THE SERVICES

Service Specification

Service	**Primary Care IT Support Service**
Commissioners	**NHS Hull Clinical Commissioning Group, NHS East Riding of Yorkshire Clinical Commissioning Group and NHS England**
Provider Lead	
Period	**1 April 2020 - 31 March 2025**
Date of Review	**31 March 2022**

1. Local / National Context

NHS Hull Clinical Commissioning Group, NHS East Riding of Yorkshire Clinical Commissioning Group and NHS England ("the Commissioners") are seeking an IT Delivery Partner who will provide a proactive, responsive and customer focussed GP IT support service to member GP practices, which, as at 30 April 2019, are 67 GP practices, across 107 sites within the geographical area (NHS Hull CCG - 35 GP practices (52 sites); NHS East Riding of Yorkshire CCG - 32 GP practices (55 sites)).

From a geographical perspective, it will be essential to recognise the alignment that the Commissioners, have as members of the Humber locality whilst ensuring that an emphasis on placed based care is established

Locally we have a Humber Locality Local Digital Roadmap Board, which is responsible for agreeing a shared digital agenda. It is essential that any trusted IT Delivery Partner is an active member of the Humber Local Digital Roadmap Board and support its ongoing work.

Nationally the CCG and it's trusted IT Delivery Partner need to support and implement a number of national initiatives, including but not limited to the GPIT Operating Model, The NHS 10 year Future Plan & GPIT Futures schemes.

2. Aims / Objectives

The IT Delivery Partner is expected to provide and deliver a quality focussed and resilient service model which operates in a sustainable, innovative and flexible way, ensuring service user satisfaction throughout. The service forms a fundamental and integral element of providing responsive front line clinical services. The service provided needs to be reliable, responsive, of high quality and deliver efficient IT systems in supporting the provision of patient care. The IT Delivery Partner will keep up-to-date with all local and national requirements and work closely with the CCGs to help it plan better, to discharge their statutory duties and, via the use of IT, exploit technology and systems. The service will operate in an environment of ever increasing demand for digital services; changes and development in technologies; and changing demands of both the local and wider healthcare economy.

The key principles of service delivery are to:

- Ensure that any transfer and transition of services is effectively managed to ensure a continuation of the existing level of service provision and to prevent de-stabilising the delivery of clinical services;
- Ensuring that Services are supported on a 24/7 basis as appropriate to requirement
- Ensuring that all systems, and associated infrastructure are securely operated and maintained
- Ensure a proactive support service is available, supporting a clinically essential service, with robust incident management processes;

- Propose innovative and cost effective strategies to address service improvement and sustainability and /or create financial efficiencies;
- Fully understand all local and national requirements and work closely with the CCGs to help them plan better; to discharge their statutory duties; and exploit technology and systems in support of the challenging NHS transformation agenda.

3. Service Delivery Requirements

The fundamental IT services to be delivered are to enable the effective commissioning and delivery of health and care. The service must be compliant with the Core and Mandated GP IT services for General Medical Services (GMS), Personal Medical Services (PMS) and Alternative Provider Medical Services (APMS) contractual conditions regarding IT and must align to:

- Securing Excellence in GP IT Services 2016 - 18 Operating Model. https://www.england.nhs.uk/wp-content/uploads/2017/03/gp-it-operating-model-16-18.pdf
- Securing Excellence in GP IT Services, 2016-18 (revisions) and the 2018/19 Addendum to the GP IT Operating Model https://www.england.nhs.uk/wp-content/uploads/2018/06/2018-19-Addendum-GP-IT-Operating-Model-2016-18-Revisions.pdf
- Securing Excellence in GP IT Services, 2016-18 (revisions) Appendix 5: GP IT Commissioning Specification Support Pack https://www.england.nhs.uk/wp-content/uploads/2018/06/gpit-specification-support-pack.pdf
- Investment and evolution: A five-year framework for GP contract reform to implement The NHS Long Term Plan https://www.england.nhs.uk/wp-content/uploads/2019/01/gp-contract-2019.pdf

The IT Delivery Partner, as a minimum, will adhere to:

- Provision of service desk functions compliant with ITIL Version 3 (or equivalent), with a commitment to accredit to ITIL Version 4, and operating to standards ISO 20000 and ISO 9000;
- Achieving ‘Standards Met’ against the NHS Data Security and Protection Toolkit (DSPT) version applicable to the Supplier organisation type e.g. “Company” or “Commissioning Support Unit” for their organisation and the services delivered under the GP IT services contract (or any successor framework). Note: Present and future reviews of standards of data security for confidential data across the NHS is continuous and the IT Delivery Partner will be required to adhere to, and support the CCGs to adhere to, the outcomes of these reviews;
- Organisational compliance with ISO 27001 standard for Information Security Management;
- Holding a current Cyber Essentials (CE), as a minimum and evidence of working towards Cyber Essentials Plus (CE+), certificate from an accredited CE Certification Body;
- Committing to and supporting the implementation of the National Data Guardian ten standards on data security;
- Compliance with EU General Data Protection Regulation (GDPR) as a data processor;
- Ensuring the provision of business critical systems and applications, currently, but not limited to:
  - Clinical systems - e.g. SystmOne, EMIS;
  - National applications and hosted services - e.g. eRS (e-referrals); Liferay; EPS2, SCR; Patient Online; Oracle Financials; Broadcare; NHS email;
  - Microsoft Office;
  - Microsoft Exchange Outlook (e-mail);
  - Network File and Print Services;
- Having robust disaster recovery and business continuity plans, reviewed, tested and validated annually for services critical to GP service continuity compliant with "NHS Business Continuity and Disaster Planning - Good Practice Guideline", these plans should include a response to threats to data security, including significant breaches or near misses;
- Working in full collaboration within other CCG commissioned third party providers, under clearly defined responsibilities and with support agreements being in place;

- Supporting the evaluation of potential third party suppliers of ICT related services commissioned by the Commissioners;
- Complete transparency of the development and delivery of the IT Delivery Partners own IT strategy supporting GP IT, including but not limited to infrastructure, application support and service desk;
- Sharing of good practice and innovative ways of working supporting new models of care deployed in other CCG locality areas;
- Transparent costs to maintain the GP IT service within the financial envelopes;
- Flexibility to optimise delivery across services and recipients to ensure value for money within the contract.

The IT Delivery Partner will be expected to deliver a range of services, which cover, but are not limited to - Appendix A provides further detail:

- Service Desk Support (Service Ref 1.1);
- General Infrastructure Service (Service Ref 1.2);
- Desktop Maintenance and Support Service (Service Ref 1.3);
- Disaster Recovery and Business Continuity (Service Ref 1.4);
- Asset Management and Software Licensing Service (Service Ref 1.5);
- Cyber Security (Service Ref 1.6)
- General Data Protection Regulation (EU) 2016/679 and Data Protection Act 2018 (Service Ref 1.7);
- Supplier Management and Procurement Service (Service Ref 2.1);
- Technology Infrastructure Refresh Service (Service Ref 3.1);
- Training Service (Service Ref 4.1);
- Project and Change Management Service (Service Ref 5.1);
- Client Relationship Management Service (Service Ref 6.1);
- Locality / District / ICS / STP wide Initiatives (Service Ref 7.1);
- Estates Strategy (Service Ref 8.1);
- Registration Authority (Service Ref 9.1) *;
- Email service (NHSmail) Local Organisation Administrator (Service Ref 10.1) *;
- Information Governance (Service Ref 11.1) *;
- Clinical Safety Assurance (Service Ref 12.1) *

* for the highlighted services there is a requirement to provide support to all primary care contractors (Community Pharmacies; Dental Practices; and Primary Ophthalmic Practices, for whom NHS England Area Team hold contracts), that have access to and use of national clinical information systems.

In providing services to GP Practices, the IT Delivery Partner will manage incident / requests received in line with the categories / priorities presented at Appendix B - Incident and Request Prioritisation and Target Response Times Matrix.

3.1 Projects

In addition, at the point of the service commencement, it is anticipated a number of projects will be in progress, these may include:

- Health and Social Care Network (HSCN);
- Windows 10;
- Office replacement;
- NHSmail;
- GP practice clinical system mergers and migrations;
- Govroam deployment;
- Shared Care Record deployment
- Building moves and changes

The IT Delivery Partner will be required to take on the responsibility for the completion of any projects in progress.

3.2 Technical Expertise Support Representation

The IT Delivery Partner will be required to ensure it is appropriately represented*, contributes and provide technical expertise to key strategic IM&T meetings, as required by Commissioners. Examples of key strategic IM&T meetings are (but not limited to):

- Local Digital Roadmap Board (monthly meeting - IT/Digital Strategy and Delivery updates from Humber wide locality);
- Primary Care IMT Strategy (monthly meeting - Primary Care IT/Digital Strategy and Delivery updates from CCG locality);
- Emergency Preparedness Resilience and Response - in the event of a major or unforeseen incident the IT Delivery Partner will form an active part of the response committee. The IT Delivery Partner is required to provide pro-active support during such instances.

*Appropriately represented defined as an individual who has delegated decision making authority.

3.3 Service Operating Hours

The IT Delivery Partner must ensure the service provision is available, as a minimum, during the following hours:

- Service Desk Support

Core Hours
Monday to Friday - 08:00-20:00
Saturday, Sunday and Bank Holidays - 08:00-15:00
The Service Desk Support provision is to be staffed throughout the operating hours in order to be contacted (via phone or web portal) to log, respond and seek resolution to incidents / requests.

Out of Hours
Monday to Friday - 20:00-08:00
Saturday, Sunday and Bank Holidays - 15:00-08:00
Out of Hours the Service Desk Support provision is to operate an ‘on-call’ arrangement to allow for the notification and management of major incidents/Priority 1 to the Commissioners

- General Infrastructure Service; and
- Cyber Security

Service availability is to be available 24 hours a day, 7 days a week, 365 days a year, subject to planned downtime

- All other service requirements

With the exception of Service Desk Support; General Infrastructure Service; and Cyber Security service, the services are to be available and delivered during the following hours:
Monday to Friday - 08:00-18:30

3.4 Scope of Service Recipients

The scope of services is to be provided to GP practice staff as a NHS England delegated responsibility to the CCG.

The Commissioners may wish to extend the service to include IT support for other organisations and service - this is a local CCG discretionary decision with additional funding where agreed.

3.5. Location of Services

The Commissioners do not provide, or intend to provide, accommodation for the housing of centralised infrastructure, storage or the IT Delivery Partners’ staff, unless otherwise specified.

Appendix A - Service Requirements Summary Detail

Service Name	Service Ref	Service Description	Service Standards	Customer responsibility	Additional services not funded in main contract
Service Desk Support - 1.1					
Service Desk	1.1.1	The Service Desk provides a single point of contact (SPOC) for all IT incidents and service requests. The Service Desk must be accessible to all users via all of the following: • a single telephone number (which must not be a premium rate service nor require an access charge); • single email address; • a web portal available for users to log and manage calls. It must be possible for all users to log a call using at least one of the above methods 24hrs per day, 7 days per week A single ticket will be allocated for the duration of a call. The IT Delivery Partner will provide the ability to re-open an incident / request should the user not be satisfied with the proposed resolution implemented to close the incident / request. * Should such instances occur, and for the avoidance of doubt the incident / request would be considered open, with the original date of incident / request being used to measure performance against target fix times for the priority allocated to the incident / request. The Service desk should be accredited to a recognised standard e.g. Service Desk Institute (SDI) in addition staff that are delivering this service must be fully trained in customer service skills, ideally by an accredited customer service standard or equivalent programme. As a minimum the Service Desk will provide the following functions: • Triage - Initial assessment and categorise / allocate a priority of the incident/service request (as set out in Appendix B); • Incident management - All calls & service requests will be managed in accordance with ITIL V3 processes from incident logging to incident closure. Incidents and service requests will be escalated by the Service Desk to	Quality Management System - ISO 9001:2015 Information Security Management System - ISO/IEC 27001:2013 IT Service Management - ISO/IEC 20000-1:2011 Information Technology Infrastructure Library (ITIL) v3 https://www.axelos.com/best-practice-solutions/itil/what-is-it-service-management	Report all IT incidents and requests for change to the IT service desk by telephone, email or web interface. Provide service desk with required information to allow the correct recording of incident/request for change. Allow IT Delivery Partner staff reasonable access to premises or access to IT equipment via remote control to allow incident resolution to take place. When escalating logged incidents to provide the incident reference number. Ensure staff take appropriate action when advised of IT service downtime	Support for organisations other than the direct customer (e.g. GP practices for non-funded services, services AQPs, etc.)

Service Name	Service Ref	Service Description	Service Standards	Customer responsibility	Additional services not funded in main contract
		appropriate support groups with an appropriate priority assigned (as set out in Appendix B) and agreed with the customer depending on the severity. The Service Desk will retain ownership of the calls throughout the lifecycle of the incident; • Resolution - The Service Desk will attempt to resolve all calls on initial contact. This will involve resetting all passwords; securely remotely accessing PCs to resolve incidents and providing advice to the user when required; - The Service Desk will ensure the user is provided with a summary of incident / request fulfilment following completion of support provided. In addition, the service desk will offer, undertake and/or provide: • General IT advice & guidance; • Audits and investigations; • Communications - proactively informing users of any planned System or Network downtime where there will be an impact on a key system or site; • Provide users with access to a comprehensive Knowledgebase, with guides and/or videos to frequently asked questions; • Proactively identify common service desk requests, where possible identify and implement improvement and, where indicated, develop user self-help resources. (e.g. on line self -service password reset tools), as a minimum monthly; • Inform the nominated members of staff including the CCG IT manager or deputy of all Priority 1 incidents and provide timely updates throughout the incident period, process as agreed with CCGs; • Proactively manage incidents and problems referred to 3rd parties ensuring timely updates, as defined by service level agreements with 3rd party supplier, advised to customer and escalated accordingly.			
Telephone Logging Service	1.1.2	The provision of a service to allow users to log calls to the Service Desk via a single UK telephone number which must not be a premium rate service nor require an access charge.			

Service Name	Service Ref	Service Description	Service Standards	Customer responsibility	Additional services not funded in main contract
		All calls will be logged, categorised and prioritised on the Service Desk system and allocated a unique reference number which will be provided to the customer for each call raised. Outside core hours callers should be referred to a web portal, and responded to within the defined timescales of the category / priority of the incident / request. Responded defined as contacting the relevant parties to provide an update on plans to resolve notified issue.			
Email Logging Service	1.1.3	The provision of a service to allow users to log calls to the Service Desk via a single email address. Calls can be logged 24/7; however will be responded to during Core Hours: Monday to Friday - 08:00-20:00; Saturday, Sunday and Bank Holidays - 08:00-15:00. Responded defined as non-automated response to the individual (or delegated party) who raised the incident / request, to provide an update on plans to resolve notified issue. All calls will be logged, categorised and prioritised on the Service Desk System and allocated a unique reference number which will be provided to the customer via email. Outside core hours emails should be referred via an automated response to a web portal, and responded to within the defined timescales of the category / priority of the incident / request.			
Web Portal (Self-Logging / Knowledge Base)	1.1.4	The provision of a web self-service to allow users to log “calls / Service Incidents” via the Web Self Service. This includes the ability to log Service Requests for new Hardware, user Accounts or amendments. Requests can be logged 24/7, however will be responded during Core Hours: Monday to Friday - 08:00-20:00; Saturday, Sunday and Bank Holidays - 08:00-15:00.			

Service Name	Service Ref	Service Description	Service Standards	Customer responsibility	Additional services not funded in main contract
		Responded defined as non-automated response to the individual (or delegated party) who raised the incident / request, to provide an update on plans to resolve notified issue. Once users have logged their requests they will automatically be provided with a unique reference number and initial priority. Users should be able to track all their own calls through the web portal, including the ability to escalate. Outside core hours reports should be responded to within the defined timescales of the category / priority of the incident / request. Provision of a Knowledge base to provide end users with access to up to date user guides and fixes to frequently asked questions. Provision of self-help tools including password reset, where appropriate (e.g. NHSmail).			
Out of Hours Major incident reporting -	1.1.5	Major incident defined as any situation which results in non-standard arrangements for service provision to be implemented - e.g. Cyber Attacks; Floods; Infrastructure disruption. Provide a 24/7 facility where major incidents can be reported to the supplier by representatives of the CCG.		To notify IT Delivery Partner of major incident details	
Account Administration	1.1.6	Provision of an active directory account administration service which includes the creation, amendment, deletion and auditing of all user accounts. Management of GP Practice distribution list (e.g. Practice Manager; Practice Secretaries; Practice Nurses). This service ensures only fully authorised users are allowed access to the Network by checking the appropriate approval has been received for each request.		Ensure internal processes (e.g. starter / leaver management) are in place so that only authorised users are granted access to the agreed resources.	Support for organisations other than the customer e.g. AQPs, GPSI services and other CCG commissioned and sponsored services.

Service Name	Service Ref	Service Description	Service Standards	Customer responsibility	Additional services not funded in main contract
		Carry out monthly audits to ensure only appropriate users are active (non-active users defined as no access within 3 months) on the network.			
Access Control Administration	1.1.7	Provision time limited (up to a maximum of 12 hours) administration access to GP Practice Managers or delegated users to allow for software updates, or CCG approved software installations. Password for administration access accounts to be unique for each request. The IT Delivery Partner to liaise with Commissioners to gain approval for all new software installations. The IT Delivery Partner will not be liable for any detrimental impact on the provision of IT services relating to software installed or updated through the provision of administration access to GP Practice Managers or delegated users.		Description of software; requirements for administration rights (i.e. software update, or request for installation of software); and source of the installation file. To notify the IT Delivery Partner when the installation has been completed.	Support for organisations other than the customer e.g. AQPs, GPSI services and other CCG commissioned and sponsored services
General Infrastructure Services - 1.2					
Active Directory	1.2.1	Provision of Active Directory services to allow access to desktop and server resources. All users will be provided with a unique Active Directory account on a suitable domain. Any planned downtime is to take place outside of core hours. The IT Delivery Partner will liaise with the relevant CCG to agree the process and communications for any planned downtime, the expectation that a minimum 48 hours' notice will be provided - in exceptional circumstances the notice period may be reviewed.	Ensure internal processes agreed with the customer in place so that only authorised users are granted access to the agreed resources.	Ensure internal processes agreed with the IT Delivery Partner are in place so that only authorised users are granted access to the agreed resources.	Support for organisations other than the customer e.g. AQPs, GPSI services and other CCG commissioned and sponsored services.
Data Storage	1.2.2	Provision and management of sufficient secure on premise or secure cloud storage to host the customer's data including archived email. Data centre design and operation should be to a standard not less than	Provision and management of sufficient secure	To ensure that stored data is appropriate and relevant for	Support for organisations other than the customer e.g.

Service Name	Service Ref	Service Description	Service Standards	Customer responsibility	Additional services not funded in main contract
		tier 3 data centre. Facilitate access to secure cloud hosted storage and document management solutions (including but not limited to AWS, MS Azure, Microsoft Office 365, Kahootz, etc.). Where agreed with the CCG, provision of document management solutions e.g. SharePoint Any planned downtime is to take place outside of core hours. The IT Delivery Partner will liaise with the relevant CCG to agree the process and communications for any planned downtime, the expectation that a minimum 48 hours' notice will be provided - in exceptional circumstances the notice period may be reviewed.	storage to host the customer's data including archived email.	business use only.	AQPs, GPSI services and other CCG commissioned and sponsored services.
Network Printing	1.2.3	The ability to host and manage print queues (either on premise or secure hosted) for customer printers. Liaison with 3rd party print solution providers. For clarity, in addition support locally connected printers and queues. Provide support for strategically beneficial printers - e.g. MFD style devices.			Support for organisations other than the customer e.g. AQPs, GPSI services and other CCG commissioned and sponsored services.
Backup & Restore	1.2.4	All customer data saved to a network drive will be backed up to an offsite location on a regular basis defined as: • Minimum of twice daily to in-house or secure cloud hosted repository; • Daily Backups to a secure repository; • Full weekly backups must be maintained for 28 days and offsite (or duplicate data centre) backups for 1 year. Restores will be requested through the IT Service Desk and incident/request categorisation will apply. Maintain detailed procedures to cover: • Backup of all services;	Business Continuity: Good Practice Guide", NHS Digital 2017	Ensure that all requests for restore of data are completed within timescales consistent with retention and recovery times. Backup of data held on local desktop or mobile devices.	Support for organisations other than the customer e.g. AQPs, GPSI services and other CCG commissioned and sponsored services.

Service Name	Service Ref	Service Description	Service Standards	Customer responsibility	Additional services not funded in main contract
		• Recovery of files and/or services from backup; • Deletion of backup data in line with retention policies or upon appropriate request; • Business continuity arrangements; • Audit and Testing of backup and business continuity arrangements; • Checklists for operational staff on common recovery processes. (see also section 1.4.1 Business Continuity & Disaster Recovery)			
Application Hosting	1.2.5	By agreement with the CCG, hosting of server-based specialist applications. Liaison with 3rd party providers to define, implement maintain appropriate server provision or network access including, where agreed with the CCG, support for 3rd party remote access solutions to enable remote management of systems or application.	Provision of sufficient resource to host applications May be subject to agreement to any additional costs for specific hardware	For 3rd party applications ensure required software application licences and support are purchased	Support for organisations other than the customer e.g. AQPs, GPSI services and other CCG commissioned and sponsored services.
Monitoring	1.2.6	Proactive monitoring and alerting of all relevant infrastructure including server, storage and network resources to anticipate and prevent IT incidents ensuring maximum availability. The IT Delivery Partner will need to put in place 24 hour monitoring and alerting system which allows for notification of unexpected / unscheduled system downtime, which may need to be reported to Commissioners	To meet NHS Digital and industry standards e.g. Microsoft System Center, Cisco network management.		
Remote Access	1.2.7	The provision and support of a secure remote access solution to provide access to hosted IT Clinical Systems and local network or cloud service resources from outside of the GP Practice from Managed devices. Where agreed with the CCG provide support and/or provision of 3rd party remote access solutions for instance to include HSCN remote access (i.e. BT N3 VPN, AuthenText or similar service).	Service should be a core offering for all users and not subject to further per user licence or support charges. Unsupported software (by software supplier), browsers, operating systems or devices		Support for VPN or similar services to access practice business systems e.g. HR, payroll, finance (Note: these may be funded directly by a practice) - subject to cyber security constraints i.e. BT N3 VPN or

Service Name	Service Ref	Service Description	Service Standards	Customer responsibility	Additional services not funded in main contract
			must not be used to access patient record systems (NDG standard 8) Connections between mobile/portable/remote devices to Health and Social Care Network (HSCN)/N3 and practice clinical systems using public network services (internet) must be encrypted to approved NHS standards.		similar service
LAN / WAN Network Services (Excluding Wireless)	1.2.8	Provision of management, support, and where appropriate configuration, of: • HSCN connections to main and branch practice sites as per national entitlement and local determination. • Wide Area Network / Private Network / Community of Interest Network (COIN) utilising shared connectivity with other partners wherever practicable and cost effective. • Secure connectivity to cloud data centres. • Filtered and managed Internet connections to all sites (where not provided through HSCN gateway) or support/management of internet access though liaison with HSCN service provider; • Any changes to IP schemes are considered business as usual. Provision of network connectivity with sufficient bandwidth, low latency and low contention ratio to support the necessary digital services. (Subject to affordability agreement with CCG). Support all active network devices (e.g. switches routers etc.) including configuration and deployment management etc. Patch management of all connected devices	https://digital.nhs.uk/health-social-care-network	Allow IT Delivery Partner informatics staff reasonable access to premises or access to IT equipment Provide clear access, safe working and adequate power provision to network communications cabinet.	OOH support Additional bandwidth required by practice where other services (e.g. OOH, AQP etc.) are operated from same location as GP Practice as agreed.

Service Name	Service Ref	Service Description	Service Standards	Customer responsibility	Additional services not funded in main contract
		Liaison with 3rd party network cabling contractor(s). Service availability - Commissioners acknowledge in exceptional circumstances third party provider service standards and availability may impact upon delivery.			
Wireless Services	1.2.9	A Wi-Fi service for GP practice sites for a range of service set identifiers (SSIDs) including but not limited to staff, guest, public, Govroam.	A Wi-Fi service for each CCG and practice meeting the NHS Wi-Fi Technical & Security Policies and Guidelines https://digital.nhs.uk/nhs-wi-fi/GP-practices Wi-Fi service usage must not impact on core general practice activities in particular performance of GPSoC hosted systems and NHS national systems Unsupported software (by software supplier), browsers, operating systems or devices must not be used by the practice to access the “corporate” Wi-Fi network in the practice. Bring Your Own Device (BYOD)	Allow IT Delivery Partner informatics staff reasonable access to premises or access to IT equipment Provide clear access, safe working and adequate power provision to network communications cabinet. Locally agreed Acceptable Use Policies, must be in place which should cover all wireless network services provided, including Guest & Public WIFI.	Subject to CCG agreement on affordability provide additional services, WAPs or SSIDs beyond core provision

Service Name	Service Ref	Service Description	Service Standards	Customer responsibility	Additional services not funded in main contract
			services (for staff) can only connect to the supported infrastructure using the public/guest Wi-Fi service and must not be used to process patient identifiable data. Govroam SSID should be available - http://www.yhpsn.org/Services/Govroam/		
Telephony Service	1.2.10	Provision, maintenance and technical support of the necessary infrastructure to support existing and new phone systems.			
Maintenance, Support and Provision of Email Accounts	1.2.11	Delivery of a legacy Microsoft Exchange email service in accordance with industry standards and service level agreements until such a time that migration to NHSmail or Office365 is completed. Provision of one email account per individual on request. Provision of shared / generic email accounts on request. The on-going maintenance of email accounts, which includes the moving and deleting of accounts, password resets and unlocking accounts.		Timely notification of starters and leavers within organisation Where available the customer will use self-service.	
Desktop Maintenance and Support Service - 1.3					
General Desktop Support Services	1.3.1	Provision of second and third line break/fix technical support for desktop hardware, software and peripherals. Provision of planning and implementation services for requested installations and moves, together with asset management, configuration management and documentation of desktop assets.	Resolve faults by telephone advice, remote technical support or by site visit. Keep customer	Allow IT Delivery Partner informatics staff reasonable access to premises or access to IT equipment via remote	Support for organisations other than the customer e.g. AQPs, GPSI services and other CCG commissioned and

Service Name	Service Ref	Service Description	Service Standards	Customer responsibility	Additional services not funded in main contract
		Support is undertaken via remote and onsite activities and adheres to agreed service level agreements. Provision of anti-virus, malware protection, encryption and access management service (see also section 1.6 Cyber Security). Deployment of core GPIT Software and other software as agreed by the CCG. Support for the assessment (including compatibility and security considerations) and, where agreed by the CCG, installation of GPIT software requested by the practice. Provide technical liaison with GP system supplier. On-going technical support for general practice core clinical systems including clinical application support where not provided by GP system supplier. (e.g. Java, browser). Liaison with core GP system supplier for management of on-going system updates as necessary.	informed and updated on progress of related incident. Regularly update relevant Service Desk software with current status. Achieve agreed KPIs. Unsupported software (by software supplier), browsers, operating systems or devices must not be used to access patient record systems (NDG Standard 8)	control to allow incident resolution to take place. The practice is responsible for the physical security, PAT testing and power supply for IT equipment	sponsored services. OOH support e.g. for Extended hours GP services Support for GP business systems unless otherwise agreed with the CCG.
Computers / Workstations	1.3.2	Installation and support of all CCG provided computers, laptops and other mobile computing devices, and peripheral equipment, meeting security standards and compatibility constraints such as mobile device management, encryption, remote lock, remote wipe, etc. Installation and support of all standard software and applications. Support for the assessment (including compatibility and security considerations) and, where agreed by the CCG, installation of additional software. Emergency equipment procured by the CCG will be maintained and held in the event of network failure e.g. spare laptops, printers, scanners etc.	Guidance on the implementation of encryption within NHS organisations", NHS Digital	Allow IT Delivery Partner informatics staff reasonable access to premises or access to IT equipment via remote control to allow incident resolution to take place. Agree with IT Delivery Partner the core hardware and software through	Support for organisations other than the customer e.g. AQPs, GPSI services and other CCG commissioned and sponsored services. Purchase and support of non-core GPIT hardware

Service Name	Service Ref	Service Description	Service Standards	Customer responsibility	Additional services not funded in main contract
		Maintenance of adequate stock levels of replacement equipment and spare parts to support agreed incident resolution times. The user workstations are locked down and managed via active directory group policies. Users are not able to install software or change critical settings. Produce and Maintain Standard Operating Procedures (SOP). Keep customer informed and updated on progress of related incident Defined and documented standardised desktop image(s) to included contact details (web-portal; phone; e-mail) for Service Desk Support and any urgent service information, with a formal change control management system.		Warranted "supported" Environment Specification" - updated at least on annual basis The purchase of extended or additional warranties for NHS England-owned hardware is the responsibility of the CCG. Purchase of adequate stock of replacement equipment and spare parts to support agreed incident resolution times will be the responsibility of the CCG (where agreed). Costs for repair of hardware outside warranty period or not covered by warranty.	
Peripheral Equipment Management	1.3.3	Deploy and maintain other hardware, for example including but not limited to: check-in kiosks, call screens, scanners, smartcard readers, barcode readers, printers including dual bin feed printers for consulting rooms and MFDs, where necessary. Where the installed & supported equipment is covered by a warranty, the IT Delivery Partner will engage with the manufacturer's support services to arrange repair or replacement, where necessary.		Consumables are the responsibility of the customer. The purchase of extended or additional warranties for NHS England-owned hardware is the responsibility of the	Purchase and support of non-core GPIT hardware Support for medical or practice acquired devices which should be the responsibility of the device providers.

Service Name	Service Ref	Service Description	Service Standards	Customer responsibility	Additional services not funded in main contract
		Liaison with 3rd party hardware providers (e.g. managed print solutions, clinical systems etc.) where required for specification, installation and support. Priority matrix for service requests / incidents as per Service Desk (Appendix B)		CCG. The practice should ensure that warranties and support for medical devices remains in place Costs for repair of hardware outside warranty period or not covered by warranty	
Disaster Recovery and Business Continuity - 1.4					
IT Delivery Partner Disaster Recovery (DR) and Business Continuity (BC)	1.4.1	• Business Continuity requirements The IT Delivery Partner will ensure all data changes over a 24 hour period will be backed up and stored off site. Note enhanced data backup services where provided will allow more frequent backup schedules. Maintain system status information with alerts for critical downtime/failures ensuring this reflects 100% of known issues and is not more than one working hour out subject to 3rd party provider information. For business critical incidents (priority level 1) a Lessons Learned Report (with relevant action plan as appropriate) to be provided to customer within 2 weeks of the recorded resolution of the incident on the service desk • Business Continuity and Disaster Recovery plan and arrangements The IT Delivery Partner is required to maintain an annually reviewed business continuity plan and validated IT disaster recovery plan for services provided within this specification. The plans are to be submitted to Commissioners annually by 1 April of each year. In the event of a major event when the plan is utilised this will trigger a review of the plan and reset the 12 month review period.			

Service Name	Service Ref	Service Description	Service Standards	Customer responsibility	Additional services not funded in main contract
		Disaster Recovery and Business Continuity Plan must be tested every 12 months as agreed with the CCGs and include a lessons learnt document which will be shared with Commissioners The Business Continuity plan will include continuity plans in response to threats to data security, including significant breaches or near misses. These plans will be based on a Recovery Time Objective as agreed with the Commissioners for essential IT services. In the event of the IT Delivery Partner Disaster Recovery or Business Continuity plan being invoked where services relevant to this specification are impacted, the IT Delivery Partner will provide an initial notification to CCG IT managers or deputies within one hour of the incident, followed by updates within timescale in accordance with agreed incident plan. A resolution report within 12 hours of resolution or within 72 hours in the case of serious incidents (and a full report including root cause and remedial actions within two weeks of the incident) to CCG IT managers or deputies.			
Business Continuity Support to practices	1.4.2	Provision of IT advice and guidance in relation to IM&T to support the development of GP practice business continuity plans. Provide Incident Support - to individual practices and CCGs or wider through identified Business Continuity Plan lead. Request for advice and guidance would be dealt with in accordance with service request / incident priority matrix.	Business Continuity arrangements for CCGs and general practice infrastructure must include the ability to isolate sites and/or individual devices, where there is an identified incident or high severity threat (relevant to that site), including the capability to isolate affected PCs from the network	Develop and maintain CCG and practice business continuity plans. Completion of the NHS England Business Impact Assessment template	

Service Name	Service Ref	Service Description	Service Standards	Customer responsibility	Additional services not funded in main contract
			immediately following detection of a cyber-attack.		
Disaster Recovery Support to practices	1.4.3	Provision of IT advice and guidance to support the development of CCGs and GP practice disaster recovery plans. Emergency equipment (funded by the CCG) will be held in the event of network failure e.g. spare laptops and mobile data cards 3G/4G, as agreed with the CCGs. Provision of support to GP practices in the event of a disaster recovery plan being invoked. Examples of this support could be liaising with third party suppliers e.g. Network provider / GP clinical system suppliers. Support and assurance to CCGs and Practices to ensure that resources hosted on IT Delivery Partners' central infrastructure have adequate DR provision. The IT Delivery Partner will be required to provide extended support as required in the event of a service level disaster. Request for advice and guidance would be dealt with in accordance with service request / incident priority matrix.		Develop, maintain and test CCG and practice disaster recovery and business continuity plans. Practice and CCG business continuity plans will include continuity plans in response to threats to data security, including significant breaches or near misses (NDG standard 7)	
Asset Management and Software Licensing Service - 1.5					
Assets - Hardware	1.5.1	100% of assets will be maintained via an electronic Configuration Management Database (CMDB). All assets (devices or systems purchased by or on behalf of the CCGs) will be provisioned with a unique asset tag and recorded in the CMDB. To note - any assets purchased by the practice through the IT Delivery Partner or CCG should be separately identified and recorded on the asset register. The lifecycle of any asset can be reported on via the electronic CMDB at any time.	Maintain accurate electronic asset list. Provision of unique asset tag records for all relevant equipment, maintaining inventory, collating and monitoring against procurement/disposal	Provide IT Delivery Partner with information relating to any hardware move, additions or deletions.	Support for organisations other than the customer e.g. AQPs, GPSI services and other CCG commissioned and sponsored services.

Service Name	Service Ref	Service Description	Service Standards	Customer responsibility	Additional services not funded in main contract
		The IT Delivery Partner is required to support on annual basis, an asset management refresh programme, this will be performed in line with NHS England criteria and funding.	and provision of appropriate asset management reports Relevant equipment includes: • Any device purchased using NHS England capital • Identified assets purchased by the practice through the IT Delivery Partner or CCG. Unsupported software (by software supplier), browsers and operating systems must not be used on managed equipment (NDG standard 8)		
Disposal of equipment	1.5.2	As agreed with the CCGs all assets will be disposed of via an authorised supplier and will be destroyed in line with EU and National Regulations and The Waste Electrical & Electronic Equipment Directive (WEEE), detailed records and certificates will be provided by the authorised supplier. Detailed records of all disposals will be maintained and authorised by senior personnel and the electronic CMDB will be updated accordingly when items are disposed of. All hard drives will be removed prior to disposal and securely destroyed with an audit trail maintained. Advise the customer if assets returned or collected for disposal could be usefully redeployed. Where redeployed the CMDB should be	EU and National Regulations and The Waste Electrical & Electronic Equipment Directive (WEEE). NHS England hardware disposal policy. Provide a warranted secure hardware disposal service in line with NHS England		

Service Name	Service Ref	Service Description	Service Standards	Customer responsibility	Additional services not funded in main contract
		updated accordingly.	hardware disposal policy. Provide an equipment disposal service compliant with European Community directives 2002/96/EV, The Waste Electrical and Electronic Equipment Directives (WEEE Directive) for all appropriate IT and telecommunications equipment. All data will be removed prior to disposal or redeployment with certificate of destruction to be provided.		
Software Licensing management and support	1.5.3	100% of IT software assets regardless of ownership used on IT Delivery Partner supported devices will be recorded via an electronic Configuration Management Database (CMDB). All software required for the provision of IT services will be maintained by the IT Delivery Partner. Provide advice to the practice and CCG in software licence management and administration ensuring legal. Provide advice on software vendor roadmaps to determine when underlying core products, such as operating system, Antivirus, office productivity etc. or browser, are planned to reach end of life.	Provide software licence and national contract management support to the CCG (ensuring licensing, legal compliance, and national contract management) Standard software for the provision of IT services includes but is not limited to :	Ensure legal compliance for all necessary software licences held by the CCG or Practice including those covered by national agreements held by NHS England or NHS Digital.	

Service Name	Service Ref	Service Description	Service Standards	Customer responsibility	Additional services not funded in main contract
			• Desktop and server operating systems, desktop and server anti-virus software, backup software (if required). • Office productivity software, encryption software, internet browser, email client, backup software, backup validations. • Clinical Systems software aligned to GPSoC (or successor programme) • Mobile device management including encryption All software and operating systems used on managed equipment by the practice 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		

Service Name	Service Ref	Service Description	Service Standards	Customer responsibility	Additional services not funded in main contract
			security risk.		
Asset Storage	1.5.4	The secure storage of all IT equipment not yet deployed or those items awaiting disposal.	Volumes to be agreed.	Volumes to be agreed.	
Cyber Security - 1.6					
Cyber security service delivery	1.6.1	Ensure that all ICT services are delivered in accordance with current and future NHS Digital CareCERT recommendations including • Risk Assessment • Risk Management • Security Architecture • Audit and Review • Incident Management • Penetration Testing • Cyber Incidents response • Vulnerability assessments Vulnerability and, where indicated Penetration, tests will be conducted at an agreed frequency not less than once per annum with outcomes and required actions shared with the CCG subject to maintaining security of findings. Security incident response should include out of hours response and onsite support where required The IT Delivery Partner must act upon and proactively update CareCERT portal with response to security alerts. The CCGs and practices should be assured that all alerts have been appropriately actioned All shared managed infrastructure should have CESG CHECK approved penetration testing carried out at least annually.	The IT Delivery Partner must comply with or have a demonstrable plan to achieve compliance, with all NHS Digital recommendations e.g. CareCERT and Cyber Essentials Plus The IT Delivery Partner must be able to demonstrate that they employ and / or utilise appropriately accredited data security specialists. ISO 27001 for Information Security Management (previously BS 7799) NHS Digital Data Security and Protection Toolkit (or any successor framework) for their organisation and the services delivered under the GP IT	Ensure that all staff receive regular training on Information Governance and Information Security. Maintain and update acceptable use policies Carry out periodic mock cyber incident to increase awareness and test processes.	Additional ad hoc costs for major incident support out of hours to be agreed with the CCG.

Service Name	Service Ref	Service Description	Service Standards	Customer responsibility	Additional services not funded in main contract
			services contract. Comply with the National Data Guardian's ten `standards Comply with the EU General Data Protection Regulation (GDPR) and the Data Protection Act (2018).		
Cyber security standards	1.6.2	Provide an IT Security (Cyber Security) service encompassing all managed infrastructure and systems provided to all practices to ensure: • Adherence to the appropriate security guidance, including - Principles of information security - 'Information Security Management: NHS Code of Practice': - NHS Digital Principles of Information Security - NHS Codes of Practice and Legal Obligations • Provide necessary IT security / cyber evidence (where this is held by the IT Delivery Partner) to support IGT(DSPT) requirements for general practice • Provide a shared Health Social Care Network security contact for practices. • Provide information to support practices in attaining Cyber Essentials Plus (CE+) certification (if / when required by NHSD/E). • Monitoring of managed infrastructure access through Active Directory to identify dormant accounts and operate a process to disable these. • Provide practices with a facility to notify the IT Delivery Partner when staff leave the practice organisation or no longer require IT access, and ensure access is removed within the performance standards for user account management Recommend and review standards on IT security Including risk assurance of proposed new IT systems or applications which attach to the shared network. Note this can include system such		Practices as independent contractors are responsible for sourcing any legal advice they may require.	Costs to support practices in implementation of non-core GPIT systems e.g. telephony, door security, CCTV etc.

Service Name	Service Ref	Service Description	Service Standards	Customer responsibility	Additional services not funded in main contract
		as telephony, door security, CCTV, internet connected devices (i.e. “Internet of Things”) etc.			
Cyber security Monitoring and reporting	1.6.3	Monitor security threats to IT systems and networks, through deployment of defence and incident management, to include: • Access control; • Application control; • Asset Management; • Boundary protection; • Device Encryption (and remote lock/wipe of mobile devices); • Hardware & software management including patching and upgrade; • Network security; • Vulnerability assessment.	Report all identified successful cyber incidents attempts to the CCG.	Acceptance that ability to deploy recommended upgrades may be limited by system/application supplier constraints. The customer should take all reasonable steps to ensure that procured systems are updated in accordance with CareCERT guidance.	
Cyber Security CareCERT	1.6.4	Provide information security consultancy and help with security issues in system design and development. Provide guidance and advice to support staff education and awareness. NHS Digital CareCERT advisories must be acted on in line with suggested timescales, and evidence through CareCERT Collect. Confirmation to Commissioners should be given within 48 hours that plans are in place to act on CareCERT Critical and high severity advisories. A primary point of contact must be registered for the IT Delivery Partner to receive and coordinate the CCGs CareCERT advisories. Note: Action might include understanding that an advisory is not relevant to your organisation’s or practices’ systems and confirming that this is the case.	Conduct unannounced cyber security tests as agreed with the CCG, on a rolling programme basis, to include: • reports, • lessons learnt • Recommendations for improvement.		

Service Name	Service Ref	Service Description	Service Standards	Customer responsibility	Additional services not funded in main contract
Cyber Security Strategy & Advice	1.6.5	Within 6 months of service commencement the IT Delivery Partner will assist the CCG to develop and maintain a strategy for protecting IT systems from cyber security threats which is based on a proven cyber security framework such as Cyber Essentials and the advice and direction of NHS Digital CareCERT service will be developed and maintained locally. This is to be reviewed at least annually. On behalf of the CCG, when mandated by NHS Digital the IT Delivery Partner will: • Register all practices to undertake an on-site data and cyber security assessment through NHS Digital's Data Security Assessment programme; • Fully cooperate with an on-site cyber and data security assessment if invited to do so; • Act on the outcome of that assessment, including implementing any recommendations. Cyber Security Advice to be available to all practices on: • Cyber security audits; • Cyber security investigations; • Specialist (IT Security). The IT Delivery Partner will offer and provide NHS Digital recommended training for GP practices.		Practices will fully cooperate with the NHS Digital assessments and the implementation of any recommendations. CCG board members, CCG and GP senior information risk owner and CIO to take part in NHSD recommended training	
Cyber Security Incident Management	1.6.6	Advice and support for CCGs and practices on incident assessment, reporting and management in accordance with national guidance and legal requirements. To include: • Advice on post-incident reviews and recommended actions for practice implementation; • Leading or directing incident reviews and investigations where highly specialist knowledge is required or complex multi-party issues are involved; • Cyber-attacks against GP services are identified and resisted and		Individual practices are responsible for reporting data and cyber security incidents when they become aware and to implement recommendations from post incident reports	

Service Name	Service Ref	Service Description	Service Standards	Customer responsibility	Additional services not funded in main contract
		CareCERT security advice is responded to by all relevant elements of the GP IT service; • Action is taken immediately following a data breach or a near miss, with a report made to senior management within the CCG and the practice within 12 hours of detection, or as soon as possible in the case of serious incidents; • Report, on behalf of the CCG, cyber incidents and near misses when the organisation becomes aware.			
Cyber Security - Supporting Projects	1.6.7	Advice for practices and the appointed project teams on Cyber Security where projects involve (but not limited to): • New technology and system procurements; • Deploying new technologies and devices; Support for projects beyond general advice for example preparing Cyber Risk Assessments should be resourced as part of the project plan. This service should work closely with the locally commissioned IG Support Service please see 11.1		Practices as independent contractors are responsible for sourcing any legal advice they may require to support any of the above activities.	
General Data Protection Regulation (EU) 2016/679 and Data Protection Act 2018 - 1.7					
Compliance	1.7.1	There is an overarching requirement and principle that the service IT Delivery Partner across the contract (and where otherwise appropriate) will: • Ensure that they are GDPR (EU) 2016/679 and Data Protection Act 2018 compliant; • Ensure that any data processor or data controller responsibilities are fully documented and agreed with the CCG; • Assure the commissioner and provide evidence when asked that the providers and their 3rd party contractors are compliant for keeping the services provided to the commissioner GDPR and Data Protection Act 2018 compliant, included in this would be advice on what action the commissioner will need to take on services/systems to ensure compliance; • Assist the CCGs in the investigation of possible and actual	https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ https://www.igt.hscic.gov.uk/IGA.aspx		

Service Name	Service Ref	Service Description	Service Standards	Customer responsibility	Additional services not funded in main contract
		information security breaches and incidents including evidence to support post-incident reviews and actions for customer implementation. Ensure that a Data Protection Impact Assessment is undertaken covering the service provision, with outcomes and recommendations shared with the Commissioner.			
Supplier Management and Procurement Service - 2.1					
CCG and GP third party Supplier Liaison	2.1.1	Where the CCG/GP Practice /GP federation holds a contract with a third party we require the IT Delivery Partner to maintain a working relationship and support the delivery of that service where agreed. Where the CCG/GP Practice/GP federation intends to contract with a third party we require the IT Delivery Partner to engage and advise as appropriate, ensuring necessary compliance and compatibility. Develop appropriate Operational Level Agreements (OLAs) where required.	CCG Third party contracts include GPSoC suppliers, NHS Digital, NHS England, managed print service, managed telephony service, MS EWA.	Inform the IT Delivery Partner prior to agreeing a contract with any third parties to ensure compliance and compatibility.	Support for organisations other than the customer e.g. AQPs, GPSI services and other CCG commissioned and sponsored services. It is recognised that the IT Delivery Partner may charge for activities in relation to mobilisation, configuration and ongoing support.
Supplier contract third party Management / Liaison	2.1.2	Where the IT Delivery Partner has 3rd party contracts in place to support the delivery of this specification there is a requirement that appropriate OLAs exist in order to meet the agreed performance indicator. Additional service provision via the use of third parties must be agreed with the CCGs. Liability for payments associated with the suppliers 3rd party contracts are the responsibility of the IT Delivery Partner.	The IT Delivery Partner must ensure that any third parties meet the service and quality standards of the overall contract.		

Service Name	Service Ref	Service Description	Service Standards	Customer responsibility	Additional services not funded in main contract
IT Equipment / Infrastructure Procurement Service	2.1.3	Procure and order all IT equipment and software as agreed with the CCG, and in line with the current GPIT operating model and against appropriate SFI's. The IT Delivery Partner will ensure all equipment from receipt of order will be issued to the recipient within 4 weeks. The IT Delivery Partner will undertake an annual review of the IT hardware catalogue with an identified group of CCG stakeholders. The IT Delivery Partner will offer the ability to GP Practices to procure IT hardware / software - which should be available via a catalogue ordering process.	All NHS capital asset purchases NHS England procurement rules and Standing Financial Instructions (SFIs) must be applied. Where possible nationally agreed purchasing frameworks should be used to ensure efficiencies and compliance with appropriate procurement standards. All equipment should be in line with the standard hardware specification deployed to customers.		
IT Procurement Support	2.1.4	Providing advice and guidance on the procurement of new IT solutions to ensure compatibility with, and compliance to, NHS standards.	Practices and CCGs purchasing non-GPSoC clinical systems and digital technologies which include hosting patient identifiable information are responsible for ensuring compliance with the NHS Data National Security Standards		

Service Name	Service Ref	Service Description	Service Standards	Customer responsibility	Additional services not funded in main contract
			A catalogue of devices and solutions should be agreed with the CCG, and re-visited annually		
Technology Infrastructure Refresh Service - 3.1					
GP IT Hardware Refresh Service	3.1.1	Provide and deliver a refresh programme that will identify and replace GP IT hardware where it has reached its service life change date, as a minimum every 4 years, subject to NHS England guidance and funding, including assessment, rollout and disposal.	Agree (with the CCG) a desktop Warranted Environment Specification (WES) which as a minimum enables NHS applications and GPSoC clinical systems.	Allow IT Delivery Partner informatics staff reasonable access to premises.	Equipment funded out of NHS England GPIT capital
Training Service - 4.1					
Training service	4.1.1	The service should include training for: • GP System of Choice (GPSoC) core clinical systems; • National digital systems e.g. SCR, EPS2, ERS. And will include training requirements arising from: • Migration; • Mergers; • New Functionality (e.g. upgrades or new clinical systems); • Staff turnover; • Refresher training; • Support practice optimisation of principle GP clinical systems and national digital systems; • Microsoft Office Suite. Service provision must include a variety of delivery methods e.g. face-to-face, online, all of which must be efficient, costs effective and timely, and appropriately evaluated.	Trainers should have appropriate capabilities and/or be accredited by clinical system supplier Training delivery should reflect: • Practice training plans and staff training needs analysis • Virtual and online delivery channels	Training for practice purchased systems e.g. Sage Accounting, clinical devices, business administration and office systems.	Additional Service on demand

Service Name	Service Ref	Service Description	Service Standards	Customer responsibility	Additional services not funded in main contract
		Support in providing Training Needs Analysis to identify gaps in knowledge of practice staff.			
Project and Change Management Service (including National Strategic Implementation Service) - 5.1					
Project and Programme Management	5.1.1	Provide Programme and Project management resources as commissioned by the CCG to include: • Production and maintenance of programme plans and documentation including Project Initiation Document, Business Case), highlight reports, exception reports, risk and issue logs, etc.; • Change Management; • Stakeholder analysis, engagement and communication; • Working within agreed governance and accountability; • Standalone risk and issue management, using a structured risk management approach such as MoR; • Benefits using an established evaluation process; • Standalone Supplier Management/Liaison within an outsourced customer-lead project or programme to maximise IT Delivery Partner efficiency, quality and value for money. Delivery of Projects should be fulfilled, where possible, using existing resources on a service priority basis.	Projects are to be managed in a structured way using the principle of one of the following: • Managing Successful Programmes (MSP); • Portfolio, Programme and Project Offices (P3O); • PRINCE2; • Agile; • Management of Risk (MoR); • Clinical safety; • Managing Benefits; or suitable equivalent	Nomination of Senior Risk Owners and governance boards as appropriate.	Resourcing of large complex projects, will be discussed on a case by case basis
Client Relationship Management Service - 6.1					
Customer Liaison Management	6.1.1	Provision of a named senior manager as contract manager. Management of complaints and issues from customers in accordance with agreed procedure. Provision of service performance reports e.g. incident closure customer survey (quarterly reports) and customer satisfaction survey (no less than once a year), with timings to be agreed.			

Service Name	Service Ref	Service Description	Service Standards	Customer responsibility	Additional services not funded in main contract
		Support the CCG in the management and advice to practices in relation to GPIT provision and development. Including provision of best practice advice and guidance relating to all aspects of GP IT service provision and delivery.			
Locality / District / ICS / STP wide initiatives - 7.1					
Locality / District / ICS / STP wide initiatives	7.1.1	Support and assess on request additional infrastructure, Software and hardware services over and above core infrastructure. Provision, maintenance and technical support of the necessary infrastructure, software and hardware to deliver add-on services as agreed by the CCG. Examples; Systems to support Clinicians, social care, public health and patients, across a local or regional health and care system. Responsive provision to meet enhanced and transformational GPIT, NHS England and NHS Digital national and local programmes and projects: • Discharge and referral messaging systems; • Record sharing initiatives and support for service/commissioning re-design; • Systems that link in to other services (e.g. order communications, local data warehouse and patient indexes); • Additional software and operating systems to support general practice clinical system enhancements; • Linkage to regional and national systems across health and care; • Compliance testing/installation/support of additional specialist software products; • Prescribing decision support tools; • Any other strategic developments within the lifetime of the contract. NHS England capital guidance must be applied when purchasing systems and hardware devices only if NHS England capital or revenue monies were utilised.			

Service Name	Service Ref	Service Description	Service Standards	Customer responsibility	Additional services not funded in main contract
Digital Solutions / Software Developments - Web Application Support and Development	7.1.2	Develop, host, maintain and support web applications including content management systems, public and private websites. Hosting (including secure hosting), configuration and monitoring of web servers.	Compliant with current industry development standards and NHS Digital Security Standards	Administration of website content and access	
Estates Strategy Service - 8.1					
Premises IT	8.1.1	Provision of advice and guidance to support the development General Practice estate relevant to the provision of ICT services and systems. Advice, assessment and compliance and support, including deployment of IT infrastructure and Desktop kit and IT kit in CCGs and General practice estate.			
Registration Authority - 9.1					
Provision of Smartcards	9.1.1	Delivery of service including configuration, issuing and management of smartcards (provision for new starters and removal of roles for leavers). The Registration Authority (RA) Service will operate within National Guidelines and polices. The RA Service ensures users are registered to e-gif level 3 standards are given appropriate access rights for their job role for use with relevant Smartcard applications within agreed service level agreements. Assurance of GP practices' adherence to RA Policy and processes. If assurance cannot be obtained, then the issue should be escalated as appropriate.			
Maintenance of Smartcards	9.1.2	Acting within RA Guidelines Smartcard Management will include the following: • General RA Troubleshooting and call escalation; • Re-issue Smartcards, as appropriate; • Promoting self-service. Sponsors in the CCG or practice will typically perform the roles below however the IT Delivery Partner may need to provide support where			

Service Name	Service Ref	Service Description	Service Standards	Customer responsibility	Additional services not funded in main contract
		required: • Add / Remove roles; • Amending Positions; • Unlocking / Reset PIN; • Renew Certificates. Provide practices with a facility to notify the RA team when staff leave the practice or no longer require RA access, and ensure access is removed within the relevant priority for user account management (National Data Guardian standard 4 - Data Security and Protection Toolkit).			
RA Training	9.1.3	The RA Service provides end users with training in the appropriate use of their Smartcard. Training and advice is given to Sponsors dealing with RA issues on-site and in the use of CIS. Documentation is also provided to sponsors following all training.			
RA Reporting	9.1.4	The provision of audit reports to be undertaken to assure smartcard compliance and appropriate access is adhered to and Cyber Security and Data Security and Protection requirements have been met. Support for ad-hoc investigations.			
Email Service (NHS Mail) Local Organisation Administrator (LOA) - 10.1					
Provision of NHSmail accounts	10.1.1	Delivery of service in accordance with national standards and service level agreements. Provision of one NHSmail account per individual on request. Provision of shared / generic NHSmail accounts on request.	https://digital.nhs.uk/services/nhsmail/nhsmail-policies	Timely notification of starters and leavers within organisation Compliance with relevant parts of https://digital.nhs.uk/services/nhsmail/nhsmail-policies	

Service Name	Service Ref	Service Description	Service Standards	Customer responsibility	Additional services not funded in main contract
NHSmail Maintenance and support	10.1.2	The on-going maintenance of NHSmail accounts, which includes the moving and deleting of accounts, password resets and unlocking accounts. Escalate to the national NHSmail Helpdesk should it require further attention. This support includes the connection of accounts to Microsoft Outlook when connected to the core network. Provide practices with a facility to notify the IT Delivery Partner when staff leave the practice or no longer require NHS mail access, and ensure access is removed within the agreed priority for user account management (National Data Guardian Standard 4 - Data Security and Protection Toolkit) Provide support to access user account information as a result of a legal request.	https://digital.nhs.uk/services/nhsmail/nhsmail-policies	Timely notification of changes required within organisation. Where available the customer will use self-service. Compliance with relevant parts of https://digital.nhs.uk/services/nhsmail/nhsmail-policies	
Information Governance - 11.1					
Incident management & investigations	11.1.1	Delivery of IG service which includes: • Compliance advice and IG Support for General Practice; • Support practices in the reporting and management of incidents; • Liaison with practice nominated and / or CCG Data Protection Officer (DPO); • Supporting cyber related Incident management and reporting. • Provision of advice and/or support to practices on the investigation of possible information security breaches and incidents. Advising on incident assessment (dependent upon severity of incident). Advice on post-incident reviews and actions for customer implementation. • Provision of advice and/or support to the CCG on the investigation of possible information security breaches and incidents in practices. Advice on post-incident reviews and actions for customer implementation.			
IG Advice and Support	11.1.2	A review at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security. This may for example be			

Service Name	Service Ref	Service Description	Service Standards	Customer responsibility	Additional services not funded in main contract
		a facilitated workshop at CCG level which would encourage shared learning (National Data Guardian Standard 5 - Data Security and Protection Toolkit). 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. Data Protection Officer (DPO) Resource A Data Protection Officer function will be available to support General Practice, as required.. The service will include: • Access for Practices 08:00-18:30 Monday to Friday, to specialist qualified advice on GDPR matters. • Advice on compliance with GDPR obligations, including those outlined in paragraph 1 of Figure 7 in this document • Advice reflecting national guidance on GDPR compliance as it is published. The primary role of the Data Protection Officer (DPO) will ensure that practices will process the personal data of its staff, patients, providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules. Advice to support Practices compliance with the National Data Guardian eight-point data sharing opt-out model. All published CareCERT Best Practice and NHS Digital Good Practice Guides will be reviewed and where applicable incorporated into GP IT Services. The service should work closely with the commissioned GP IT Security (Cyber Security) Service.			

Service Name	Service Ref	Service Description	Service Standards	Customer responsibility	Additional services not funded in main contract
Clinical Safety Assurance - 12.1					
Clinical Safety Assurance Advice & Guidance	12.1.1	A comprehensive clinical safety assurance service, ensuring that providing the necessary advice and guidance is given relevant to national requirements for management of clinical risk in relation to the deployment and use of health software.	Clinical safety and assurance for the deployment and use of health IT systems ISB0160 Ensuring implementation of clinical safety in the production of health IT systems ISB0129.		

Appendix B - Incident and Request Prioritisation and Target Response Times Matrix

Priority Level	Incident Category	Definition	Target Response Time (see notes)	Target Fix Time (see notes)	Typical Examples (not exhaustive)
1	High Impact (Business Critical Systems / Applications - see notes)	An issue requiring immediate attention affecting a whole site/service or the loss of a business critical system / service for greater than 50% of user estate. The impact of the issue seriously affects organisational goals. Issue affects or threatens a key system or service	Less than 15 working minutes of incident / request being received.	Less than 4 hours of incident / request being received. Where it is not possible to meet the target, apply an agreed temporary solution with a timescale, agreed with the practice and CCG, for a permanent solution to be implemented	Total loss of access to business critical systems for all staff on a single site. Total loss of access to a critical system for greater than 50% of user base. IT Security incident or significant threat/near miss involving patient data. Currently active unauthorised access to clinical system. Virus attack which is compromising the integrity of an application and/or database.
2	Medium Impact (Serious Fault)	An issue requiring urgent attention affecting multiple customers at a site but not site-wide. A partial loss of a business critical system or service, including slow performance. One department or team within a site unable to connect to a business critical system or service. A business critical system or service has failed affecting a single user and no alternative is available	Less than 15 working minutes of incident / request being received.	Less than 8 hours of incident / request being received. Where it is not possible to meet the target, apply an agreed temporary solution to address essential business impact with an agreed timescale for a permanent solution to be implemented	Partial loss of access to business critical systems for between 20% and 50% of user base. For any clinical user - loss of essential clinical functions e.g. prescriptions, data entry, referrals, appointments. Network degradation - on LAN where performance of business essential systems is significantly degraded
3	Low Impact (Other faults or issues)	An unplanned interruption or reduction in the quality of an IT service to a small number of users or individual user. A non-key service is down affecting multiple users and several locations The issuing of replacement hardware	Within 24 hours of incident / request being received.	Less than 3 working days of incident / request being received. Where it is not possible to meet the target, apply an agreed temporary solution to address essential business	Loss of access to supported/warranted systems, printing facilities PC and / or printer faults resulting in impaired usage. The issuing, amending and revoking of smartcards

Priority Level	Incident Category	Definition	Target Response Time (see notes)	Target Fix Time (see notes)	Typical Examples (not exhaustive)
				impact with an agreed timescale for a permanent solution to be implemented	
4	Standard Service Request	A request from a user for a standard change	Within 24 hours of incident / request being received.	Less than 5 working days of incident / request being received.	NHSmail accounts, group permissions, supported application access accounts, network accounts (for project requests see 5) New accounts for clinical staff (i.e. GP Locums) - IT Delivery Partner to use best endeavours to provide account access as soon as possible following request.
5	Non-standard service request	A request from a user for a non-standard change. Service Requests, queries and advice	Within 5 working days of incident / request being received	By agreement with the CCG on a per incident basis	PC application incidents, nuisance value General advice and guidance Equipment and service requests New project request, training requests, office moves Quotations etc.
P	Request - Procurement	Procurement - a request from a user with delegated authority to order / request a new issue of standard hardware/software	Within 24 hours of incident / request being received.	Less than 4 weeks (28 working days) of request from a user with delegated authority, hardware / software to be issued and received by the identified user.	Issuing of new standard hardware or software, GP IT refresh excluded from
0	Unsupported systems	Unsupported systems - service request	By agreement with the CCG on a per incident basis	By agreement with the CCG on a per incident basis	3rd party systems liaison Non clinical practice systems
	Exceptional circumstances				
A	Major Impact	Priority assigned to incidents relating to major service disruption across multiple sites.	Within 1 hour of incident being received	By agreement with the CCG on a per incident basis which may extend into out of hours work, realignment of	Cyber Incident affecting multiple sites Initiation of emergency preparedness

Priority Level	Incident Category	Definition	Target Response Time (see notes)	Target Fix Time (see notes)	Typical Examples (not exhaustive)
				resources or commissioning of additional capacity. Where it is not possible to meet target in priority 1 then apply an agreed temporary solution with an agreed timescale for a permanent solution to be implemented Additional resources may, by agreement with the customer, to be allocated to the issue.	

Notes:

Business Critical Systems / Applications

1. Business Critical Systems / Applications are defined as:
   - Clinical Systems - e.g. SystmOne; EMIS
   - Access to national applications and hosted services - e.g. e-RS (e-referrals); Liferay; EPS2; SCR; Patient Online; Oracle Financials; Broadcare; NHSmail; etc.
   - Microsoft Office;
   - Microsoft Exchange Outlook (e-mail);
   - Network File and Print Services

Target Response Time / Target Fix Times

2. Target Response Time defined as the elapsed period between the user reporting the incident/request to the service desk and the commencement of investigative activity;
3. Target Fix Time defined as is the elapsed period between the user reporting the incident/request and restoration / completion of the incident / request. (Subject to 3rd party response and fix times);
4. All Target Response Times and Target Fix Times exclude travel time and delays arising from any inability to access Customer's premises. Where an activity is required to be completed by the User in order to rectify the fault, the time taken to complete this task is excluded from the measurement of the Service Level. (Subject to 3rd party response and fix times).