• Essential connectivity for consuming and provisioning Internet-based digital services as well as services currently only available over the NHS private network. • WiFi-GP • Essential Infrastructure

Applicable Standards	• The standards for HSCN suppliers known as Consumer Network Service Providers (CN-SPs)
	  ○ HSCN Obligations Framework
	  ○ HSCN Compliance Operating Model -
	  ○ HSCN Compliance Release and Configuration Note
	  ○ HSCN Mandatory Supplemental Terms
	• The HSCN Obligations Framework covers a set of obligations which include adherence to policies and standards for interoperability, service (e.g. service management, testing and assurance) and governance. For example, it requires CN-SPs to provide connectivity services that are interoperable with all other CN-SPs and meet a UK Government assurance standard called CAS-T (CESG Assured Service Requirement for Telecommunications), including ISO 27001.

Applicable Guidance	• HSCN compliance • HSCN migration checklist • HSCN overlays • HSCN Connectivity Options • HSCN Technical Guidance Further information: hscnenquiries@nhsdigital.nhs.uk

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.
Actions Required & Timescales	**From April 2019**: Funding for HSCN-GP included in CCG baseline. **From April 2019**: Asymmetric Digital Subscriber Line (ADSL) services no longer to be procured for primary connectivity and existing ADSL primary connections to be upgraded to superfast broadband, preferably as Fibre to the Premises (FTTP) service or Fibre to the Cabinet (FTTC) service as a minimum, at the earliest opportunity - and no later than March 2020. Where such services are not readily available, CCGs should contact NHS England Regional Teams to discuss options for establishing fibre services to practice premises. **From April 2019**: All future HSCN procurements for existing and new practice premises are required to implement full-fibre connectivity either as a Fibre to the Premises (FTTP) service, where these meets download and upload speed requirements, or Ethernet leased-line service. **By March 2020**: All remaining ADSL services providing the primary connectivity to practice premises to have been upgraded to superfast broadband (FTTC) connectivity as a minimum. GP premises must complete migration to HSCN connectivity and terminate legacy Transition Network (N3) connectivity by the **specific dates provided by NHS Digital relating to the planned cessation of legacy Transition** Network infrastructure (Points of Presence). **By August 2020:** All GP premises must have completed migration to HSCN connectivity and terminated all legacy Transition Network (N3) connections.

	By August 2020: Legacy Transition Network to be decommissioned.

Additional notes

If a CCG has not yet placed orders for HSCN connectivity it should ensure superfast or ultrafast broadband services are ordered as a minimum. If a CCG has recently ordered or installed ADSL connectivity it should be possible to upgrade this to a faster Fibre to the Cabinet (FTTC) service using existing contracts without delaying migration to HSCN.

It is recognised that most CCGs will only recently have procured new HSCN connectivity services to replace their legacy Transition Network connections. CCGs should migrate to these services as planned but prepare to adopt full-fibre connectivity (Fibre to the Premise (FTTP) or lease-line Ethernet) at the next procurement point or sooner if possible.

HSCN is based on commercial grade industry standards for internet provision augmented to provide additional cyber security controls; additional service management controls; and access to the digital services not yet available over the Internet. Despite these additional elements, the cost of connectivity that meets the HSCN standard is in line with or cheaper than equivalent non-HSCN commercial-grade internet or private network connectivity.

Desktop Infrastructure

Requirement	A desktop device support service, which includes provision and maintenance of the managed 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 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, access management and port control on all active desktop devices • Encryption to NHS standards on all mobile/portable devices as outlined in guidance on the implementation of encryption within NHS organisations (NHS Digital): • Remote desktop support management available to 100% of workstations
Specialist Support Services	Availability: Standard Service Hours • Defined and documented standardised desktop image(s), with a formal change control management system. • Compliance testing and installation of standard software products. • Compliance testing of software upgrades with NHS national digital services. • Development and maintenance of a local Warranted Environment Specification (WES) to include (i) minimum specifications for hardware to be used locally (ii) any required standards for operating and maintenance consumables needed for the hardware e.g. printers.
Infrastructure	• The GP IT infrastructure estate supporting GP IT includes desktop computers, laptops, printers and other equipment, as necessary to operate those solutions selected to meet the core and mandated and the enhanced capabilities as provided to the practices. • An agreed desktop Warranted Environment Specification (WES) which as a minimum, meets the national WES and the relevant clinical system requirements. • User desktop workstations and laptops must be locked down and well managed, with advanced tools, processes and policies in place to support diagnosis, repair and updates. Unauthorised users must not be able to install unlicensed and unauthorised software or change critical settings. • 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 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 "Asset Management and Software Licencing Service").
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.
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.
Dependencies with other capabilities	Asset Management. Software Licencing Service. Controlled Digital Environment.
Applicable Standards	• NDG Standard 8. • Information Security Management: NHS Code of Practice • Note and comply with: Guidance on the implementation of encryption within NHS organisations.
Applicable Guidance	• CareCERT Best Practice Guides • Recommendation A local SLA should be based upon an agreed desktop estate volume.
Assurance	PC DMAT: • (IND14.0) There is an agreed local strategy and approach for core GP IT infrastructure & software investment to meet the needs of (i) maintaining existing IT estate required for core GP IT needs (ii) practice organic/incremental growth (iii) practice developments eg mergers (iv) significant primary care developments eg new builds. • (IND15.0) There is a clear agreed local (CCG) budgeted plan for the full funding of all core GP IT requirements for the next 2 years.

	• (IND34.0) The GP IT infrastructure estate supporting core GP IT (includes desktop, mobile, server and network equipment) has a fully documented plan for refresh and replacement. This must include a local WES (Warranted Environment Specification) for such equipment which as a minimum will meet the WES for the principal clinical systems used and any NHS mandated national systems and infrastructure. • (IND58.0) There is a locally agreed WES (Warranted Environment Specification) for GP IT equipment which enables practices to effectively operate concurrently applications necessary to delivery both core and enhanced GP IT.

Local Clinical Server

Requirement	Provision and technical support of any local clinical servers where necessary for the operation of a clinical system (as determined by the vendor's agreed warranted environment specification) purchased under GP IT Futures (see Actions & Timescales below).
Out of Scope	Externally hosted clinical systems Clinical systems not procured through GP IT Futures Framework as a core & mandated capability.
Transactional Support Services	Availability: Operational Service Hours • The integrity of local backup media for any local GP IT Futures clinical systems must be regularly validated (quarterly). Backup media should be replaced when faulty and not less often then every three years. • Replacement and secure disposal at end of life will be part of the IT equipment asset management requirement.
Specialist Support Services	Availability: Standard Service Hours Where local clinical servers are necessary as part of the GP IT Futures clinical solution, these will be secure, maintained and in line with clinical system vendor(s) specifications. These will be: • physically secured (see practice responsibilities), • technically secured, • backed up where persistent clinical data is held, • have an uninterruptible power supply, with battery backup, that incorporates safe automatic power-down in the event of power loss. Where remote access to the clinical server is required • by 3rd parties • by practice staff This must: • be agreed in advance by the CCG. • provided by the CCG to the standards required in this operating model. • or provided by a 3rd party (approved by the CCG) to the standards required in this operating model.
Infrastructure	• Practice based clinical system server (if essential) with HSCN connectivity to meet approved clinical system vendor(s) specification. • This service will include the cost of any local backup media needed for GP IT Futures Foundation Solution.
Systems and applications	• Operating system, including patch management and upgrades, and anti-virus • Software, browsers and operating systems not supported or maintained by the supplier must not be installed or used on local clinical servers. • Users must not be able to install unlicensed and unauthorised software or change critical settings.

Practice Responsibilities	• Physical security, equipment and necessary environmental requirements on practice premises to ensure the equipment is:
	  • physically secure,
	  • accessible only to authorised personnel,
	  • operated in an appropriate climate-controlled environment,
	  • adequate power capacity, surge protected and with managed emergency shutdown protection
	  • provided with adequate fire protection.
	• Where local backup media is required and as applicable the practice will be responsible for managing the local backup process e.g. changing & storing the media.
	• Local backup media must be stored in an appropriate environment and tested periodically to ensure that data is recoverable. An appropriate storage environment for backup media will comprise a fire proof safe, preferably at an offsite location, but certainly somewhere other than the server room if the backup must be stored in the same building. Backup media from the previous evening should be removed and placed into safe storage the following morning.

Dependencies with other capabilities	• Asset Management • Software Licencing Service. • Managed digital environment. • Remote access to the clinical system at the point of care. • Remote access to the clinical system for administrative purposes. • Cyber Security.
Applicable Standards	• Relevant vendors warranted environment specification for the application. • Hosting & Infrastructure standards for GP IT Futures • Note and comply with: NHS Digital Good Practice Guides
Applicable Guidance	• CareCERT Best Practice Guides
Actions Required & Timescales	**From April 2019:** CCGs and Practices are recommended they do not deploy any new local hosted solutions. **By March 2021:** CCGs and Practices should work with their suppliers to migrate any local hosted solutions to accredited hosted solutions.

WiFi-GP

Requirement	WiFi-GP 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 & Security Policies and Guidelines are in place.
Specialist Support Services	Availability: Standard Service Hours • Provision of usage information to CCG commissioners
Infrastructure	Appropriate WiFi-GP services for practices ensuring: • National WiFi-GP security standards are followed. • WiFi-GP service usage does not impact on core Practice activities in particular performance of GP IT Futures Foundation Solutions and NHS national systems. There is compliance with NHS data security & 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. • Web page.
Dependencies with other capabilities	HSCN-GP
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	PC DMAT: • (IND171.0) Within primary care locations WiFi access is available to primary care staff, guests & visitors and public to approved standards.
Actions Required & Timescales	• CCGs to ensure that these overlay services are not disrupted by migration to HSCN-GP services.

	• Where services are in place before migration to HSCN services, ensure continued availability is in place post-migration. • CCGs to continue submitting usage data to NHS Digital • Funding for WiFi-GP (maintenance) included in CCG baseline from April 2019.

Remote access to the clinical system at the point of care

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 consultation at point of care, including any necessary mobile infrastructure. This includes provision, maintenance and return to base support of software and managed infrastructure including mobile devices necessary to support clinical system access at the point of care.
Out of Scope	Any remote access solutions involving the use of personal devices or not part of the managed GP IT infrastructure.
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. The use of mobile computing systems is controlled, monitored and audited to ensure their correct operation and to prevent unauthorised access, supporting DSPT requirements for general practice.
Infrastructure	Availability: Standard Service Hours • 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 as outlined in guidance on the implementation of encryption within NHS organisations (NHS Digital) • Connections between mobile/portable/remote devices to HSCN/N3 and the practice clinical system using public network services (internet) must be encrypted to approved NHS standards. Remote access solutions must not be used which bypass or otherwise reduce the effectiveness of the security measures within the GP IT Futures Framework Services, the National Digital Services and the Managed GP IT Infrastructure (including smartcard access). Refresh Programme: • The CCG will, in collaboration with the practice, determine the number and deployment of mobile devices required for remote access to foundation solutions. • 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.
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.
Dependencies with other capabilities	Asset Management Software Licencing Service.
Applicable Standards	• NDG standard 8 • Information Security Management: NHS Code of Practice • As a minimum note and meet the following: Guidance on the Implementation of Encryption within NHS Organisations.
Applicable Guidance	• Recommendation: The local SLA is based upon an agreed mobile estate volume.
Assurance	PC DMAT: • (IND33.3) The practice principal clinical system is accessible outside the practice for the following purposes: Access from patient homes using mobile technologies (subject to local provider network coverage)

Electronic messaging for direct patient communication

Requirement	Electronic messaging (SMS or equivalent) for direct patient clinical 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 'normal' test results.
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, for direct unidirectional individual patient communication, to be utilised for clinical and associated administrative purposes.
Dependencies with other capabilities	Communication management. Patient Information Maintenance Appointments management – GP
Other Controls	• Privacy and Electronics communications Regulations (ICO). • General Data Protection Regulation (GDPR) • Data Protection Act 2018.
Assurance	PC DMAT: • (IND9.0) All practices have access to SMS (or equivalent messaging system) integrated with the practice principal clinical system to support direct communications with patients.

Controlled Digital Environment

Requirement	The effective and secure management of the GP IT estate and GP Digital Services requires that there is an accurate and contemporaneous record of the digital environment and that the desktop estate can be updated and monitored centrally.
Out of Scope	Practice owned, and practice managed IT equipment not connected to the managed GP IT infrastructure e.g. photocopier, practice telephony system. Personal devices.
Transactional Support Services	Availability: Operational Service Hours • There must be the capability for the central control of desktop security, patch control, access and software installation for all desktops & laptops within the managed GP IT estate. • Provide practices with a facility to notify the GP IT Supplier 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 i.e. 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 equipment will be recorded individually on an electronic database. This will include a unique asset / serial number, location, date installed, planned replacement date. Low value accessory items (e.g. keyboard, mice etc) should be excluded. Where appropriate items can be aggregated e.g. mouse, keyboard, Keyboard, Monitor to a single recordable asset. All IT equipment with data storage must be included. All Windows 7 operating systems must be replaced with Windows 10 operating systems on managed devices by January 2020 through the Windows Managed Service which must include Advanced Threat Protection (ATP). A custom support agreement (CSA) must be in place (at local cost) for any remaining use of Windows 7 after this date.

Dependencies with other capabilities	• Essential Clinical System Capabilities. • Effective Commissioning of GP IT. • GP IT Support Service Desk. • IT Equipment Asset Management. • Software Licence Management. • Essential Infrastructure. • Desktop Infrastructure. • Local Clinical Server. • WiFi-GP. • Remote access to the clinical system at the point of care. • Controlled Digital Environment. • Cyber & Data Security. • Information Governance Support. • Digital Services Procurement Advisory Service. • Estates Strategy. • Local Digital Strategy.
Applicable Guidance	Where centralised technologies are deployed particular attention should be given to security, end user performance and system resilience such that the security, performance and resilience of GP IT Futures Framework solutions and National Digital Services is not compromised.
Assurance	PC DMAT: • (IND184.1) The CCG has implemented a capability for the central control of desktop security, patch control, access and software installation across at least 90% of its managed GP IT devices.

Cyber Security

Requirement	Cyber security management and oversight, including configuration support, audit, investigation, incident management and routine monitoring, relevant to the services and managed GP IT infrastructure • Protective technical and organisational measures to reduce the likelihood and impact of cyber security incidents • Management of high severity cyber security incidents • Oversight of management of low & medium severity cyber incidents • Disaster Recovery and Business Continuity plans for systems and infrastructure relevant to GP IT Services. • Supporting Practice Business Continuity Plans
Out of Scope	Disaster Recovery and Business Continuity Plans for national digital services and for GP IT Futures Framework will be managed nationally, although these should be referenced 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 service incident** alerting, logging and escalation in accordance with the approved business continuity and disaster recovery plans. • Cyber-attacks against General Practice services are identified and resisted. • 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. • Action is taken as soon as possible following a cyber incident with a report made to the senior management within the commissioning CCG and the impacted practice within 12 working hours of detection. • Significant cyber-attacks are to be reported in line with national guidance promptly following detection. • For high severity incidents a Lessons Learned Report (with relevant action plan as appropriate) to be provided to the CCG within 2 weeks of the recorded resolution of the incident on the service desk. • The Data Security Centre operated by NHS Digital offers a range of specialist services that help health and care organisations manage cyber risk and recover in the event of an incident. • In the event of a national cyber incident being formally declared (e.g. by the NHS Digital Data Security Centre) 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 Providers 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 DSP Toolkit for General Practice. • Audit and investigative services are available • Specialist (cyber Security) advice is available • There is a shared HSCN-GP security contact for practices. Monitoring through Active Directory to identify dormant accounts for practice staff and operate a process to archive & disable these. Provide practices with a facility to notify the GP IT Supplier 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). **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 practice activities. • 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 this will trigger a review of the plan. • In the event of the Business continuity and/or Disaster Recovery plan being invoked where services relevant to GP Services were impacted (including IT security threats & incidents) the CCG should receive an initial report within 12 (working) hours of the incident and a full

	report including root cause and remedial actions within 2 weeks of the incident. **Practice Business Continuity Plans** • 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 & 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. **CareCERT advisories**: CCGs must ensure: • CareCERT advisories are acted on in line with suggested timescales. Action on high severity Advisories are evidenced through CareCERT Collect. • Confirmation is given within 48 hours that plans are in place to act on high severity CareCERT advisories. • A primary point of contact for the CCG or its GP IT Delivery Partner to receive and coordinate your organisation's response to CareCERT advisories is registered. Note: Action might include understanding that an advisory 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 48 (actual) hours of a cyber attack.
Systems and applications	• Systems provided under GP IT Futures Framework have their own contracted service level specifications. • National Digital services have their own contracted service level specifications.
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 & 88 for further detail) and if so take prompt steps to report and manage this (see Information governance and support). • Each practice will maintain a business continuity plan (BCP) approved by the CCG which should include a response to threats to data security. • Assurance will be provided through the general practice Data Security and Protection Toolkit which each practice is required under the CCG-Practice Agreement to complete annually.

	• Advice & guidance to support the development of the digital element of practice Business Continuity plans, 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
Dependencies with other capabilities	Information Governance Support. IT Support Desk. Essential Infrastructure. Controlled Digital Environment.

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:
	  • NHS Information Governance – to demonstrate satisfactory compliance as defined in the NHS Data Security and Protection Toolkit (DSPT) for the relevant organisation type.
	  • Where the organisation is not accredited to ISO 27001 for Information Security Management it will by June 2021 achieve accreditation to Cyber Essentials Plus (CE+).
	• and registered for:
	  ▪ NHS Digital CareCERT Collect Access,
	  ▪ NHS Digital CareCERT Alerts.

Other Controls	• General Data Protection Regulation (GDPR) • Data Protection Act 2018 • Primary Medical Care Policy and Guidance Manual.
Assurance	PC DMAT: • (IND2.0) The CCG commissioned service provider for GP IT services will have an annually reviewed & tested Business Continuity Plan and validated IT Disaster Recovery Plan for services critical to GP service continuity. • (IND29.0) GP IT services available include cyber & IT Security advice and oversight, including configuration support, audit, investigation and routine monitoring. • (IND172.0) There is clear assurance process to ensure that GP IT delivery partners action in a timely manner all

	high severity CareCERT recommendations that apply to the local GP IT infrastructure. • (IND180.0) The CCG ensures that the commissioned GP IT Delivery Partner has allocated equivalent senior level responsibility for data and cyber security within their organisation. • (IND181.0) As part of the CCG commissioned IT security and IG service, specialist support for Cyber Security incident reporting and management is accessible to general practices. • (IND182.0) The CCG confirms that their GP IT delivery partner has cooperated and supported on-site assessments undertaken by NHS Digital when requested and is acting on the outcomes and recommendations of the assessment, including the sharing of the outcomes with the commissioner. A NO answer means that the on-site assessment has not yet been undertaken with the GP IT delivery partner. • (IND183.0) The CCG ensures that it commissions GP IT services from providers with the required certification as described in the Operating Model. If the CCG is also the GP IT service provider, that it also meets the appropriate certification.

Information Governance Support

Requirement	Information governance support, guidance and advice to support practice compliance with common-law duty of confidence, records management, information security, DSP Toolkit, Data Protection Act 2018 and Caldicott standards and to ensure all devices and systems are managed and used in a secure and confidential way.
Out of Scope	Legal advice
Transactional Support Services	Availability: Standard Service Hours **Data Breaches** A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed. Any data breach (or near miss) of practice patient personal information will require actions by one or more of the following; • The individual practice as data controller. • National NHS commissioned GP Digital services suppliers as data processor(s). • Local CCG commissioned GP IT provider as data processor AND as specialist support service to practice. • Local health & 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 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 EU 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 compliance** Provide advice and guidance to practices on how to complete the DSPT, including the collection and collation of evidence in support of DSPT submissions. Provide practices with evidence required for DSPT where this is held by the CCG or its commissioned IT providers. **IG consultancy and support** Provision of advice, guidance and support on IG related issues, including existing operational processes and procedures or new business initiatives. Advice and guidance on personal data access (but not extending to legal advice). **IG advice and Data Protection Officer (DPO) Support** Provision of advice, guidance and support on IG related issues including existing operational processes and procedures or new business initiatives to support practice designated Data Protection Officers including existing operational processes and procedures or new business initiatives. To include • Access for Practices during normal service hours to specialist qualified advice on GDPR matters. • Advice on compliance with GDPR obligations • Advice reflecting national guidance on GDPR compliance as it is published. • A review at least annually to identify and improve processes which have caused breaches or near

misses, or which force 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 by March 2020.

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

- All published CareCERT Best Practice and 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, DPIA completion and cyber security considerations where projects involve

- Change of Foundation Solution for the practice (including data migration activities)
- New initiatives involving sharing patient data with third parties
- Merging practices
- Closing practices
- Significant estate developments and new builds
- Deploying new technologies

This is not an exclusive list. Specialist support for projects beyond general advice for example preparing Data Privacy

	Impact Assessments should be resourced as part of the project plan. **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 as set out in the CCG-Practice Agreement in accordance with the digital services acquired and regularly reviewed.
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 EU 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 EU GDPR and Data Protection Act 2018 • Mandatory compliance with the National Data Opt-Out policy by March 2020. Individual practices are responsible for sourcing any legal advice required to support these activities.

Dependencies with other capabilities	Cyber Security Data Security Awareness Training.

Applicable Standards	• Data Security and Protection Toolkit (DSPT)
	• NDG Standards
	• Incident reporting tool for data security and protection incidents within the Data Security and Protection Toolkit
	• As minimum note & comply with:
	  ○ Records Management Code of Practice for Health and Social Care 2016
	  ○ Code of practice on confidential information
	  ○ 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	• CareCERT Best Practice Guides • NHS Digital Good Practice Guides • Patient Online Services in Primary Care - Good Practice Guidance on Identity Verification
Other Controls	• General Data Protection Regulation (GDPR) • Data Protection Act 2018
Assurance	PC DMAT: • (IND8.1) All practices complete DSPT • (IND35.1) Records of processing activities are documented for all uses and flows of personal information • (IND160.0) A GP IG support service is provided as specified in the GP IT Operating Model • (IND158.0) The CCG ensures that appropriate IG and information standards/requirements are clearly specified within any local GP IT service specification and associated service level agreement (SLA) and contractual arrangements with IM&T delivery partners including DSPT completion to required standard. • (IND188.0) Practice has either appointed a Data Protection Officer or has plans to do so
Actions Required & Timescales	CCGs must commission a DPO service, offering a named DPO to practices, from April 2019.

Clinical Safety Assurance

Requirement	Clinical safety assurance advice and support
Out of Scope	The responsibility and burden of effort for Clinical Safety Assessment and assurance under DCB0129 rests with the system developer. This includes any third-party software incorporated into the system. The requirement for this service is to secure assurance from system suppliers that this has been met during procurement or contract review stages.
Specialist Support Services	Availability: Standard Service Hours Ensuring that the necessary standards are met for management of clinical risk in relation to the deployment and use of health software. **Advice and Supporting Assurance** Advise CCG and practices on compliance with: • Clinical Risk Management: Its application in the manufacture of health software DCB0129: during procurement. • Clinical Risk Management: Its application in the deployment and use of health IT systems DCB0160 (where required): during deployment and business as usual. • Medical Device Directive where a system/software (or part of it) is classified as a medical device. **Incident Management** Support and advice for practices in the identification, reporting and management clinical safety incidents (information system related) within practices. **Supporting Projects** Advice for practices and the appointed project teams on Clinical Safety (DCB0160) where projects involve; • Change of 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 e.g. 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.
Practice Responsibilities	Practices must report clinical safety incidents in line with national guidance. Practices as independent contractors are responsible for sourcing any legal advice they may require supporting any of these activities.
Dependencies with other capabilities	Information Governance Support. Essential Clinical System Capabilities. Project and change management service. Clinical Systems Training and Optimisation.
Applicable Standards	• DCB0160: Clinical Risk Management: Its Application in the Deployment and Use of Health IT Systems. • DCB0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems. • EU Medical Devices Regulations (MDR). • EU In-Vitro Diagnostic medical device Regulations (IVDR). • Clinical Safety Management: Clinical Incident Reporting (NHS Digital) • Provider staff should be appropriately trained and qualified to recognised industry standards such as NHS Digital's Clinical Safety Officer Foundation Course or equivalent level recognised industry standard.
Applicable Guidance	**Clinical Safety Guidance – NHS Digital** **Introductory guide to the new MDR & IVDR** (MHRA)
Assurance	PC DMAT: • (IND11.0) The practices have access to a formal Clinical Safety System (DCB0160) and qualified clinical safety officer.

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 GP IT Futures Framework.
Out of Scope	Funding for the digital solution being procured and support for its deployment and implementation is not part of the procurement support service as this is an internal CCG (or general practice) responsibility.
Specialist Support Services	Availability: Standard Service Hours **General Digital Procurement Support** • Provide strategic procurement advice, recommending collaboration and standard specifications to optimise efficiency and support costs. • Advice and assistance in the development of outputs-based specifications to support GP 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. • Accessing where applicable, the National Commercial & 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. **GP IT Futures procurement support** Supporting mini-competition work for the procurement by CCGs from the GP IT Futures Services Framework. Meeting practice capabilities within nominated CCG funding allocations whilst ensuring excellent value for money **Non-GP IT Futures procurement support** Practices and CCGs purchasing non- GP IT Futures Framework clinical systems and digital technologies which include hosting patient identifiable information are responsible for ensuring that the hosted solution provider (as data processor) meets standards detailed below.
Dependencies with other capabilities	Digital Services Contract Support National Commercial & Procurement Hub.
Other Controls	Procurement legislation.

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

Digital Services Contract Support

Requirement	Facilitating CCG GP IT delivery with support for contract and supplier management and technical support. Solutions procured through GP IT Futures Framework or directly by the CCG for use by its practices. As end users of services practices are required to comply with any end user terms and conditions of use but wherever the contract is held by the CCG or NHS Digital a support service is required to manage local technical and contractual issues on behalf of the practice with the supplier.
Out of Scope	Support for contracts for practice business support systems Support for contracts held by parties other than CCG or NHS Digital. Support for contracts directly held by the practice. Payments and invoice processing for the contracted digital solutions is not part of the contract support service as this is an internal CCG (or general practice) responsibility.
Specialist Support Services	Availability: Standard Service Hours • Ongoing support for practice clinical systems including technical liaison with system supplier and clinical application support where not provided by system supplier. • In the event of any unresolved issues, escalate to suppliers on behalf of practices to facilitate a satisfactory resolution. • 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 GP IT Futures Framework 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 GP IT Futures Framework suppliers regarding future requirements and developments. • Management of ongoing system updates as necessary where these are not directly managed by the system supplier • Supporting practice data migration end to end process for GP IT Futures Foundation Solutions (GPSOC principal

	clinical systems prior to these being available) in line with applicable data migration standard.
Dependencies with other capabilities	Digital Services Procurement Support.
Assurance	GP IT Futures CRM reports – to be automatically incorporated (annually) into the Primary Care Data Maturity Assessment Toolkit. PC DMAT: • (IND157.0) CCG has contracted for GP IT enabling services ensuring value for money through effective use of national framework contract or other robust procurement in adherence with SFIs and procurement legislation.

Estates Strategy

Requirement	Provision of advice and guidance to support the development of GP estate relevant to the provision of GP IT services and systems.
Out of Scope	Funding and resourcing support for new estates developments should be provided through the relevant business case for that development.
Specialist Support Services	Availability: Standard Service Hours • Advice on IT infrastructure requirements and standards • Identify, as required, suppliers for 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 to meet core & 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's 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 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.
Dependencies with other capabilities	Essential Clinical System Capabilities.
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	PC DMAT: • (IND7.0) There is a comprehensive ongoing training and clinical system optimisation service to support GP Principal clinical systems and national clinical services available to all practices

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 & 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	PC DMAT: • (IND30.0) There is a comprehensive data quality advice and guidance service is available to all GPs, including training in data quality, clinical coding and information management skills. • (IND177.0) As part of the data quality advice and guidance service SNOMED CT requirements are included in all elements of the service • (IND185.0) The practice has a process in place to systematically review all locally developed Templates and Searches to ensure alignment with the transition to SNOMED CT

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 and end to end project management of GP IT Futures Foundation Solutions (GPSOC principal clinical systems prior to these being available), including: • Change of Foundation Solution (GPSOC principal clinical systems prior to these being available) 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	Provider staff should be appropriately trained and qualified to recognised industry standards such as APMG in; project management – eg Prince II Practitioner, programme management – eg Managing Successful Programmes Practitioner, change management – eg Change Management Practitioner Or equivalent level recognised industry standard. GP IT Futures Data Migration Standard

	GP IT Futures Training Standard
Assurance	PC DMAT: • (IND32.0) The commissioned GP IT services include formal P3M (Project, Programme and Portfolio Management) methodologies which are recognised and used in the deployment of GP Clinical systems, local implementation of national solutions and major primary care IT infrastructure changes.

Local Digital Strategy

Requirement	Strong local leadership to develop and deliver a local digital strategy and digital roadmap, including GP IT. The CCGs should: • Have access to horizon scanning and advice on best practice and digital innovation. • Appoint a Chief Clinical Information Officer (CCIO) or equivalent accountable officer (dedicated or shared) who will provide (clinical) leadership for the development of local digital strategy including the development of GP IT services. • Develop a 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	PC DMAT: • (IND12.0) There is a local GP IT strategy and programme with roadmap annually reviewed and aligned with local commissioning priorities • (IND153.0) The commissioner (CCG) owns the strategic digital direction and ensures that this is driven by local commissioning objectives. It recognises and exercises its responsibility for innovation and technology enabled change, with a clear vision for health and care articulated, with an associated digital strategy in place.

National Digital Services Implementation

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

Enhanced Requirements

These are enhanced GP digital requirements the provision of which is agreed locally to support local strategic initiatives and commissioning strategies to improve service delivery. They should support the CCG(s) local digital strategy and Local Digital Roadmap 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, ICS, MCP and PACS organisational models.

   Where the practice is represented within an ICS or STP, 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 with the ICS/STP.

   CCGs may use local GP IT funds, subject to CCG 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 & mandated requirements to practices.

3. **Additional GP contract digital capabilities** - Required to deliver those elements of a GP contract additional to providing essential primary medical services to a registered patient list, e.g. 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 & mandated GP IT enabling requirements necessary to support and enable those enhanced requirements commissioned locally.

Unlike Foundation Capabilities accredited solutions are not contractually mandated but accreditation may be required if it is defined within any standard attributed to the capability. In all cases CCGS should only procure solutions which meet the standards referenced in this Operating Model and where authoritative accreditation is available e.g. the GP IT Futures Framework or the National Dynamic Purchasing System Framework (for online consultation solutions) then CCGs are strongly advised to procure accredited solutions to meet these capabilities. If GP IT Futures notional CCG funds are used the solutions can only be sourced through the GP IT Futures Framework.

Compliance with CCG SFIs will require demonstration of value for money and product quality & safety.

Provision of enhanced requirements through commissioner funding is secondary to funding core & mandated requirements, but they should not be seen as less important as they underpin service improvement transformation in the locality.

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.

Capabilities available through GP IT Futures Framework

Capability	Description	Productive	Transformational
Communicate with Practice – Citizen	Supports secure and trusted electronic communications between Citizens and the Practice. Integrates with Patient Information Maintenance.		Yes
Telehealth	Enables Citizens and Patients that use health monitoring solutions to share monitoring data with health and care professionals to support remote delivery of care and increase self-care outside of clinical settings.		Yes
Clinical Decision Support	Supports clinical decision-making to improve Patient safety at the point of care.	Yes	
Reporting	Enables reporting and analysis of data from other Capabilities in the Practice Solution to support clinical care and Practice management.	Yes	Yes
Unstructured Data Extraction	Enable automated and manual interpretation and extraction of structured data from paper documents and unstructured electronic documents to support their classification and matching with Patient Records.	Yes	
Workflow	Supports manual and automated management of work in the Practice. Also supports effective planning, tracking, monitoring and reporting.	Yes	
Online-consultations (patient/user to professional)	Enables Patients/Service Users to access support from Health and Care Professionals, across a range of settings, without the need for a face to face encounter.	Yes	
Online-consultations (professional	Enables the communication and sharing of specialist knowledge and advice		Yes

to professional)	between Health and Care Professionals to support better care decisions and professional development.		
Medicines Optimisation	Supports clinicians and pharmacists in reviewing a Patient's medication and requesting changes to medication to ensure the Patient is taking the best combination of medicines.	Yes	
Social Prescribing	Supports the referral of Patients/Service Users to non-clinical services to help address their health and well-being needs.	Yes	Yes
Data Analytics for integrated and federated care	Supports the analysis of multiple and complex datasets and presentation of the output to enable decision-making, service design and performance management.		Yes
Telecare	Supports the monitoring of Patients/Service Users or their environment to ensure quick identification and response to any adverse event.		Yes
Caseload Management	Supports the allocation of appropriate Health and Care Professionals to Patients/Service Users in need of support, ensuring balanced workloads and the efficient use of staff and other resources.	Yes	
Cross-org Appointment booking	Enables appointments to be made available and booked across Organisational boundaries, creating flexibility for Health and Care Professionals and Patients/Service Users.	Yes	Yes
Cross-org Workforce Management	Supports the efficient planning and scheduling of the health and care workforce to ensure that services can be delivered effectively by the right staff.	Yes	Yes
Cross-org Workflow Tools	Supports and automates clinical and business processes across Organisational boundaries to	Yes	Yes

	make processes and communication more efficient.		
Unified Care Record	Provides a consolidated view to Health and Care Professionals of a Patient/Service User's complete and up-to-date records, sourced from various health and care settings.		Yes
Shared Care Plans	Enables the maintenance of a single, shared care plan across multiple Organisations to ensure more co-ordinated working and more efficient management of activities relating to the Patient/Service User's health and care.		Yes
Personal Health Budget	Enables a Patient/Service User to set up and manage a Personal Health Budget giving them more choice and control over the management of their identified healthcare and well-being needs.		Yes
Personal Health Record	Enables a Patient/Service User to manage and maintain their own Electronic Health Record and to share that information with relevant Health and Care Professionals.		Yes
Population Health Management	Enables Organisations to accumulate, analyse and report on Patient healthcare data to identify improvement in care and identify and track Patient outcomes.	Yes	
Domiciliary Care	Enables Service Providers to effectively plan and manage Domiciliary Care services to ensure care needs are met and that Care Workers can manage their schedule	Yes	
Care Homes	Enables a record of the Resident’s health and care needs to be maintained and shared with parties who are involved in providing care, to support decision making and the effective planning and delivery of care.	Yes	

Risk Stratification	Supports Health and Care Professionals by providing trusted models to predict future Patient events, informing interventions to achieve better Patient outcomes.		Yes
Productivity	Supports Patients/Service Users and Health and Care Professionals by delivering improved efficiency or experience related outcomes	Yes	

Capabilities sourced through non-accredited sources

Any of the enhanced capabilities available through the GP IT Futures Framework (see above) may also, subject to any restrictions on the use of designated funds, be procured through other appropriate routes. However, CCGs and Practices are strongly encouraged to use accredited solutions available through the GPIT Futures Framework wherever possible. Compliance with CCG SFIs will require demonstration of value for money and product quality & safety for which the GP IT Futures Framework can provide assurances.

Non-accredited solutions must still meet any standards attributed to the capability defined in this operating model.

Other enhanced capabilities may not be available through the GP IT Futures Framework.

Patient Facing Digital Services (local)

Requirement	Locally commissioned patient facing digital services, where these capabilities are not part of national digital services provided and are not part of the core & mandated patient facing capabilities. This includes: • Online Consultation (citizen-practice and professional-professional) where not sourced through the GP IT Futures Framework or the NHS App.
Out of Scope	National Digital Services - Patient Facing Services (centrally funded). Patient Facing Digital Services provided as part of a core & mandatory capability (through GP IT Futures Framework or through NHS App). Other patient facing digital services sourced through GP IT Futures Framework.
Systems and applications	Specialist applications (meeting required standards)
Applicable Standards	• NHS Apps Library – Digital Assessment. • 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. •
Applicable Guidance	Patient Facing digital services provided by the NHS should not be provided at a cost to the patient For on-line consultation (patient): • Online Consultation best practice procurement & specification guidance. • Patient Online Services in Primary Care – Good Practice Guidance on Identity Verification. • Medical device stand-alone software including apps: Guidance, MHRA.

GP Hubs, GP Federation and GP Collaborative enablement

Requirements	Digital enablers required to support GP collaborative and at scale operations including, but not restricted to: • Practices working collaboratively e.g. in federations (or other arrangement), • Practice co-location to share resources, • Hubs to share resources and improve patient access
Out of Scope	Systems, Support and Infrastructure provided to support Primary Care Networks (PCNs)
Infrastructure	Practices working collaboratively may require specific IT infrastructure including: • Shared infrastructure capabilities e.g. Active Directory, file management, intranet etc. • Practice location independent access to IT Infrastructure and digital services (including patient records).
Systems and applications	Practices working collaboratively may require specific clinical systems capabilities including: • Access to clinical records between practices, • Shared patient administration, appointment management and transactions between practices, • Reporting capabilities across practice federations e.g. central reporting, • Population management functions across federation practice populations, • Digital solutions that support 7 day working.
Tracking	Primary Care Data Maturity Assessment Toolkit (PC DMAT): • IND 57.1 – Where the practice works within a federation it is able to use its clinical system to share records. • IND 57.2 – Where the practice works within a federation it uses its clinical system to book appointments. • IND 57.4 – Where the practice works within a federation it shares reporting on activity & coded clinical data.

Advanced Telephony

Requirements	Digital enablement of transformed primary care & primary care at scale.
Out of Scope	Standard practice telephony funded through global sum.
Infrastructure	Telephony solutions where they are: • Community/inter-practice footprint; and • Integrated with other digital services; and • Enable transformed primary care, • Enabling advanced GP services e.g. online & video consultations. CCGs may choose to support the development of advanced telephony capabilities where there is an agreed case that it will support significant service improvement and transformation. This would therefore become a enhanced digital capability. CCGs may wish to consider ETTF or other capital sources to support the implementation of advanced telephony solutions. Practices and other users of at-scale advanced telephony systems will be in receipt of funding (global sum or national provider tariff), such funds along with business efficiency savings from using the new technology, should fund the operating costs of the system. A CCG may therefore <u>at its discretion</u> choose to fund (i) capital investment, including deployment costs, of such a system, (ii) IT infrastructure costs where the proposed system utilises the managed GP IT infrastructure. CCGs must ensure the use of managed GP IT infrastructure for telephony (or other enhanced capabilities) does not negatively impact on the performance of foundation solutions in the practices. Practices, and any other local organisation utilising the system, should continue to be responsible for operating costs including maintenance charges, line rentals, call charges.
Systems and applications	Supporting software e.g. call logging, call recording, directory services.
Practice Responsibilities	Telephony systems used within a single practice should remain the sole responsibility of the practice.
Tracking	PC DMAT: • (IND57.3) Where the practice works within a federation or other collaborative arrangement it is able to use its IT infrastructure to support shared working between practices in the following ways: Integrated telephony systems across practices

Practice Efficiency & Service Quality Enablers

Requirements	Digital solutions which enable the more efficient and effective delivery of the GP contract function.
Infrastructure	Hardware for: • Patient arrival and kiosk systems, patient touch screens, • Patient information display screens (for example large TV screens and "Jayex" Boards), projectors, multi-function devices, webcams, • Dictation Systems, • Diagnostic equipment with digital integration e.g. spirometry, cardiac monitoring, ECG monitors, specialist cameras, BP monitoring. NB this is not an exhaustive list
Systems and applications	Software for: • Patient arrival and kiosk systems, patient touch screens, • Display screens (for example large TV screens and Jayex Boards), projectors, multi-function devices, webcams, • Local diagnostic tools: blood pressure monitoring, spirometry, ECG, digital cameras, • 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 e.g. Hospital PAS, Hospital radiology viewers. NB this is not an exhaustive list
Applicable Standards	Procurement standards.

Tracking	PC DMAT:
	• (IND46.) The practice routinely electronically orders or receives the following diagnostics tests with their main acute provider:
	  ○ (IND46.1) Place orders for common laboratory diagnostic tests
	  ○ (IND46.2) Place orders for common imaging & diagnostic tests
	  ○ (IND46.3) Receive diagnostic reports for common imaging & diagnostic tests
	• (IND48.) Local acute trust discharge letters/summaries are received by the practice electronically in the following ways:
	  ○ (IND48.2) The MAJORITY of local A&E discharge summaries are received electronically
	  ○ (IND48.3) The MAJORITY of local acute INPATIENT discharge summaries/letters are received electronically

	○ (IND48.4) The MAJORITY of local acute OUTPATIENT discharge summaries/letters are received electronically

Digital services supporting additional GP Contract services

Requirements	Digital requirements for those elements of a GP contract additional to providing essential primary medical services to a registered patient list – 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 GPSi Schemes.
Out of Scope	Provision or funding for these services is included in the agreed contract tariff or otherwise funded.
Infrastructure	IT infrastructure supporting specialist service clinical software.
Systems and applications	Specialist service clinical software for local Directed Enhanced Services and GP specialist interest schemes.

GP IT Enabling Requirements

This includes;

- Specific requirements for services not included as core & mandated GP IT enabling requirements – examples given below but these are not exhaustive.
- Any extension of the core & mandated GP IT enabling requirements necessary to support and enable those enhanced requirements commissioned locally either through GP IT Futures Framework or through local procurement.

Requirements include;

- CQRS Support,
- GP Data Quality Accreditation Service,
- Enhanced Infrastructure and
- Remote access to the clinical systems for administrative purposes.

CQRS Support

Requirement	CQRS training, advice and guidance for practices. Note: CQRS provides support for calculating approximately 12-14% of General Practice incentive-based payments (e.g. 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.
Specialist Support Services	Availability: Standard Service Hours 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
Infrastructure	CQRS uses an Internet based payment calculation system: Management and support for provision payment calculation system services, supporting QOF and Enhanced Service payments
Systems and applications	The CQRS system has a separate LMS for users to access the learning materials.
Dependencies with other capabilities	GPES CQRS
Applicable Guidance	**Calculating Quality Reporting Service** Further information: **enquiries@nhsdigital.nhs.uk**
Tracking	PC DMAT: • (IND168.0) A proactive support service is in place locally to support Quality and Outcomes (QOF) data collection and reporting, which includes review, report management and remedial action planning, particularly around exception reporting, to ensure appropriate data quality within GP sites to enable effective QOF reporting.

GP Data Quality Accreditation Service

Requirement	A structured data quality accreditation programme is available for practices to ensure continuous review and improvement.
Specialist Support Services	Availability: Standard Service Hours 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	• SNOMED Clinical Terms (CT) in General Practice / Standards Change Notice SCCI0034 Amd 35/2016. • Data Security and Protection Toolkit (DSPT) (data quality assertions)
Applicable Guidance	ICO Records Management Guidance.
Tracking	PC DMAT: • (IND167.0) A formal and structured data quality accreditation programme is commissioned by the CCG and available for GP sites to ensure continuous review and improvement of data quality within General Practice. This will incorporate a baseline assessment, reporting and remedial action planning, together with ongoing data quality advice, guidance and training in data quality and information management techniques and practice.

Enhanced Infrastructure

Requirement	Infrastructure requirements which enable enhanced digital capabilities, or which support a more efficient, effective or secure means of GP IT provision in the locality.
Infrastructure	Networking Services: • Management and support for provision of additional HSCN services. • Where 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: • Where the COIN is used to support GP IT there is a clear requirement for this in addition to HSCN connectivity. • Where the COIN is shared between providers, the costs need to be appropriately proportioned. • 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 Interface (VDI), • Citrix Access Gateway (CAG), • Smartcard/Remote Secure Access Token authentication, • Single sign on, • Bring Your Own Device (BYOD). Bring Your Own Device (BYOD) services (for practice staff) in practices can only connect to the managed GP IT infrastructure using the Public WiFi-GP service and must not be used to process patient identifiable data.
Dependencies with other capabilities	Essential Infrastructure.
Applicable Standards	See Essential Infrastructure.
Applicable Guidance	Where centralised infrastructure (for example but not limited to network infrastructure and virtual desktop infrastructure) is deployed particular attention should be given to security, end user performance and system resilience such that the security, performance and resilience of GP IT Futures Framework solutions and National Digital Services is not compromised.
Tracking	PC DMAT:

	• (IND31.0) Where there is a local community network wholly or part funded through GPIT and used in addition to, or in place of, HSCN/N3 by general practices AND other locations and care settings the costs are shared between these organisations.

Remote access to the clinical systems for administrative purposes

Requirement	Provision, maintenance and technical support of software and managed GP IT infrastructure including mobile and desktop devices necessary to provide remote access to the clinical system for administrative purposes.
Infrastructure	Where mobile and desktop devices are provided or managed for practices to remotely access clinical systems for administrative purposes: The use of mobile computing systems is controlled, monitored and audited to ensure their correct operation and to prevent unauthorised access, supporting DSPT requirements for general practice. Managed Devices (i.e. NHS owned or part of the managed GP IT Infrastructure) must be locked down and well managed, with advanced tools, processes and policies in place to support diagnosis, repair and updates. Encryption to NHS standards is applied on all mobile, portable and remote devices 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. Users must not be able to install unlicensed or unauthorised software or change critical settings. Remote access solutions must not be used which bypass or otherwise reduce the effectiveness of the security measures within the GP IT Futures Framework Services, the National Digital Services and the Managed GP IT Infrastructure (including smartcard access) Refresh Programme: • CCG budgeted plan for mobile GP IT equipment refresh. Availability of these will be defined in the agreed IT refresh plan The CCG will commission a continual refresh programme that will identify and replace hardware where it has reached its service life change date, including assessment, procurement and rollout
Systems and applications	Software, browsers and operating systems not supported or maintained by the supplier must not be used on NHS managed infrastructure. Connections between mobile/portable/remote devices to HSCN/N3 and the practice clinical system using public network services (internet) must be encrypted to approved NHS standards.

Applicable Standards	• NDG Standard 8
Applicable Guidance	• Guidance on the Implementation of Encryption within NHS Organisations (NHS Digital) • Information Security Management: NHS Code of Practice • Recommendation: The local SLA is based upon an agreed mobile estate volume.
Other Controls	• General Data Protection Regulation (GDPR) • Data Protection Act 2018
Tracking	PC DMAT: • (IND33.2) The practice principal clinical system is accessible outside the practice for the following purposes: Access remotely eg home for administrative & maintenance purposes

General Practice Business Requirements

Digital systems, technologies and services necessary to run the internal practice business and organisational governance i.e.;

- General practice business support systems,
- General practice legal and regulatory obligations,
- General practice websites,
- Dispensing Practices,
- General Practice Operating Costs,
- General Practice Buildings & 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 (i.e. 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. Practices may bid, through the CCG, for financial support through non-recurrent or capital funds such as ETTF to support practice buildings and estate development projects.

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 demonstrable benefit of incorporating elements of GP business support services eg telephony/Voice Over IP 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 e.g. 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).
Out of Scope	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. Practices procuring their practice business support systems are responsible for resourcing and managing their own procurement and contract management processes but 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. CCGs have an obligation to ensure services already NHS funded are not funded as enhanced GP IT services.
Transactional Support Services	Production of practice staff ID cards for new employees and changes to existing employees (name, role etc.).
Specialist Support Services	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
Infrastructure	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. Where there is demonstrable benefit of incorporating elements of GP business support services e.g. telephony/VOIP 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. Equipment which only support 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 (i.e. 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 and applications	Email systems other than NHS Mail Systems that only support the practice as a business for example. Payroll, HR systems

General practice legal and regulatory obligations

Requirement	Legal and regulatory obligations e.g. assigning a DPO, Caldicott Guardian, serious incident reporting etc. Practice compliance with • Data Protection legislation. • Health & Safety legislation. • Freedom of Information legislation • NHS DSP Toolkit
Out of Scope	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.

Dispensing general practices

Requirement	Digital capabilities required to support the dispensing operations in practices which hold a dispensing contract.
Out of Scope	Digital capabilities required to support the dispensing operations in practices which hold a dispensing contract are out of scope except for services such as personally administered vaccinations and immunisations which are part of primary care essential services provision.
Infrastructure	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.
Systems and applications	Specialist software and communication tools to support the dispensing function and FMD compliance.
Applicable Standards, Guidance and Controls	FMD EPS Dispensing Systems Compliance Specification.

General practice websites

Requirement	General Practice websites including; • Domain Registration, • Hosting of website, • Maintenance of website and • Design.
Out of Scope	Online patient facing digital capabilities as defined in core & mandated requirements. NB-The practice website must however provide a link for the public/patients to these online services.
Transactional Support Services	Responsive service to resolve performance and access issues and to implement necessary changes as required to fulfil the practice GP contract obligations.
Specialist Support Services	Website design and maintenance.
Infrastructure	Website hosting requirements.
Systems and applications	Integration with GP online services.
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 new 5 year GP contract framework requires by April 2020 all practices will need 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 new GMS regulations also place restrictions on the advertising and hosting of private GP services including through practice websites. 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	Digital System Consumables (printer paper, printer ink/cartridges). Power utility charges. Telephony operating costs and call charges. Backup media for any local servers.
Applicable Standards, Guidance and Controls	Where specified in the local 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 & 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 e.g. physical security, fire suppression and air conditioning/cooling equipment. Health & Safety requirements associated with the buildings and estate. PAT testing of IT equipment held on site if required (regardless of ownership). Building Security. Power supply infrastructure for IT Equipment (including cabling and outlets).

APPENDIX B –Responsibilities and accountabilities

General Responsibilities	General	Financial	Cyber & 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 & 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 & 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 GP IT Futures	Contracting Authority for GP IT Futures	
NHS Digital	GP IT Futures Framework. Assurance, accreditation management. Commissions National Digital Services. Set & manage national standards.	Compliance with Standing Financial Instructions	Operate Data Security Centre. DSPT provision & management. Set Cyber & Data security standards.

Nationally Commissioned Providers	Provide digital services to agreed contract, service specifications and standards.		DSPT completion CE + or ISO27001. Data processor responsibilities.
CCGs	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. Compliance with procurement legislation. Confirmed support from CCG Chief Finance Officer (CFO) for capital bids.	Commission GP IT enabling services to include cyber security and information governance – providing advice & 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	DSPT completion. CE + or ISO27001. Data processor responsibilities. Registration for CareCERT portal and alerts.

		procurement challenges arising from commissioned work with CCG.	
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 email and mobile phone number for urgent text & email alerts with MHRA CAS

Core & Mandated Requirements: Responsibilities	Essential clinical system capabilities available through GP IT Futures Framework.	National digital services	GP IT Enabling Requirements
NHS England	Operating Model determines core & mandated capabilities. Step in Services in exceptional circumstances as described in the Data Processing Deed		Operating Model determines core & mandated requirements. Directs CCGs to commission & provide. Assurance.
NHS England Regional Teams	Assuring CCGs meet responsibilities listed below		
DHSC	Contracting Authority for GP IT Futures Step in Services in exceptional circumstances as described in the Data Processing Deed		
NHS Digital	Commissions. Sets standards. Manages GP IT Futures Framework & catalogue. Product assurance to framework standards. Service management & Performance Step in Services in exceptional circumstances as described in the	Commissions. Sets standards. Publish system utilisation data.	

	Data Processing Deed		
Nationally Commissioned Providers	Onboarding to GP IT Futures Framework. Service provision to required standards.	Provide contracted services.	
CCGs	Order through call off agreements using GP IT Futures Framework. 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 GP IT Futures Framework (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 GP IT Futures Framework	Capabilities sourced through non-GP IT Futures Framework routes	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 Step in Services in exceptional circumstances as described in the Data Processing Deed		
NHS Digital	Commissions. Sets standards. Manages GP IT Futures Framework & catalogue. Product assurance to framework standards. Service management & performance Step in Services in exceptional circumstances as described in the		

	Data Processing Deed		
Nationally Commissioned Providers	Onboarding to GP IT Futures Framework Service provision to required standards.		
CCGs	Order through call off agreements using GP IT Futures Framework. Management of GP IT Futures nominal funding allocations. Contract management and accountability. CCGs **may not** delegate GP IT Futures Framework call off agreements. Choice of solutions from GP IT Futures Framework 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 GP IT Futures Framework.	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.
NHS England Regional DCO Teams	
NHS Digital	
Nationally Commissioned Providers	
CCGs	CCG may at its discretion provide infrastructure and support through the GP IT Enabling Requirements.
Locally Commissioned Providers	
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 – Primary Care Digital Maturity Assurance Tool Indicators

INDICATOR	DIGITAL MATURITY	GRANULARITY	SOURCE
(IND2.0) The CCG commissioned service provider for GP IT services will have an annually reviewed & tested Business Continuity Plan and validated IT Disaster Recovery Plan for services critical to GP service continuity.	Core & Mandated	CCG	CCG Questionnaire
(IND3.0) The practice is enriching the Summary Care Record of patients who have given their consent, including those living with severe frailty.	Productive	GP	eDEC
(IND7.0) There is a comprehensive ongoing training and clinical system optimisation service to support GP Principal clinical systems and national clinical services available to all practices	Core & Mandated	CCG	CCG Questionnaire
(IND8.1) All practices complete DSPT	Core & Mandated	GP	DSPT Reports (NHS Digital)
(IND9.0) All practices have access to SMS (or equivalent messaging system) integrated with the practice principal clinical system to support direct communications with patients.	Core & Mandated	CCG	CCG Questionnaire
(IND10.1) Contracts with all third parties that handle personal information are compliant with GDPR	Core & Mandated	GP	DSPT Reports (NHS Digital)
(IND11.0) The practices have access to a formal Clinical Safety System (DCB0160) and qualified clinical safety officer.	Core & Mandated	CCG	CCG Questionnaire
(IND12.0) There is a local GP IT strategy and programme with roadmap annually reviewed and aligned with local commissioning priorities	Core & Mandated	CCG	CCG Questionnaire

(IND14.0) There is an agreed local strategy and approach for core GP IT infrastructure & software investment to meet the needs of (i) maintaining existing IT estate required for core GP IT needs (ii) practice organic/incremental growth (iii) practice developments eg mergers (iv) significant primary care developments eg new builds	Core & Mandated	CCG	CCG Questionnaire
(IND15.0) There is a clear agreed local (CCG) budgeted plan for the full funding of all core GP IT requirements for the next 2 years.	Core & Mandated	CCG	CCG Questionnaire
(IND20.0) GP IT services are commissioned and contracted with robust and clear service specifications	Core & Mandated	CCG	CCG Questionnaire
(IND21.1) All practices sign the CCG – practice agreement v2	Core & Mandated	GP	CCG Questionnaire Plus
(IND24.0) The CCG has completed a formal review of IT Services with each Practice in the last 12 months.	Core & Mandated	CCG	CCG Questionnaire
(IND26.0) CCG Commissioned GP IT support provides consistent support for core GP contract hours (0800 – 1830 Mon – Fri excluding Bank holidays)	Core & Mandated	CCG	CCG Questionnaire
(IND28.0) The GP IT support service desk has current formal accreditation through a recognised (NHS or other industry) scheme	Core & Mandated	CCG	CCG Questionnaire
(IND29.0) GP IT services available include cyber & IT Security advice and oversight, including configuration support, audit, investigation and routine monitoring	Core & Mandated	CCG	CCG Questionnaire
(IND30.0) There is a comprehensive data quality advice and guidance service is available to all GPs, including training in data quality, clinical coding and information management skills.	Core & Mandated	CCG	CCG Questionnaire

(IND31.0) Where there is a local community network wholly or part funded through GPIT and used in addition to, or in place of, HSCN/N3 by general practices AND other locations and care settings the costs are shared between these organisations.	Productive	CCG	CCG Questionnaire
(IND32.0) The commissioned GP IT services include formal P3M (Project, Programme and Portfolio Management) methodologies which are recognised and used in the deployment of GP Clinical systems, local implementation of national solutions and major primary care IT infrastructure changes.	Core & Mandated	CCG	CCG Questionnaire
(IND33.2) The practice principal clinical system is accessible outside the practice for the following purposes: Access remotely eg home for administrative & maintenance purposes	Productive	GP	eDEC
(IND33.3) The practice principal clinical system is accessible outside the practice for the following purposes: Access from patient homes using mobile technologies (subject to local provider network coverage)	Productive	GP	eDEC
(IND34.0) The GP IT infrastructure estate supporting core GP IT (includes desktop, mobile, server and network equipment) has a fully documented plan for refresh and replacement. This must include a local WES (Warranted Environment Specification) for such equipment which as a minimum will meet the WES for the principal clinical systems used and any NHS mandated national systems and infrastructure.	Core & Mandated	CCG	CCG Questionnaire
(IND35.1) Records of processing activities are documented for all uses and flows of personal information	Core & Mandated	GP	DSPT Reports (NHS Digital)

(IND36.0) All NHS owned GP IT equipment is recorded in an accurate asset register.	Core & Mandated	CCG	CCG Questionnaire
(IND37.1) All software (including operating systems) used on managed GP IT infrastructure by the practice must be approved and recorded on an software asset & licence register which must confirm the software is appropriately and legally licenced for such use.	Core & Mandated	CCG	CCG Questionnaire
(IND38.0) All NHS owned GP IT equipment is subjected to an approved IT reuse & disposal policy and procedures – using authorised contractors. This is fully integrated with the asset management system	Core & Mandated	CCG	CCG Questionnaire
(IND39.0) All practices have secure data storage services available for any electronic patient identifiable and clinical data other than that stored in their GPSOC/GP IT Futures clinical systems and NHS Mail to a standard not less that tier 3 data centre.	Core & Mandated	CCG	CCG Questionnaire
(IND39.1) All practices have secure cloud-based data storage services available for any electronic patient identifiable and clinical data other than that stored in their GPSOC / GP IT Futures clinical systems and NHS Mail to a standard compliant with “NHS and social care data: off-shoring and the use of public cloud services guidance”	Core & Mandated	CCG	CCG Questionnaire
(IND45.1) Functionality status of the Practice system for enabling the use of online Patient Record Access Services for ‘online patients’ to view their Detailed Coded Care Record	Core & Mandated	GP	POMI – NHS Digital
(IND45.2) At least 10% of registered patients registered to use online Patient Record Access Service to access elements of the Detailed Coded Care Record	Productive	GP	POMI – NHS Digital

(IND45.3) At least 20% of registered patients registered to use online Patient Record Access Service to access elements of the Detailed Coded Care Record	Productive	GP	POMI – NHS Digital
(IND45.4) At least 30% of registered patients registered to use online Patient Record Access Service to access elements of the Detailed Coded Care Record	Productive	GP	POMI – NHS Digital
(IND46.1) The practice routinely electronically orders or receives the following diagnostics tests with their main acute provider: Place orders for common laboratory diagnostic tests	Productive	GP	eDEC
(IND46.2) The practice routinely electronically orders or receives the following diagnostics tests with their main acute provider: Place orders for common imaging & diagnostic tests	Productive	GP	eDEC
(IND46.3) The practice routinely electronically orders or receives the following diagnostics tests with their main acute provider: Receive diagnostic reports for common imaging & diagnostic tests	Productive	GP	eDEC
(IND48.2) Local acute trust discharge letters/summaries are received by the practice electronically in the following ways: The MAJORITY of local A&E discharge summaries are received electronically	Core & Mandated	GP	eDEC
(IND48.3) Local acute trust discharge letters/summaries are received by the practice electronically in the following ways: The MAJORITY of local acute INPATIENT discharge summaries/letters are received electronically	Core & Mandated	GP	eDEC

(IND48.4) Local acute trust discharge letters/summaries are received by the practice electronically in the following ways: The MAJORITY of local acute OUTPATIENT discharge summaries/letters are received electronically	Core & Mandated	GP	eDEC
(IND50.1) There are clear data security and protection policies in place and these are understood by staff and available to the public	Core & Mandated	GP	DSPT Reports (NHS Digital)
(IND52.2) Functionality status of the online system at the Practice for enabling the use of online Patient Transactional Services for booking and/or cancelling appointments through the Principal system	Core & Mandated	GP	POMI – NHS Digital
(IND52.4) At least 20% of registered patients registered to use online Patient Transactional Service to book and/or cancel appointments	Productive	GP	POMI – NHS Digital
(IND52.5) At least 30% of registered patients registered to use online Patient Transactional Service to book and/or cancel appointments	Productive	GP	POMI – NHS Digital
(IND53.1) There is senior ownership (designated individual) of data security and protection within the practice organisation	Core & Mandated	GP	DSPT Reports (NHS Digital)
(IND54.1) Staff receive suitable data security and protection training	Core & Mandated	GP	DSPT Reports (NHS Digital)
(IND57.1) Where the practice works within a federation or other collaborative arrangement it is able to use its principal clinical system and its IT infrastructure to support shared working between practices in the following ways: Clinical system (records)	Productive	GP	eDEC

(IND57.2) Where the practice works within a federation or other collaborative arrangement it is able to use its principal clinical system and its IT infrastructure to support shared working between practices in the following ways: Appointment booking and management	Productive	GP	eDEC
(IND57.3) Where the practice works within a federation or other collaborative arrangement it is able to use its principal clinical system and its IT infrastructure to support shared working between practices in the following ways: Integrated telephony systems across practices	Productive	GP	eDEC
(IND57.4) Where the practice works within a federation or other collaborative arrangement it is able to use its principal clinical system and its IT infrastructure to support shared working between practices in the following ways: Reporting on activity & coded clinical data	Productive	GP	eDEC
(IND57.5) Where the practice works within a federation or other collaborative arrangement it is able to use its principal clinical system and its IT infrastructure to support shared working between practices in the following ways: Morbidity Registers across aggregated (federation) populations	Productive	GP	eDEC
(IND58.0) There is a locally agreed WES (Warranted Environment Specification) for GP IT equipment which enables practices to effectively operate concurrently applications necessary to delivery both core and enhanced GP IT.	Productive	CCG	CCG Questionnaire
(IND59.1) There are physical controls that prevent unauthorised access to sites	Core & Mandated	GP	DSPT Reports (NHS Digital)

(IND60.1) There is a continuity plan in place for data security incidents, and staff understand how to put this into action	Core & Mandated	GP	DSPT Reports (NHS Digital)
(IND60.2) The practice has a documented business continuity plan approved by the CCG in the event of power failures, system failures, natural disasters and other disruptions	Core & Mandated	GP	CCG Questionnaire Plus
(IND62.1) A confidential system for reporting security breaches and near misses is in place and actively used	Core & Mandated	GP	DSPT Reports (NHS Digital)
(IND66.0) The practice has a procedure for electronic transmission of patient data in line with national policy including mechanisms to ensure that computerised medical records/data are transferred to a new practice when a patient leaves.	Core & Mandated	GP	eDEC
(IND67.1) Practice can provide a list of all systems/information assets holding or sharing personal information	Core & Mandated	GP	DSPT Reports (NHS Digital)
(IND72.0) All local GPs, PCNs and providers of health & social care sharing patient digital information agree to a consistent information sharing model (including common consent protocols)	Transformation	CCG	CCG Questionnaire
(IND73.0) All local providers of health & social care sharing patient digital information have systems which maintain a full automated audit of read and write access to individual patient records	Transformation	CCG	CCG Questionnaire
(IND79.0) A local Electronic Palliative Care Co-ordination System (EPaCCS) supporting the recording and sharing of people's care preferences and key details about their care at the end of life which is integrated with principal primary care clinical systems and meets the requirements of ISB 1580 (End of Life Care Co-ordination: Core Content) is available.	Transformation	CCG	CCG Questionnaire

(IND84.0) All health & care organisations (including GPS) can access their principal record systems from all local commissioned provider locations.	Transformation	CCG	CCG Questionnaire
(IND85.0) Access to WiFi services is available to general practice clinical staff across local commissioned provider locations.	Transformation	CCG	CCG Questionnaire
(IND86.0) The CCG has appointed a Chief Clinical Information Officer (CCIO) or equivalent accountable officer (dedicated or shared) who will provide (clinical) leadership for the development of local IT strategy including the development of primary care IT services.	Core & Mandated	CCG	CCG Questionnaire
(IND88.4) The practice promotes and offers the facility for patients and residential homes and nursing homes to receive consultations electronically, either by email, video consultation or other electronic means. Email consultation functionality enabled for patients	Productive	GP	eDEC
(IND88.5) The practice promotes and offers the facility for patients and residential homes and nursing homes to receive consultations electronically, either by email, video consultation or other electronic means. Video consultation functionality enabled for patients	Productive	GP	eDEC
(IND88.6) The practice promotes and offers the facility for patients and residential homes and nursing homes to receive consultations electronically, either by email, video consultation or other electronic means. Telephone consultation functionality enabled for patients	Productive	GP	eDEC
(IND88.7) The practice promotes and offers the facility for patients and residential homes and nursing homes to receive consultations electronically, either by email, video consultation or other electronic means.	Productive	GP	eDEC

Online consultation functionality enabled for patients			
(IND88.8) The practice promotes and offers the facility for patients and residential homes and nursing homes to receive consultations electronically, either by email, video consultation or other electronic means. Email consultation functionality enabled for Nursing Homes	Productive	GP	eDEC
(IND88.9) The practice promotes and offers the facility for patients and residential homes and nursing homes to receive consultations electronically, either by email, video consultation or other electronic means. Video consultation functionality enabled for Nursing Homes	Productive	GP	eDEC
(IND88.10) The practice promotes and offers the facility for patients and residential homes and nursing homes to receive consultations electronically, either by email, video consultation or other electronic means. Telephone consultation functionality enabled for Nursing Homes	Productive	GP	eDEC
(IND88.11) The practice promotes and offers the facility for patients and residential homes and nursing homes to receive consultations electronically, either by email, video consultation or other electronic means. Online consultation functionality enabled for Nursing Homes	Productive	GP	eDEC
(IND88.12) The practice promotes and offers the facility for patients and residential homes and nursing homes to receive consultations electronically, either by email, video consultation or other electronic means. Email consultation functionality enabled for Residential Homes	Productive	GP	eDEC

(IND88.13) The practice promotes and offers the facility for patients and residential homes and nursing homes to receive consultations electronically, either by email, video consultation or other electronic means. Video consultation functionality enabled for Residential Homes	Productive	GP	eDEC
(IND88.14) The practice promotes and offers the facility for patients and residential homes and nursing homes to receive consultations electronically, either by email, video consultation or other electronic means. Telephone consultation functionality enabled for Residential Homes	Productive	GP	eDEC
(IND88.15) The practice promotes and offers the facility for patients and residential homes and nursing homes to receive consultations electronically, either by email, video consultation or other electronic means. Online consultation functionality enabled for Residential Homes	Productive	GP	eDEC
(IND90.0) CCG Commissioned GP IT support Service supports practices to provide extended hours services under the "improved access to general practice" arrangements.	Productive	CCG	CCG Questionnaire
(IND91.0) CCG Commissioned GP IT support Service supports general practice to provide 7-day week services to patients where these are offered.	Productive	CCG	CCG Questionnaire
(IND92.1) Functionality status of the online system at the Practice for enabling the use of online Patient Transactional Services for ordering repeat prescriptions through the Principal system.	Core & Mandated	GP	POMI – NHS Digital
(IND92.3) At least 20% of registered patients registered to use an online repeat prescription ordering	Productive	GP	POMI – NHS Digital

(IND92.4) At least 30% of registered patients registered to use an online repeat prescription ordering	Productive	GP	POMI – NHS Digital
(IND93.1) Where there is legitimate access and consent the practice and other local health & social care providers are able to share electronic patient data by view access to records in the following ways: Other local health providers can access practice records	Transformation	GP	eDEC
(IND93.2) Where there is legitimate access and consent the practice and other local health & social care providers are able to share electronic patient data by view access to records in the following ways: Local social care providers can access practice records	Transformation	GP	eDEC
(IND93.3) Where there is legitimate access and consent the practice and other local health & social care providers are able to share electronic patient data by view access to records in the following ways: Practice can access records from other local health providers	Transformation	GP	eDEC
(IND93.4) Where there is legitimate access and consent the practice and other local health & social care providers are able to share electronic patient data by view access to records in the following ways: Practice can access records from local social care providers	Transformation	GP	eDEC

(IND100.1) The practice & its registered patients have access to a shared online system which allows patients to engage with their GP by: Patients can record their personal health data which is accessible online by the GP	Productive	GP	eDEC
(IND100.2) The practice & its registered patients have access to a shared online system which allows patients to engage with their GP by: Patients and GPs can on-line collaboratively set goals and care outcomes and track progress against these	Productive	GP	eDEC
(IND101.1) Individuals been informed about their rights and how to exercise them	Core & Mandated	GP	DSPT Reports (NHS Digital)
(IND150.0) Clear standing financial protocols are in place between commissioners and delivery organisations to ensure commissioners comply with their SFIs. Clear reporting, monitoring and review arrangements established to ensure CCG oversight of GPIT funding and expenditure, with clear escalation points agreed.	Core & Mandated	CCG	CCG Questionnaire
(IND152.0) Formal governance and accountability arrangements clearly articulated and embedded, which effectively engage strategic partners, with terms of reference and reporting responsibilities clearly defined, including the following forums/structures: 1. Health and Care (cross community stakeholders) 2. CCG/Primary Care Strategic Level 3. GPIT / Operational Delivery including clinical/LMC representation	Core & Mandated	CCG	CCG Questionnaire

(IND153.0) The commissioner (CCG) owns the strategic digital direction and ensures that this is driven by local commissioning objectives. It recognises and exercises its responsibility for innovation and technology enabled change, with a clear vision for health and care articulated, with an associated digital strategy in place.	Core & Mandated	CCG	CCG Questionnaire
(IND154.0) Commissioning of clinical services, routinely includes clinical (CCIO) consideration of digital technologies/systems, together with associated benefits.	Core & Mandated	CCG	CCG Questionnaire
(IND155.0) Service specifications for commissioning of clinical services, encompass core digital requirements, including, but not limited to data management and reporting, data security, data sharing, systems access, digital technology requirements.	Core & Mandated	CCG	CCG Questionnaire
(IND156.0) Formal governance arrangements are established which ensure the effective mapping and provision of digital enablers that will support delivery of locally identified health and care priorities. Business cases (where necessary) are shared with and agreed with relevant partners in the local area. Business cases where required for Informatics-enabled programmes with cross-community impact are approved by a relevant cross-community Board.	Core & Mandated	CCG	CCG Questionnaire
(IND157.0) CCG has contracted for GP IT enabling services ensuring value for money through effective use of national framework contract or other robust procurement in adherence with SFIs and procurement legislation.	Core & Mandated	CCG	CCG Questionnaire
(IND158.0) The CCG ensures that appropriate IG and information standards/requirements are clearly specified within any local GP IT service specification and associated service level agreement (SLA) and contractual	Core & Mandated	CCG	CCG Questionnaire

arrangements with IM&T delivery partners including DSPT completion to required standard.			
(IND159.0) DSPT compliance is assured through the standard contractual routes with wider health economy providers.	Transformation	CCG	CCG Questionnaire
(IND160.0) A GP IG support service is provided as specified in the GP IT Operating Model	Core & Mandated	CCG	CCG Questionnaire
(IND161.0) The CCG as local commissioner, through formal local governance arrangements, is responsible for ensuring benefit realisation from local investment in digital technology.	Transformation	CCG	CCG Questionnaire
(IND162.0) Benefits are explicitly defined, tracked and captured within individual projects.	Core & Mandated	CCG	CCG Questionnaire
(IND164.0) CCGs have appropriate mechanisms in place to effectively manage risks and issues in accordance with system wide procedures to help ensure the safe and successful delivery of outcomes associated with digital investment.	Core & Mandated	CCG	CCG Questionnaire
(IND167.0) A formal and structured data quality accreditation programme is commissioned by the CCG and available for GP sites to ensure continuous review and improvement of data quality within General Practice. This will incorporate a baseline assessment, reporting and remedial action planning, together with ongoing data quality advice, guidance and training in data quality and information management techniques and practice.	Productive	CCG	CCG Questionnaire
(IND168.0) A proactive support service is in place locally to support Quality and Outcomes (QOF) data collection and reporting, which includes review,	Productive	CCG	CCG Questionnaire

report management and remedial action planning, particularly around exception reporting, to ensure appropriate data quality within GP sites to enable effective QOF reporting.			
(IND171.0) Within primary care locations WiFi access is available to primary care staff, guests & visitors and public to approved standards.	Core & Mandated	CCG	CCG Questionnaire
(IND172.0) There is clear assurance process to ensure that GP IT delivery partners action in a timely manner all high severity CareCERT recommendations that apply to the local GP IT infrastructure.	Core & Mandated	CCG	CCG Questionnaire
(IND173.0) In the past 12 months the following items have been reviewed with the GPIT delivery partner(s): - operating system, software and anti-virus updates, including road maps - risk assessments of data and cybersecurity threats and any mitigation measures - management of non-GPSOC applications and CCG/GP procured devices used to process patient data	Core & Mandated	CCG	CCG Questionnaire
(IND174.0) Where STP/ACS/ACO are established, there should be effective governance and management arrangements for core & mandated GP IT services and how these contribute to integrated care, population health management capability and improved patient choice.	Transformation	CCG	CCG Questionnaire
(IND176.0) The CCG, GPIT Delivery Partner and General Practices have collaboratively identified all unsupported systems using (connected to) the managed GP IT infrastructure and have	Core & Mandated	CCG	CCG Questionnaire

agreed action plan to remove, replace or mitigate and actively manage the risks associated with these systems.			
(IND177.0) As part of the data quality advice and guidance service SNOMED CT requirements are included in all elements of the service.	Core & Mandated	CCG	CCG Questionnaire
(IND180.0) The CCG ensures that the commissioned GP IT Delivery Partner has allocated equivalent senior level responsibility for data and cyber security within their organisation.	Core & Mandated	CCG	CCG Questionnaire
(IND181.0) As part of the CCG commissioned IT security and IG service, specialist support for Cyber Security incident reporting and management is accessible to general practices.	Core & Mandated	CCG	CCG Questionnaire
(IND182.0) The CCG confirms that their GP IT delivery partner has cooperated and supported on-site assessments undertaken by NHS Digital when requested and is acting on the outcomes and recommendations of the assessment, including the sharing of the outcomes with the commissioner. A NO answer means that the on-site assessment has not yet been undertaken with the GP IT delivery partner.	Core & Mandated	CCG	CCG Questionnaire
(IND183.0) The CCG ensures that it commissions GP IT services from providers with the required certification as described in the Operating Model. If the CCG is also the GP IT service provider, that it also meets the appropriate certification.	Core & Mandated	CCG	CCG Questionnaire
(IND184.1) The CCG has implemented a capability for the central control of desktop security, patch control, access and software installation across at least 90% of its managed GP IT devices.	Core & Mandated	CCG	CCG Questionnaire

(IND185.0) The practice has a process in place to systematically review all locally developed Templates and Searches to ensure alignment with the transition to SNOMED CT	Core & Mandated	GP	eDEC
(IND186.0) Where the practice has directly purchased IT services, infrastructure or systems (connected to the managed GP IT infrastructure), the practice as contract holder, has reviewed these arrangements for compliance with the ten NDG data security standards and applicable legal requirements and appropriate certification ie ISO/IEC 27001: 2013, Cyber Essentials (CE) and CE+, where appropriate.	Core & Mandated	GP	eDEC
(IND188.0) Practice has either appointed a Data Protection Officer or has plans to do so	Core & Mandated	GP	eDEC
(IND189.0) The practice has completely digitised all of its paper records (Lloyd George) and paper records are no longer kept on site or in storage.	Transformation	GP	eDEC
(IND189.1) The practice uses off-site storage for its patient records.	Transformation	GP	eDEC
(IND190.0) The practice makes 25% of their appointments available for booking online (this relates to the complete range of appointments practices offer to patients).	Core & Mandated	GP	eDEC
(IND191.0) The practice can process directly booked appointments from NHS 111.	Core & Mandated	GP	eDEC

APPENDIX D – GP IT Specification Commissioning Support Pack

This support pack has been developed to support ALL CCGs who are procuring 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

1. GPIT Specification Support Pack v3.0.docx

2. GPIT Data Capture Service Schedule v3.0.xlsm *

(* note this is a macro enabled Excel spreadsheet)

APPENDIX E – Procurement Technical Checklist

Practices and CCGs purchasing non-GP IT Futures Framework clinical systems and digital technologies which include hosting patient identifiable information should ensure that the system provider (as data processor) where applicable is able to:

1.1	Provide Information Governance assurances for their organisation via the NHS Data Security and Protection Toolkit.	
1.2	Confirm that the manufacturer/developer of the system has applied clinical risk management as required under DCB0129 (Clinical Risk Management: it's Application in the Manufacture of Health IT Systems) during the development of the product procured.	
1.3	Confirm where the product procured is classified as a medical device the product complies with the medical device directives.	
1.4	If the digital service uses a clinical decision support tool (i.e. utilising predefined algorithms and/or a knowledge base) for direct use by the patient or a remote clinician, provide details on how these are checked for accuracy and provenance.	
1.5	Comply with national guidance on citizen identity verification, including "Patient Online Services in Primary Care - Good Practice Guidance on Identity Verification".	
1.6	As data processor can and will comply with GDPR and DPA legislation. This will include providing a compliant Data Processing Agreement.	
1.7	If data is hosted outside England provide • 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.	
1.8	Describe how the system 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.	
1.9	As data processor can support the practice (the data controller) in carrying out a DPIA.	
1.10	Has a defined process for assessing third party products and evidence that any third-party products have been assessed against all relevant standards.	
1.11	Provide details on any clinical coding system used for (history, diagnosis, symptoms, findings, diagnostic investigations and results, treatment, prescribed drugs).	

1.12	Confirm the system uses the NHS number as primary patient identifier	
1.13	Describe how the support for the system will be provided during practice business hours.	
1.14	Describe how the system will be maintained and upgraded (operationally, technically and contractually).	
1.15	How the system integrates with the practice clinical system and what standards are used to integrate.	
1.16	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 system 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 and CCGs purchasing GP IT hardware equipment where applicable are able to:

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 GP IT managed infrastructure.	

APPENDIX F – Glossary of Terms

Term	Description
ADSL	Asymmetric Digital Subscriber Line
ANM	Advanced network Monitors
APMS	Alternative Provider Medical Services
ATP	Advanced Threat Protection
BC	Business Continuity
BCP	Business Continuity Plan
BCS	British Computer Society
BMA	British Medical Association
BYOD	Bring Your Own Device
CAG	Citrix Access Gateway
CareCERT	Care Computer Emergency Response Team
CAS	Central Alerting System
CCG	Clinical Commissioning Group
CCN	Change Control Notice
CE	Cyber Essentials
CE +	Cyber Essentials Plus
CIS	Care Identity Service
CNSP	Consumer Network Service Providers
COIN	Community of Interest Network
CQRS	Calculating Quality Reporting Service
CRM	Customer Relationship management
CTV3	Clinical Terms Version 3
DCB	Data Coordination Board
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
DHSS	Department of Health & Social Care
DoF	Director of Finance
DPA	Data Protection Act

DPIA	Data Privacy Impact Assessment
DPO	Data Protection Officer
DR	Disaster Recovery
DSP	Data Security and Protection
DSPT	Data Security and Protection Toolkit
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
FMD	EU Falsified Medicines Directive
FOIA	Freedom of Information Act
FTTC	Fibre to Cabinet
GDPR	General Data Protection Regulation
GDUK	General Dynamics United Kingdom
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
GPFV	General practice Forward View
GPSI	General Practitioner with Special Interests
GPSoC	GP Systems of Choice Framework
HSCN-GP	Health & Social Care Network for General Practice
HSSF	Health Systems Support Framework
ICO	Information Commissioner's Office
ICS	Integrated Care Systems
IFU	Instructions For Use
IG	Information Governance
ISMS	Information Security Management System
ITT	Invitation to Tender

IVDR	In-Vitro Diagnostic medical device Regulations
KPI	Key Performance Indicator
LA	Local Administrator
LDR	Local Digital Roadmap
LMC	Local Medical Committee
LMS	Learning management system
LPF	Lead Provider Framework
MDR	EU Medical Devices Regulations
MESH	Message Exchange for Social & Health Care
MHRA	Medicines and Healthcare Products Regulatory Agency
MSP	Managing Successful Programmes
National Commercial & Procurement Hub	National Commercial & Procurement Hub
NCSC	National Cyber Security Centre
NDG	National Data Guardian
NHSID	NHS Identity
ODS	Organisational Data Services
P3M	Project, Programme and Portfolio Management
PAT	Portable Appliance Testing
PC DMAT	Digital Primary Care Maturity Assurance Tool
PCN	Primary Care Network
PDS	Personal Demographics Service
PHMD	Population Health Management Dashboard
PMS	Personal Medical Services
Prince II	PRojects IN Controlled Environments 2nd edition
Principal Clinical System	GPSoC Principal Clinical System
QOF	Quality Outcomes Framework
RA	Registration Authority
PBAC	Position Based Access Control
RCGP	Royal College of General Practitioners
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SCR	Summary Care Record
SFI	Standing Financial Instructions
SIRI	Serious Incidents Requiring Investigation

SIRO	Senior Information Risk Owner
SLA	Service Level Agreement
SMS	Short Message Service
SoSHSC	Secretary of State for Health and Social Care
STP	Sustainability & Transformation Plan
VDI	Virtual Desktop Interface
VPN	Virtual Private Network
W10	Microsoft Windows 10
WES	Warranted Environment Specification
WiFi-GP	WiFi-GP access for practice staff and patients in general practice
WMS	Windows Managed Service