



## **2018/19 Addendum to the GP IT Operating Model, Securing Excellence in GP IT Services, 2016-18 (revisions)**

June 2018

To be read in conjunction with “Securing Excellence in GP IT Services: 2016/2018 Operating Model”

## NHS England INFORMATION READER BOX

### Directorate

Medical	<b>Operations and Information</b>	Specialised Commissioning
Nursing	Trans. & Corp. Ops.	Strategy & Innovation
Finance		

### Publications Gateway Reference:

08172

<b>Document Purpose</b>	Guidance
<b>Document Name</b>	2018/19 Addendum to the GP IT Operating Model, Securing Excellence in GP IT Services, 2016-18 (revisions)
<b>Author</b>	NHS England
<b>Publication Date</b>	June 2018
<b>Target Audience</b>	CCG Accountable Officers, Care Trust CEs, NHS England Regional Directors, Directors of Finance, GPs, NHS England (Finance, Commissioning Development, and Regional / DCO Leads / Informatics Heads).
<b>Additional Circulation List</b>	CSU Managing Directors, NHS Digital , Directors of Finance
<b>Description</b>	<p>This document sets out to extend the operating arrangements for the delivery of GP IT services across England until 2019. It outlines clear accountability, responsibility, financial and support arrangements for General Practice in England to receive high quality IT support services.</p> <p>NHS England will retain full accountability for GP IT and delegate the commissioning, operational and financial management responsibilities to CCGs, with the associated funding.</p> <p>NHS England will retain responsibility for certain IT services which will be directly commissioned through Regional DCO Teams.</p>
<b>Cross Reference</b>	<p>Securing Excellence in GP IT Services: Operating Model, 3rd edition (2016-18), published in April 2016.</p> <p>CCG Practice Agreement, published in March 2015.</p> <p>General Practice IT Infrastructure Specification, published 28th September 2014.</p>
<b>Superseded Docs</b> (if applicable)	N/A
<b>Action Required</b>	NHS England and CCGs to operationalise this guidance
<b>Timing / Deadlines</b> (if applicable)	N/A
<b>Contact Details for further information</b>	<p>Sue Cooke Senior Programme Lead for Digital Primary Care Quarry House Leeds LS1 7UE england.digitalprimarycare@nhs.net</p>

### Document Status

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet.

# **2018/19 Addendum to the GP IT Operating Model, Securing Excellence in GP IT Services, 2016-18 (revisions)**

Version Number:

First published: May 2016

Updated: June 2018

Prepared by: NHS England, Digital Primary Care

Classification: Official

## Contents

1	Foreword .....	5
2	The Addendum .....	6
3	Appendix 1: 2018/19 Addendum to the GP IT Operating Model, Securing Excellence in GP IT Services, 2016-18 (revisions) .....	7
3.1	Primary Care IT Enabling Services (PCES) .....	7
3.2	National Data Security Standards for Health and Social Care / Cyber Security / General Data Protection Regulations (GDPR) .....	8
3.3	Operating Systems & Software Licencing .....	12
3.4	Health & Social Care Network (HSCN) .....	14
3.5	Wi-Fi in General Practice .....	16
3.6	Online Consultation Systems Programme .....	17
3.7	SNOMED Clinical Terms (CT) in General Practice .....	18
3.8	Digital Primary Care Maturity Assurance (DPC MA) .....	20
3.9	GP IT Commissioning Specification Support Pack .....	21
3.10	New Models of Care Contracts .....	22
3.11	Capital Submissions & Treatment – GP IT & ETTF .....	23
3.12	Glossary of Terms .....	24
4	Appendix 2: Schedule of Services GP IT – Revisions .....	27
5	Appendix 3: Detailed Changes to Figures and Tables .....	32
5.1	Figure 7: Information Governance, Data & Cyber Security accountabilities and responsibilities .....	32
5.2	Figure 8: Detailed IG Responsibilities .....	37
5.3	Figure 11: Detailed responsibilities for Primary Care IT Enabling Services .....	38
6	Appendix 4: Digital Primary Care Maturity Assurance Indicators .....	40
7	Appendix 5: GP IT Commissioning Specification Support Pack .....	47

# 1 Foreword

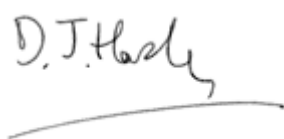
## 2018/19 Addendum to the GP IT Operating Model, Securing Excellence in GP IT Services, 2016-18 (revisions)

This document outlines revisions to the current GP IT Operating Model, [‘Securing Excellence in GP IT Services 2016-18’, 3<sup>rd</sup> Edition](#) that will help to ensure that GP IT services remain fit for purpose, flexible and responsive to developing General Practice requirements.

The arrangements outlined in the attached GP IT Operating Model Addendum 2018-19 (Appendix 1) support the aims within the current GP IT Operating Model; for increased ‘local’ flexibility and ownership that will enable commissioners to effectively respond to a rapidly changing Primary Care landscape, whilst also supporting a local collaborative approach to digital enablers that will help support delivery of the [GP Forward View](#) (GPFV) and the broader integration of health and care as part of local Integrated Care Systems and Sustainability and Transformation Partnerships (ICS/STPs).

A significant part of this addendum addresses the changes required to support General Practice with cyber and data security requirements resulting from the cyber-attack on the NHS in 2017, the new National Data Guardian (NDG) Standards and recommendations and obligations for GP contractors under the new EU General Data Protection Regulations (GDPR) due to come into force from May 2018. In addition, the GP IT Schedule of Services (Appendix Two) has been updated to reflect the [2017/18 General Medical Services Digital Guidance](#).

This addendum to the GP IT Operating Model, will take the current operating model into 2019, with a full revision of the GP IT Operating Model to be undertaken for release in 2019/20. Given the changing face of General Practice provision and contracts, the necessity to consider whole system impacts such as cyber security and with the impending expiry of the current GP Systems of Choice (GPSoc) contract, it is anticipated that the future revision will include a wider and more holistic view of digital support requirements for General Practice.



Dominic Hardy  
National Director for Primary Care Delivery



Will Smart  
Chief Information Officer for Health and Social Care

## 2 The Addendum

- With effect from March 2018 the GP IT Operating Model, 'Securing Excellence in GP IT Services 2016-18', 3<sup>rd</sup> Edition (the 2016-18 Operating Model) is amended as follows: The 2018/19 Addendum in Appendix 1 (including the GP IT Commissioning Specification Support Pack in Appendix 5) of this document is appended to the 2016-18 Operating Model
- Appendix C – Schedule of Services GP IT of the 2016-18 Operating Model is amended as set out in Appendix 2
- Figures 7, 8 and 9 in the 2016-18 Operating Model are amended as set out in Appendix 3 and a Cybersecurity flow diagram is presented
- Appendix D – Digital Primary Care Maturity Assurance Indicators of the 2016-18 Operating Model is amended as set out in Appendix 4
- The terms set out in the Glossary of Terms in section 3.12 of this document are inserted into the Glossary in Chapter 11 of the 2016-18 Operating Model, and where such terms are already included, in the 2016-18 Glossary, the terms in this document shall replace those in the 2016-18 Glossary

In the event of any conflict between the 2016-18 Operating Model and the 2018/19 Addendum, the 2018/19 Addendum shall take precedence.

### 3 Appendix 1: 2018/19 Addendum to the GP IT Operating Model, Securing Excellence in GP IT Services, 2016-18 (revisions)

#### 3.1 Primary Care IT Enabling Services (PCES)

##### Context & Rationale

This addendum outlines revised commissioning and funding provision for PCES for General Practices. Previously NHS England retained responsibility, through its regional DCO teams, for funding and directly commissioning fundamental support services for General Practice, collectively known as Primary Care IT Enabling Services (PCES) which include:

- Registration Authority support services
- Information Governance (IG) support services
- Clinical Safety Officer support
- NHS Mail administration support

The [2016-18 GP IT Operating Model](#) clarified commissioning responsibilities, to provide these services for those contractors providing essential primary care services (GP Contractors).

From 1<sup>st</sup> April 2018 commissioning responsibility for provision of PCES for General Practice, including developing requirements as outlined within this addendum, will be delegated to Clinical Commissioning Groups (CCGs), together with funding reflected in the allocation uplift. This will enable flexibility in the commissioning and provision of PCES services that meet the local needs and requirements of General Practice, ensuring critical alignment of IG support services with CCG commissioned GP IT Cyber and Data Security services, together with enabling local efficiencies through ICS/STP wide planning and commissioning arrangements.

CCGs commissioning PCES should consider support requirements for General Practice to meet the National Data Security Standards for Health and Social Care, Cyber Security recommendations and the new data protection reform i.e. the EU General Data Protection Regulation (GDPR) which will apply in the UK from 25 May 2018 and further the Data Protection Act 2018 (upon receiving Royal Assent and coming into force) which will accompany the GDPR and exercise derogations in UK law permitted by the GDPR.

For other primary care contractors, NHS England regional DCO teams will continue to assure that appropriate IT support service arrangements are in place for those contractors who have access to and use of national clinical information systems, as part of local commissioning arrangements. This includes community pharmacies, appliance contractors, dental practices, primary ophthalmic providers and primary care provided within prisons.

The commissioned PCES for General Practices must include appropriately skilled and resourced Clinical Safety Officer Support and Information Governance Support. Clinical Safety, Information Governance and Information Security risk and impact assessments should be an integral part of any clinical system deployment, reconfiguration and interfacing project.

### **Current GP IT Operating Model Reference(s)**

Reference: Section 5.5: Primary Care IT Enabling Services (PCES) (page 26)  
Section 7.3.3: Funding for Primary Care IT Enabling Services (PCES) (page 34)  
Figure 10: Key PCES accountabilities and responsibilities (page 53)

### **Timescales**

- 1 April 2018 commissioning responsibility for provision of PCES for General Practice is delegated to CCGs

### **Actions**

CCGs and NHS England regional DCO teams will need to work together to ensure the smooth and safe transition of the commissioning, procurement and provision of PCES services for General Practice.

*NB: In most cases an immediate change in provider is not anticipated in advance of current contract expiry.*

### **Funding & Commissioning Arrangements**

For 2017/18, funding and commissioning responsibility for PCES will remain with DCOs. From April 2018, PCES funding will be reflected in CCG baseline allocations.

## **3.2 National Data Security Standards for Health and Social Care / Cyber Security / General Data Protection Regulations (GDPR)**

### **Context & Rationale**

On 12 July 2017 within [‘Your Data: Better Security, Better Choice, Better Care’](#) the government accepted the ten data security standards recommended by Dame Fiona Caldicott, the National Data Guardian for Health and Care, outlined in her July 2016 report, [Review of Data Security, Consent and Opt-Outs](#).

In January 2018, the Department of Health, NHS England and NHS Improvement published the [2017/18 Data Security and Protection Requirements](#), which sets out the steps all health and care organisations will be expected to take in 2017/18 to demonstrate that they are implementing the ten data security standards recommended by the National Data Guardian, including further details on the assurance framework for 2018 onwards.

Through the Data Security Centre and the Data Security and Protection Toolkit (DSPT), NHS Digital will support organisations to put these standards into practice.

Under the [2017/18 General Medical Services Digital Guidance issued jointly by NHS England and the General Practitioners Committee \(GPC\)](#), practices are encouraged to implement the ten new data security standards in the National Data Guardian Security Review and NHS England and the GPC have agreed to jointly promote compliance.

The EU General Data Protection Regulation (GDPR) comes in to effect on 25 May 2018. It will directly apply in EU Member States (e.g. the UK) irrespective of national legislation. However, the GDPR permits Member States to derogate from the GDPR in certain areas, and a new Data Protection Act 2018 (upon receiving Royal Assent and coming into force) will replace the current Data Protection Act 1998 and accompany the GDPR to exercise



those derogations in UK law and establish continuity of the GDPR in the UK post Brexit. General Practice contractors as data controllers are required to comply with the data protection reform, i.e. GDPR and further the Data Protection Act 2018 (upon receiving Royal Assent and coming into force).

### **Current GP IT Operating Model Reference(s)**

Reference: CCG-Practice Agreement (page 15)

Section 7.9: Data Security (page 51)

Figure 7: Key Information Governance accountabilities and responsibilities

(page 48)

### **Timescales**

- By April 2018 – Replace, remove or isolate unsupported operating systems in the General Practice IT estate
- By April 2018 - Have a plan agreed and commenced to replace, remove or isolate all other unsupported software, browsers or devices in the General Practice IT estate
- April 2018 – Revised IG Toolkit, the Data Security and Protection Toolkit (DSPT) available
- 25 May 2018 – GDPR legal compliance
- By 14 January 2020 – Replace, remove or isolate all Windows 7 operating systems in the General Practice IT estate

### **Actions**

General Practices and CCGs, with the support of their locally commissioned GP IT Delivery Partner(s), should adopt the ten data security standards published by the National Data Guardian and follow the guidance from the National Cyber Security Centre, [Ten Steps to Data Security](#).

Under EU GDPR which will be directly applicable as law in the UK from 25 May 2018, it is mandatory for all public authorities (and data controllers who carry out large scale processing of health data)) to designate a named Data Protection Officer (DPO), although multiple public authorities can agree to designate a single DPO.

Public authorities will be defined within the forthcoming Data Protection Act 2018. The latest draft bill provides that General Practices will be regarded as public authorities in relation to the processing of personal data for the purposes of providing NHS primary care services. General Practices also carry out large scale processing of health data. Therefore all General Practices will require a DPO.

There are many other new requirements arising under GDPR which all data controllers must ensure compliance with from 25 May 2018, the full details of which are beyond the scope of this document. [Guidance for General Practices](#) has been published by the Information Governance Alliance. General Practices should have a plan in place to achieve and demonstrate compliance with these requirements.

As part of the 'core and mandated' IG support service (PCES) to be commissioned by CCGs from 1<sup>st</sup> April 2018, a Data Protection Officer (DPO) support function should be provided to support General Practice designated Data Protection Officers.

Locally, CCGs can negotiate an enhanced GPIT service with their GP IT Delivery Partner as a call off agreement (i.e. chargeable to practices), under the main service contract for the

provision of nominated individual(s) to practices that wish to designate a DPO from the service.

Each General 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 existing practice obligations to *identify the person with lead responsibility for IT matters in the Practice* (CCG-Practice Agreement – section 5.3). The CCG as commissioner of GP IT services will be responsible for providing specialist support to this role but each practice remains accountable. CCGs must ensure their commissioned GP IT Delivery Partner has allocated equivalent senior level responsibility for cyber and data security within their organisation.

Each General Practice is accountable for ensuring data security incidents and near misses are reported when they become aware of these, in accordance with national reporting guidance and legal requirements (NHS GP Information Governance Toolkit ref 14.1-320 and NDG Standard 6).

Specialist support for GP Cyber Security incident reporting and management with access to NHS Digital CareCERT is a required part of **core** commissioned GP IT security and information governance services.

CCGs must ensure locally commissioned GP IT delivery partner(s) register for and act on CareCERT Advisories within required timescales, with the CCG holding accountability through exception reporting. Confirmation must be given within 48 hours that plans are in place to act on any CareCERT High Severity Advisories. CCGs must ensure that their commissioned GP IT Delivery Partners register with CareCERT Collect.

CCGs must ensure that all local GP IT delivery partners have appropriate Disaster Recovery/Business Continuity arrangements in place to manage identified incidents or high severity threats.

Business Continuity arrangements for 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 within 48 hours of a cyberattack (see Section 3.3).

CCGs must ensure GP IT Delivery Partners have disaster recovery and business continuity plans in place which must be based on a Recovery Time Objective (RTO) for essential GP IT services of no more than 48 hours.

**IMPORTANT:** CCGs and GPs must ensure 'unsupported' software (by software supplier), internet browsers, operating systems or devices are not used to connect to the supported GP IT infrastructure (other than the public Wi-Fi service) or to access patient records.

Digital systems purchased by the practice or the CCG outside core and mandated GP IT arrangements and the GP Systems of Choice (GPSoc) framework, which store or process patient identifiable data or which connect to the GP IT managed infrastructure, should be reviewed for compliance with the ten NDG data security standards and applicable legal requirements (e.g. GDPR). The responsibility for this rests with the individual contract

holder ie the GP or CCG, who should liaise with the locally commissioned GP IT delivery partner, for assistance in ensuring new and existing systems are compliant.

CCGs to ensure that locally commissioned GP IT delivery providers (CSUs and others) submit plans, to NHS Digital by June 2018 for compliance with CE+ certification standard by 2021.

All parties responsible for infrastructure and systems in the GP IT estate must by April 2018 replace, remove or isolate unsupported operating systems. All parties must work together to ensure existing functionality provided by these systems necessary for the safe and effective delivery of patient services is maintained during this process.

All parties must also have a plan agreed and commenced to replace, remove or isolate all other unsupported software, browsers or devices.

CCGs should ensure that local service specifications and contracts for GP IT and PCES are reviewed and updated, agreeing Change Control Notices where required, to reflect these recommendations and guidance.

Associated changes required to the Schedule of Services for GP IT are detailed in Appendix 2.

### **Funding & Commissioning Arrangements**

IT/cyber security and GP Information Governance support services are part of 'core & mandated' GP IT requirements and should be funded through GP IT revenue.

*NB: From April 2018 PCES funding will be reflected in CCG baseline allocations (see Section 3.1).*

Funding requirements resulting from changes or upgrades needed to services and systems outside 'core and mandated' GP IT operating arrangements are the responsibility of the local 'contract holder'.

### **Assurance Arrangements**

From April 2018 the replacement for the Information Governance Toolkit (IGT), the Data Security and Protection Toolkit (DSPT) will form part of a new framework assuring organisations are implementing the ten data security standards and are meeting their statutory obligations for data protection and data security (GDPR).

GP IGT (and subsequent DSPT) data and other relevant criteria, including progress on managing unsupported software, are captured within the Digital Primary Care Maturity Assurance (DPC MA) tool which will provide insight to support local and national assurance.

### **Further information & Support**

[NHS Digital CareCERT](#)

[NHS Information Governance Toolkit](#)

EU General Data Protection Regulation: <http://eur-lex.europa.eu/>

[Information Governance Alliance GDPR advice for GPs](#)

## National Data Guardian Review

National Cyber Security Centre: <https://www.ncsc.gov.uk/>

## GMS Digital Guidance 2017-18

2017/18 Data security and protection for health and care organisations (DH, October 2017, updated January 2018):

Encryption Good Practice Guide (NHS Digital)

### **3.3 Operating Systems & Software Licencing**

#### **Context & Rationale**

As part of their delegated responsibilities to provide GP IT services, CCGs should ensure that there is continued investment in GP IT to maintain, develop and upgrade existing IT services and infrastructure. This includes desktop hardware, operating systems, browsers and software applications necessary to continue effective delivery against the requirements outlined within the GP IT Operating Model.

CCGs must ensure that desktop hardware, operating systems and applications meet locally agreed Warranted Environment Specification<sup>1</sup> (WES) requirements, which as a minimum, should meet the national WES, the relevant GP Systems of Choice (GPSoC) clinical system requirements and the GP IT Infrastructure Specification (under review). There must be effective patch, upgrade and asset management arrangements in place for operating systems and applications. The development of a local WES will identify those operating systems, browsers and software applications necessary for the safe and functional operation of the principal GPSoC clinical systems and national NHS applications used by practices locally.

#### **Actions**

All software (including operating systems) used on NHS owned GP IT infrastructure, 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 security risk. CCGs commissioning GP IT services and GPs utilising IT infrastructure must ensure that no unsupported operating systems, browsers or software are used within General Practice.

There must be the capability (or a plan and timescale to implement this capability by December 2018) for the central control of desktop security, patch control, access and software installation across the managed GP IT estate. This should include the ability to

---

<sup>1</sup> The national WES contains the technical specifications to access spine systems with a smartcard. Periodically updated by NHS Digital, it is used by GP IT system suppliers in designing systems to integrate with spine services. GP IT delivery partners use the WES to ensure that the operating systems, browsers, Java virtual machines and smartcard printer drivers deployed locally to end users are fully supported.

isolate sites and/or individual devices, where there is an identified incident or high severity threat (relevant to that site).

Where such central control is not yet fully developed/deployed, as an interim measure CCGs must ensure that all local GP IT delivery partners have appropriate Disaster Recovery/Business Continuity arrangements in place to manage identified incidents or high severity threats. Business Continuity arrangements for general practice infrastructure must include the capability to isolate affected PCs from the network within 48 hours of a cyberattack.

NB: NHS Digital is now able to offer local organisations Microsoft Windows operating system licences, including Advanced Threat Protection (ATP). This is free of charge to local NHS organisations who agree to implement the ATP facility. The ATP facility gives local organisations better cyber security protection and, since it is also linked into the NHS Digital Data Security Centre (DSC), it improves cyber security protection for local health and care communities and the NHS as a whole.

NB: Within the Transition Network and Health and Social Care Network (HSCN), the Advanced Network Monitoring and Networks Analytics Service arrangements have capability to identify and notify the NHS Digital Data Security Centre of potential security incidents. A site may be isolated from the network in the event of an incident. This would be initiated through discussion with the site's network provider and proactive communication relating to the site by the NHS Digital CareCERT team, using the contact details provided in the HSCN Connection Agreement, which CCGs as responsible commissioners of GP IT services, must sign on behalf of GPs (see Section 3.4).

Where the WES does not yet support upgraded Operating Systems, CCGs may wish to procure and deploy operating system licences with roll-back / roll-forward capability, providing that unsupported operating systems are not used. Locally commissioned GP IT delivery partners can advise on the technical aspects required for effective GP IT estate management to facilitate the necessary operating system transition requirements.

Arrangements must be in place to ensure that supported Windows operating systems are fully deployed before predecessor systems become unsupported.

NB: Microsoft extended support for Windows 7 operating system ends on the 14<sup>th</sup> January 2020. CCGs should be working with the locally commissioned GP IT delivery partner to ensure a replacement programme is in place to meet this deadline.

### **Funding & Commissioning Arrangements**

Operating system and necessary application licenses can be funded from GP IT capital where there is payment for 2 or more years and the investment complies with the wider NHS England Finance Guidance for capital accounting. Where the expense is payable annually, this can only be charged against GP IT revenue.

### **Current GP IT Operating Model Reference(s)**

Reference: Section 7.4: Capital Provision (page 34)

## **Timescales**

- By April 2018 – replace, remove or isolate unsupported operating systems in the General Practice IT estate
- By April 2018 - have a plan agreed and commenced to replace, remove or isolate all other unsupported software, browsers or devices in the General Practice IT estate
- By 30 September 2018 - capability for (or a plan and timescale to implement this capability by December 2018) central control of desktop security, patch control, access and software installation across the managed General Practice IT estate.
- By 14 January 2020 – replace, remove or isolate all Windows 7 operating systems in the General Practice IT estate

## **Further Information and Support**

For Microsoft Windows Licensing:

General Contact details and information can be found on the NHS Digital website:  
<https://digital.nhs.uk/services/data-and-cyber-security-protecting-information-and-data-in-health-and-care/microsoft-windows-operating-system-licences-including-advanced-threat-protection>

[Microsoft Windows operating system licences with Advanced Threat Protection - Service overview \(NHS Digital, May 2018\)](#)

Contacts detail for the service agreement is through the NHS Digital licensing partner Bytes ([www.bytes.co.uk/nhs](http://www.bytes.co.uk/nhs))-call 01372 418763 or email: [nhsea@bytes.co.uk](mailto:nhsea@bytes.co.uk).

## **3.4 Health & Social Care Network (HSCN)**

### **Context & Rationale**

The Health and Social Care Network (HSCN) replaced the N3 national network arrangements, which expired on 31 March 2017. The end of the N3 agreement will not have an immediate impact on the network services General Practices receive, as existing service orders will endure under N3 transition arrangements, to enable migration to replacement HSCN services.

The HSCN establishes a standards-based, multiple-supplier model for network connectivity that will enable NHS organisations to locally source network connectivity from a choice of assured HSCN compliant suppliers, using a variety of procurement routes.

This addendum outlines commissioning and funding provision for N3 transition arrangements and HSCN service provision for General Practices.

Commissioning responsibility for HSCN service provision for General Practice is delegated to CCGs, together with associated funding provision. This will enable flexibility in the commissioning and provision of HSCN services that meet local needs and requirements of General Practice and align with broader ICS/STPs.

### **Current GP IT Operating Model Reference(s)**

Reference: Section 3.4: N3/Health and Social Care Network (HSCN) – transition arrangements (page 14).

### **Actions**

CCGs must sign the HSCN Connection Agreement on behalf of GPs.

CCGs will have initiated procurement for HSCN services for their constituent General Practices, with a range of procurement options available as outlined on the NHS Digital [HSCN website](#).

The purchasing route will not affect HSCN connectivity services accessible to General Practice or the level of funding devolved to CCGs to locally commission HSCN services. However CCGs that choose to direct award HSCN contracts will be expected to be able to demonstrate compliance with Standing Financial Instructions (SFIs) and value for money in the absence of a competitive procurement process.

For all procurement options, CCGs are responsible for the contract ownership and management on behalf of General Practices.

### **Funding & Commissioning Arrangements**

From 1 April 2017 CCGs are responsible for commissioning and paying for General Practice network connectivity services as part of core and mandated GP IT operating arrangements. This includes transitional N3 connectivity and future commissioning of HSCN core services, with central funding for transitional N3 connectivity devolved to CCGs. This will ensure that network funding and commissioning arrangements for General Practice are aligned with core and mandated GP IT operating arrangements, providing the associated governance and assurance framework for GP IT investments.

As the commissioner of HSCN services for General Practice, CCGs will need to review local General Practice network requirements and consider broader ICS/STP arrangements in order to identify HSCN requirements, agree appropriate contract length and value for money investment.

### **Assurance Arrangements**

An 'HSCN Compliant' Assurance Mark has been established that enables suppliers to demonstrate compliance with nationally agreed standards to offer HSCN services to health and care organisations. Information about the supplier compliance process can be found on the [NHS Digital HSCN webpages](#), together with detail on HSCN compliant suppliers.

CCGs should include the [HSCN mandatory supplementary requirements](#) when procuring network services.

### **Transition Arrangements**

Connection Agreements: CCGs are required to sign a single [Connection Agreement](#) for services delivered to their constituent General Practices. Signing the Connection Agreement will demonstrate:



- An understanding of the data protection relationship between organisations still using legacy N3 connectivity services (Transition Network customers) or organisations who have migrated to HSCN (HSCN customers) and NHS Digital, thereby satisfying the requirement under GDPR for data controllers to have written agreements in place with data processors.
- Commitment from the customer to establish good data security.
- Readiness to connect to HSCN once HSCN connectivity services have been locally procured.

CCGs need assurance from locally commissioned GP IT delivery partners that they support the CCG (and General Practices) in delivering the above responsibilities, including adherence to appropriate information governance and IT/cyber security requirements as outlined in the GP IT Operating Model and CCG-Practice Agreement.

### **Further information & Support**

General contact details together with further information can be found on the NHS Digital HSCN website:

<https://digital.nhs.uk/health-social-care-network>

NHS Digital [HSCN Regional Migration Managers](#) (RMM) will provide ongoing support and advice on new connectivity.

HSCN enquiry mailbox for general HSCN enquiries: [enquiries@nhsdigital.nhs.uk](mailto:enquiries@nhsdigital.nhs.uk)

[Mandatory standards and HSCN Supplier Obligations](#)

## **3.5 Wi-Fi in General Practice**

### **Context & Rationale**

The General Practice Forward View (GPFV) made a commitment to provide Wi-Fi services in General Practice for staff and patients (within practice settings).

Commissioning responsibility for provision of Wi-Fi services for General Practice is delegated to CCGs, together with funding as detailed in the CCG Confirmation of Funding for Wi-Fi Services in General Practice letter circulated to CCGs in June 2017. This will enable flexibility in the commissioning and provision of Wi-Fi services that meet local needs and requirements of General Practice and can also support broader ICS/STPs.

### **Current GP IT Operating Model Reference(s)**

Reference: Appendix C, Schedule of Services:

- Wi-Fi for clinical primary care staff (page 114)
- Public Facing Wi-Fi in General Practice (page 117)

### **Timescales**

- **April 2017:** Funding made available to cover implementation and service costs.

### **Actions**

CCGs will commission Wi-Fi services for General Practices ensuring:



- National Wi-Fi security standards are met and adequate support arrangements as outlined in the [NHS Wi-Fi Technical & Security Policies and Guidelines](#) are in place. Note: these standards include a requirement that patient identifiable data can only be transmitted on the practice Wi-Fi using either “corporate user class” or “medical device” access.
- Wi-Fi service usage does not impact on core General Practice activities, in particular performance of GPSoC hosted systems and NHS national systems
- There is compliance with NHS data security & protection requirements, including appropriate content filtering.
- 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.
- Locally agreed Acceptable Use Policies, must be in place which should cover all wireless network services provided, including Guest and Bring Your Own Device arrangements.

### **Funding & Commissioning Arrangements**

Time limited national funding for Wi-Fi provision in General Practice has been delegated to CCGs, to support the implementation of a managed service, which includes initial deployment and support costs.

The continued provision of Wi-Fi services in General Practice is a ‘core & mandated’ requirement in the GP IT Operating Model, which will ensure that network funding and commissioning arrangements are aligned with GP IT operating arrangements, providing the appropriate governance and assurance framework for GP IT investments.

### **Assurance Arrangements**

The Digital Primary Care Maturity Assurance (DPC MA) tool will include indicators for Wi-Fi access within General Practice. In addition, CCGs should ensure that locally commissioned services meet the NHS published standard including usage and alert reporting.

### **Further information & Support**

General contact details together with further information can be found on the NHS Digital Wi-Fi website:

[www.digital.nhs.uk/nhs-wi-fi](http://www.digital.nhs.uk/nhs-wi-fi)

Enquiry mailbox for general Wi-Fi enquiries: [nhswifi@nhs.net](mailto:nhswifi@nhs.net)

## **3.6 Online Consultation Systems Programme**

### **Context & Rationale**

As part of the [General Practice Forward View](#) commitment a £45 million revenue fund has been established to stimulate the use of online consultation systems within General Practice aimed at improving access and making best use of clinicians’ time.

### **Current GP IT Operating Model Reference(s)**

Reference: Section 8.3: Digital Primary Care Maturity Assurance Model (page 64)

## **Actions**

Online consultation systems remain an 'enhanced GP IT service' within the GP IT Operating Model. CCGs are encouraged to utilise the Online Consultation Systems funding provision under the GPFV to support practices in the adoption of online consultation solutions to help improve efficiency and effectiveness within General Practice.

## **Funding & Commissioning Arrangements**

Funding arrangements are outlined in the GPFV Online Consultation Systems fund information ([Online Consultations Fund. Operational Information](#)) published by NHS England.

CCGs with the support and engagement of General Practices as system users (eg through LMC or other representative groups) will undertake procurement of online consultation systems on behalf of their General Practices.

A Commercial and Procurement Hub commissioned by NHS England will provide expert advice to support the local procurement of Online Consultation Systems.

In addition, a [Dynamic Purchasing System](#) (DPS) Framework has been established to provide an approved supplier list to support local procurement of online consultation systems.

## **Further information & Support**

Support arrangements, including good practice guidance on online consultation specifications together with details on the Commercial and Procurement Hub and DPS Framework, are outlined in the guidance '[Online Consultations Fund. Operational Information](#)' published by NHS England.

Further information on the DPS Framework can be found at:

<https://www.england.nhs.uk/digitaltechnology/info-revolution/digital-primary-care/commercial-procurement-hub/dynamic-purchasing-system/>

General contact details together with further information can be found on the NHS England GPFV Online Consultation Systems webpage (NHS England):

<https://www.england.nhs.uk/gp/gpfv/redesign/gpdp/consultation-systems/>

Enquiry mailbox for general Online Consultation Systems

enquiries: [england.onlineconsultations@nhs.net](mailto:england.onlineconsultations@nhs.net)

Enquiry mailbox for Commercial and Procurement HUB enquiries:

[commercial.procurementhub@nhs.net](mailto:commercial.procurementhub@nhs.net)

## **3.7 SNOMED Clinical Terms (CT) in General Practice**

### **Context & Rationale**

SNOMED CT will replace Read/CTV3 codes in General Practice; this is to align with national plans for a unified coding scheme in patient records across all health and care systems. This will enable improved and safer patient care, facilitate seamless data exchange and enhance clinical data analysis and reporting.

SNOMED CT is an international clinical terminology that provides a structured coding system to support the direct management of the health and care of an individual, enabling clinically relevant information to be consistently and reliably recorded and effectively processed by electronic clinical systems.

SNOMED CT is the only current information standard for clinical terminology as outlined in the [Information Standards Notice SCCI0034](#); [this](#) seeks to ensure its implementation aligns with national requirements in relation to electronic records.

### **Current GP IT Operating Model Reference(s)**

Reference: Appendix B, Schedule of Services – GP Data Quality Service (page 113), GP Data Quality Accreditation Service (page 114)

### **Timescales**

From 1<sup>st</sup> April 2018: SNOMED CT to be implemented within General Practice.

*NB: SNOMED CT is to be implemented in Secondary Care, Acute Care, Mental Health, Community systems and other systems used in the direct management of care of an individual by 1<sup>st</sup> April 2020, although a number of organisations already use SNOMED CT coding.*

### **Actions**

Individual General Practices remain responsible for the quality of their patient records and the application and use of clinical terminology.

As part of current 'core and mandated' GP Data Quality service requirements, CCGs are responsible for ensuring that a comprehensive support service is available to practices including training in data quality, clinical coding and information management skills. CCGs should ensure that locally commissioned GP Data Quality support services are reviewed and updated to reflect the requirements of SNOMED CT and align with associated support supplied under GPSOC arrangements.

CCGs should familiarise themselves with SNOMED CT and the support available via NHS Digital and GPSOC clinical system suppliers. CCGs should work closely with locally commissioned GP IT delivery partners and practices in order to facilitate a seamless transition to SNOMED CT for General Practice.

CCGs have provided NHS Digital with a nominated point of contact for SNOMED CT related matters and should ensure any subsequent changes are notified by emailing [snomedprimarycare@nhs.net](mailto:snomedprimarycare@nhs.net).

CCGs should ensure General Practices are fully sighted on the transition requirements, highlighting the associated benefits and signposting available support. Transition to SNOMED CT requires an initial review and risk assessment of local templates and reports, to ensure business continuity in the early stages of transition to the SNOMED CT vocabulary.

SNOMED CT provides a rich and sophisticated clinical terminology nomenclature. Once initial implementation has taken place, General Practices will require ongoing support from

GP IT delivery providers as part of 'core and mandated' data quality support services, to fully realise the benefits that can be achieved through the use of SNOMED CT. This includes regular and systematic review and risk assessment of local templates and reports, to fully utilise and gain optimum benefit from the more extensive vocabulary available within SNOMED CT.

As local NHS Commissioners, CCGs are also advised to:

- Review locally commissioned reporting/data analysis services that support clinical commissioning activity, to ensure that any associated data warehousing, extraction and/or analysis tools can accommodate SNOMED CT requirements.
- Review local formularies to ensure these accurately reflect SNOMED CT.
- Review interoperable and integrated systems which utilise existing clinical coding and ensure that these reflect SNOMED CT requirements.
- Where third party systems are in use and require upgrading to be compatible with SNOMED CT, the responsibility and cost of these upgrades will sit with the contract holder for that system. CCGs may at local discretion use ETTF or local funding streams to support these upgrades.

### **Assurance Arrangements**

The DPC Maturity Assurance model includes indicators to review:

- Provision of a GP Data Quality Service with SNOMED CT support
- Practice engagement on SNOMED CT transition

### **Further information & Support**

General contact details together with further information and resources to support the transition to SNOMED CT can be found on the NHS Digital SNOMED CT website:

<https://digital.nhs.uk/SNOMED-CT-implementation-in-primary-care>

CCG checklist is available on the NHS D SNOMED webpages:

[https://hscic.kahootz.com/gf2.ti/f/762498/30646661.2/PDF/-/SNOMED\\_CT\\_CCG\\_Checklist\\_v2.0.pdf](https://hscic.kahootz.com/gf2.ti/f/762498/30646661.2/PDF/-/SNOMED_CT_CCG_Checklist_v2.0.pdf)

SNOMED CT Implementation in Primary Care workspace:

[https://hscic.kahootz.com/connect.ti/t\\_c\\_home/view?objectId=299987&exp=e1](https://hscic.kahootz.com/connect.ti/t_c_home/view?objectId=299987&exp=e1)

Information Standards Notice SCCI0034:

<http://content.digital.nhs.uk/isce/publication/scci0034>

GPSoC Framework:

<https://digital.nhs.uk/GP-Systems-of-Choice/GPSoC-Services>

Enquiry mailbox for general SNOMED CT enquiries: [enquiries@nhsdigital.nhs.uk](mailto:enquiries@nhsdigital.nhs.uk)

## **3.8 Digital Primary Care Maturity Assurance (DPC MA)**

### **Context & Rationale**

The Digital Primary Care Maturity Assurance model was launched in May 2016 and provides a rich source of information to support assurance and provide insight to support investment in digital services in General Practice. Data is collected annually from NHS Digital systems and directly from General Practices (eDEC) and CCGs (annual CCG

questionnaire), with information available for review via the [Primary Care Web Tool \(PCWT\) portal](#).

Given the drivers of the GPFV, new contracts & models of care and emerging ICS/STPs it is vital to ensure GP IT operating arrangements demonstrate value to the system. The DPC MA model is under review to ensure it is able to support the following key requirements:

- To support local commissioners (CCGs) and NHS England in ensuring local GP IT services support GMS contractual requirements, meet NHS commitments and mandates, are safe and secure and appropriately utilise delegated GP IT funds.
- To support General Practice in improving service and organisational efficiency and effectiveness by utilising digital technology enablers. This aligns with the ambitions outlined in the GPFV.
- To support emerging ICS/STPs and new models of care based on integrated care by contributing General Practice digital datasets to wider “place based” digital maturity models.

#### **Current GP IT Operating Model Reference(s)**

Reference: Figure 15: The Digital Primary Care Maturity Assurance Model (page 65)

#### **Actions:**

All CCGs should complete the annual CCG questionnaire.

All General Practices are encouraged to complete the GP IT components, including “voluntary” questions, in the Annual Practice Declarations (eDEC), which provides essential data for the model.

#### **Further information & Support**

The list of changes made to the indicators is provided as Appendix 4 to this document.

General contact details together with further information can be found on the NHS England Digital Primary Care website:

<https://www.england.nhs.uk/digitaltechnology/info-revolution/digital-primary-care/>

Primary Care Web Tool: <https://www.primarycare.nhs.uk/>

Enquiry mailbox for general Digital Primary Care enquiries:

[england.digitalprimarycare@nhs.net](mailto:england.digitalprimarycare@nhs.net)

## **3.9 GP IT Commissioning Specification Support Pack**

### **Context & Rationale**

In May 2015 NHS England advised CCGs that, in order to secure value for money for GP IT services and minimise the risk of fragmentation, where GP IT is currently sourced from a Commissioning Support Unit (CSU), CCGs are required to re-procure the service through the Lead Provider Framework (LPF) to at least a minimum standard national specification.

A GP IT Commissioning Specification Support Pack has been developed that is intended to support ALL CCGs who are procuring GP IT services. This is designed to assist CCGs with

those specialist aspects that make up GP IT services and includes support for the development of a local specification for the tender of services. This includes a template to support the capture of key information, as part of 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 ongoing revisions to the GP IT Operating Model, including those outlined within this addendum.

Note: This must include a review of cyber & data security services.

#### **Current GP IT Operating Model Reference(s)**

Reference: Section: 7.4.2 Value For Money (page 35)

#### **Actions**

CCGs are advised to use the support pack, data collection tool and specification template in the market testing and commissioning of GP IT services.

CCGs are advised to use the support pack to review current GP IT service provision where a re-procurement is not scheduled in the near future.

#### **Further information & Support**

The support pack is provided as Appendix 5 to this document.

General contact details together with further information can be found on the NHS England Digital Primary Care website:

<https://www.england.nhs.uk/digitaltechnology/info-revolution/digital-primary-care/>

Enquiry mailbox for general Digital Primary Care enquiries:

[england.digitalprimarycare@nhs.net](mailto:england.digitalprimarycare@nhs.net)

### **3.10 New Models of Care Contracts**

#### **Context & Rationale**

Framework documents have been published for population-based care models including Multispecialty Community Providers (MCPs) and Primary and Acute Care Systems (PACS) which are based on the GP registered list. Both MCPs and PACS include primary, community, mental health and social care and apply a new model of enhanced primary and community care:

- An MCP combines the delivery of primary care and community-based health and care services – incorporating a wider range of services and specialists as appropriate locally, to achieve optimum service delivery
- In addition to this, PACS include hospital services

As MCPs and PACS become more formalised and established with funding flows, contractual and organisational structures defined, there is a need to ensure that GP IT operating arrangements continue to align with and reflect these emerging models of care.



## **Actions**

To comply with existing GMS GP IT contractual obligations. Whilst new contractual forms and service models become fully established, the scope of GP IT services provided locally should be those 'core & mandated' GP IT requirements needed to support contracted Primary Care Essential Services to a registered patient list.

## **Current GP IT Operating Model Reference(s)**

Reference: Section 3: Introduction (page 11).

## **3.11 Capital Submissions & Treatment – GP IT & ETTF**

### **Context and Rationale**

GP IT capital funds are available for CCGs to invest on behalf of NHS England in GP IT infrastructure needed to deliver 'core & mandated' GP IT services.

Estates and Technology Transformation Funds (ETTF) funds are available for CCGs to invest on behalf of NHS England in GP IT infrastructure & systems required to support 'Enhanced' and 'Transformational' GP IT. Providing these developments meet the criteria of these GP IT services as outlined in the [GP IT Operating Model](#) and comply with the NHS England Finance Guidance for capital accounting, they can be classified as GP IT capital. If these conditions are met then capital depreciation arrangements as outlined in Section 7.4.1 of the current GP IT Operating Model will apply. The NHS England Finance Guidance can be accessed via CCG, DCO and CSU Finance Teams.

*NB: Wider technology investments for non GP Primary Care or community services will be for CCG's or other local organisations eg provider organisation, to own locally.*

## **Current GP IT Operating Model Reference(s)**

Reference: Section 7.4: Capital Provision (page 34)

Section 7.6: Alternative Funding Sources (page 37)

## **Actions**

Submissions for GP IT capital and ETTF should be submitted subject to compliance with relevant SFIs and using the appropriate bid template for GP IT & ETTF < £1 million bids, ETTF £1m - £3m and >£3m bids. As a minimum the following should be provided in the submission:

- Scheme description offering clarity and understanding of the proposed investment
- Appropriate description for the strategic need of the investment
- If relevant, appropriate assurance of estates impact
- Confirmation of capital funding source and affordability
- Confirmation of accounting classification and that expenditure will be incurred within the financial year that the investment relates to
- Confirmation of revenue (including depreciation) funding source and affordability
- Appropriate description of quantitative and / or qualitative benefits associated with the investment
- Procurement plan for investment confirmed
- Confirmed support from CCG Chief Finance Officer (CFO)

The DCO Director of Finance (DoF) & Digital Technology leads will provide CCGs with advice and confirm support for submissions which meet the above criteria.

### 3.12 Glossary of Terms

Acronym	Term	Definition
	Core and mandated GP IT services	These are technologies, systems and support services required to deliver General Practice Essential Services. These are the mandatory services to be commissioned by CCGs, for GP practices as contractually required (through GMS) or as required to deliver a national NHS mandated initiative.
	Enhanced GP IT	These are technologies, systems and support services which enable and improve efficiency and effectiveness of general practice. These are discretionary GP IT services that are developed and agreed locally to support local strategic priorities and commissioning strategies to improve GP service delivery. Innovative and effective approaches that support GP Forward View and will better support changes in the delivery of primary care services, including seven day and extended hours working and 'at scale' models.
	Transformation GP IT	These are technologies, systems and support services which enable new models of care, service integration include STP led initiatives, and wider GP functions including Multi-speciality Care Providers (MCPs) and Primary and Community Care Services (PACS) organisational models. These are discretionary GP IT services that are developed and agreed locally to support local strategic initiatives and commissioning strategies to improve service delivery.
	GP IT Operating Model	The operating model sets out how we will achieve world class digital primary care systems that provide flexible, responsive and integrated services for patients, giving them greater control over their health and care. The model describes the financial operating arrangements, accountabilities, responsibilities, assurance process and leadership required to support the effective delivery of GP IT services.
	GP IT delivery partner	GP IT delivery partners are organisations commissioned by CCGs to deliver IT services for GP Practices against clearly defined service level agreements and KPIs. These will include CSUs, LPF providers, FTs, and private commercial organisations.
CareCERT	Care Computer	NHS Digital has been commissioned by the Department of Health to develop this service



Acronym	Term	Definition
	Emergency Response Team	which offers advice and guidance to support health and social care organisations to respond effectively and safely to cyber security threats
DPS	Dynamic Purchasing System	A dynamic purchasing system (DPS), established by the national Commercial and Procurement Hub, provides a compliant procurement process by which online consultation systems can be procured.
ETTF	Estates and Technology Transformation Funds	NHS England's Estates and Technology Transformation Fund (ETTF) is a multi-million pound investment (revenue and capital funding) in general practice facilities and technology across England (between 2015/16 and 2019/20).
ICS	Integrated Care Systems	A local partnership in which commissioners and NHS providers, working closely with GP networks, local councils and others, voluntarily agree to take shared responsibility (in ways that are consistent with their individual legal obligations) for how they operate their collective resources for the benefit of local populations.
GDPR	General Data Protection Regulation	This is the European Union (EU) legislation which covers data protection for individuals and which will apply from 25 May 2018. This replaces the EU's Data Protection Directive 1995.
IGT	Information Governance Toolkit	The Information Governance Toolkit is a performance tool produced by the Department of Health and now hosted by NHS Digital. It draws together the legal rules and central guidance and presents them in one place as a set of information governance requirements. From April 2018, the Data Security and Protection Toolkit (DSPT) will replace the IGT.
PCWT	Primary Care Web Tool	This is the web portal that enables access to, among others, the primary care digital maturity index data ( <a href="https://www.primarycare.nhs.uk/default.aspx">https://www.primarycare.nhs.uk/default.aspx</a> )
SNOMED CT	Systematized Nomenclature of Medicine Clinical Terms	This is a standardized, multilingual vocabulary of clinical terminology that is used by physicians and other health care providers for the electronic exchange of clinical health information.
STP	Sustainability and Transformation Partnership	STPs aim to help meet a 'triple challenge' set out in the NHS Five Year Forward View – better health, transformed quality of care delivery, and sustainable finances.
WES	Warranted Environment	The Warranted Environment Specification defines the versions of software required to be

Acronym	Term	Definition
	Specification	installed on client machines in order that they are supported by national and local providers of digital systems and services. NHS Digital publishes the national WES in order to access NHS Spine systems and applications requiring a Smartcard.

## 4 Appendix 2: Schedule of Services GP IT – Revisions

The following changes (additions) are made to the GP IT Schedule of Services (appendix C) within the GP IT Operating Model, Securing Excellence in GP IT Services, 2016-18, 3rd Edition:

Service name	Change Reason	Changes
IT Security Service	National Data Security Standards for Health and Social Care / Cyber Security EU General Data Protection Regulation (GDPR) Health & Social Care Networks (HSCN)	<p>Revision of this requirement to:</p> <p>An IT Security (Cyber Security) service will be available to all GPs encompassing all managed infrastructure and systems to ensure:</p> <ul style="list-style-type: none"> <li>• Adherence to the appropriate security guidance, including principles of information security and the 'Information Security Management: NHS Code of Practice': <ul style="list-style-type: none"> <li>NHS Digital Principles of Information Security</li> <li>NHS Codes of Practice and Legal Obligations</li> </ul> </li> <li>• Provide necessary IT security / cyber evidence to support IGT requirements for General Practice</li> <li>• Audit and investigative services</li> <li>• Specialist (IT Security) advice</li> </ul> <p>Provide a shared HSCN security contact for practices.</p> <p>Monitoring of managed infrastructure access through Active Directory to identify dormant accounts and operate a process to archive &amp; disable these. Provide practices with a facility to notify the GP IT Supplier when staff leave the practice organisation or no longer require IT access, and ensure access is removed within the performance standards for user account management (NDG Standard 4).</p> <p>A strategy for protecting GP IT systems from cyber security threats which is based on a proven cyber security framework such as Cyber Essentials (NDG Standard 9) and the advice and direction of NHS Digital CareCERT service will be developed and maintained locally. This is to be reviewed at least annually.</p> <p><u>CareCERT advisories:</u> CCGs must ensure:</p> <ol style="list-style-type: none"> <li>i. CareCERT advisories are acted on in line with suggested timescales, and evidence this through CareCERT Collect.</li> <li>ii. Confirmation is given within 48 hours that plans are in place to act on critical CareCERT advisories.</li> <li>iii. 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.</li> </ol> <p>Note: Action might include understanding that an advisory is not relevant to your organisation's systems and confirming that this is the case.</p> <p>(NDG Standard 6)</p> <p><u>IT Security Incidents:</u> Cyber-attacks against General Practice services are identified and resisted in accordance with CareCERT advisories. Action is taken immediately following a cyber incident or data breach or a near miss, with a report made to the senior management within the CCG and the practice within 12 hours of detection. Significant cyber-attacks are to be reported in line with national guidance and legal requirements immediately following detection. (NDG Standard 6).</p> <p>A cyber security flow diagram (5.4) has been added</p> <p><u>On-Site Assessments:</u></p> <p>CCGs will ensure all General Practices:</p> <ol style="list-style-type: none"> <li>I. Are registered to undertake an on-site data and cyber security assessment through NHS Digital's Data Security Assessment programme.</li> <li>II. Will undertake/fully cooperate with an on-site cyber and data security assessment if invited to do so</li> <li>III. Act on the outcome of that assessment, including implementing any recommendations where applicable to the practice</li> </ol> <p>General Practices must fully cooperate with the above assessments</p>

Service name	Change Reason	Changes
		<p>and the implementation of any recommendations. (NDG Standards 8,9)</p> <p>All shared managed infrastructure should have Communications-Electronics Security Group (CESG) approved penetration testing carried out at least annually.</p> <p>GP IT services must only be commissioned from organisations compliant with the following applicable industry standards:</p> <ul style="list-style-type: none"> <li>• ISO 27001 for Information Security Management (previously BS 7799)</li> <li>• NHS Information Governance - that demonstrates satisfactory compliance as defined in the NHS Information Governance Toolkit (version applicable to the supplier organisation type eg "Commercial Third Party", "Any Willing Provider" or "Commissioning Support Unit"). From 2018/19 this will be the Data Security and Protection Toolkit.</li> <li>• Cyber Essentials (Plus) or equivalent by 2021</li> </ul> <p>This service should work closely with the locally commissioned IG Support Service(s).</p>
Core Infrastructure Service	Health & Social Care Networks (HSCN)	<p>Additional Requirement:</p> <p>Commission local HSCN services for General Practice</p> <p>Support the safe transition of N3 services for General Practice to HSCN services by signing new connection agreements and supporting migration activities as advised by the national HSCN team.</p>
Enhanced Infrastructure Service	National Data Security Standards for Health and Social Care / Cyber Security	<p>Additional requirements:</p> <p>Bring Your Own Device (BYOD) services (for staff) in practices can only connect to the supported GP IT infrastructure using the Public Wi-Fi service and must not be used to process patient identifiable data.</p>
Local Device Maintenance and Support Service including Clinical Server Support	National Data Security Standards for Health and Social Care / Cyber Security A lessons learned review of the WannaCry Ransomware Cyber Attack	<p>Additional requirement:</p> <p>Unsupported software (by software supplier), browsers, operating systems or devices must not be used by the practice to access patient record systems (NDG Standard 8).</p> <p>The capability for (or a plan and timescale to implement this capability by December 2018) the central control of desktop security, patch control, access and software installation across the managed GP IT estate. Where such central control is not yet fully available, Business Continuity arrangements for 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 within 48 hours of a cyberattack.</p>
Remote access to the clinical system at the point of care	National Data Security Standards for Health and Social Care / Cyber Security GDPR	<p>Additional Requirement:</p> <p>Unsupported software (by software supplier), browsers, operating systems or devices must not be used by the practice to access patient record systems (NDG Standard 8).</p> <p>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.(GDPR)</p>
Remote access to the clinical systems for administrative purposes	National Data Security Standards for Health and Social Care / Cyber Security GDPR	<p>Additional Requirement:</p> <p>Unsupported software (by software supplier), browsers, operating systems or devices must not be used by the practice to access patient record systems (NDG Standard 8).</p> <p>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.(GDPR)</p>

Service name	Change Reason	Changes
Disaster Recovery and Business Continuity Support Service (part 1)	National Data Security Standards for Health and Social Care / Cyber Security	Additional Requirement: The practice business continuity plan will include continuity plans in response to threats to data security, including significant breaches or near misses. (NDG Standard 7)
Disaster Recovery and Business Continuity Support Service (part 2)	National Data Security Standards for Health and Social Care / Cyber Security	Additional Requirement: In the event of the GP IT supplier business continuity or disaster recovery plan being invoked where services relevant to General Practice are impacted the GP IT supplier will provide an initial report to the CCG within 12 hours of the invocation and a full report including root cause and remedial actions within 2 weeks of the invocation. (NDG Standard 7). These plans should be based on a Recovery Time Objective (RTO) for essential GP IT services of no more than 48 hours.  Business Continuity arrangements for 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 within 48 hours of a cyberattack.
Asset Management and Software Licencing Service	National Data Security Standards for Health and Social Care / Cyber Security	Additional Requirement:  Unsupported software (by software supplier), browsers and operating systems must not be used on managed equipment (NDG Standard 8).  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 security risk.
IT Procurement and Support Service	National Data Security Standards for Health and Social Care / Cyber Security	Additional Requirement: Practices and CCGs purchasing non-GPSoC clinical systems and digital technologies which include hosting patient identifiable information are responsible for ensuring that the hosted solution provider (as data processor): <ul style="list-style-type: none"> <li>• Can provide Information Governance assurances for their organisation via the NHS Information Governance Toolkit (or successor framework). From 2018/19 this will be the Data Security and Protection Toolkit.</li> <li>• Can confirm that the manufacturer/developer of the system has applied clinical risk management as required under SCCI0129 (Clinical Risk Management: it's Application in the Manufacture of Health IT Systems) during the development of the product procured.</li> <li>• Can confirm where the product procured is classified as a medical device the product complies with the medical device directives</li> <li>• Complies with the National Data Guardian's recommended ten Data Security Standards.</li> <li>• Can comply as a data processor with new GDPR legislation.</li> <li>• Can, if applicable, comply with national guidance on citizen identity verification, including "Patient Online Services in Primary Care - Good Practice Guidance on Identity Verification".</li> <li>• Can, if applicable, comply with the National Data Guardian eight-point data sharing opt-out model.</li> </ul> (NDG Standard 10)
Effective Commissioning of GP IT Services	GP IT Lead Provider Framework procurement support	Additional Requirements:  CCGs should use the GP IT Commissioning Specification Support Pack in the re-procurement of GP IT services and in the ongoing review of GP IT services with current GPIT suppliers.

Service name	Change Reason	Changes
		In addition to individual practice annual service reviews, where local IT and/or system performance issues are identified individual practices can request an additional service & infrastructure review (under the CCG Practice Agreement), to be triggered by a checklist based on a national template (under development) to be locally agreed with practices, CCGs and GP IT delivery partner(s).
GP Data Quality Service	SNOMED Clinical Terms (CT) in General Practice / Standards Change Notice SCCI0034 Amd 35/2016	<p>Additional Requirement:</p> <p>Locally commissioned Data Quality services should be reviewed and fully updated to reflect SNOMED CT clinical coding standards and requirements, including training and facilitation for staff and associated support materials in order to support the effective transition to SNOMED CT in General Practice.</p> <p>Following initial implementation, General Practices will require ongoing support from GP IT delivery providers as part of 'core and mandated' data quality support services, to fully realise the benefits that can be achieved through the use of SNOMED CT.</p>
Wi-Fi for Clinicians	<p>Wi-Fi in General Practice – GP Forward View</p> <p>National Data Security Standards for Health and Social Care / Cyber Security</p>	<p>Rename Service to: Wi-Fi in General Practice</p> <p>Revision of requirement to: Appropriate Wi-Fi services for General Practices ensuring:</p> <ul style="list-style-type: none"> <li>National Wi-Fi security standards (<a href="http://www.digital.nhs.uk/nhs-wi-fi">www.digital.nhs.uk/nhs-wi-fi</a>) are followed</li> <li>Adequate support arrangements as outlined in the NHS Wi-Fi Technical &amp; Security Policies and Guidelines are in place.</li> <li>Wi-Fi service usage does not impact on core General Practice activities in particular performance of GPSoC hosted systems and NHS national systems</li> <li>There is compliance with NHS data security &amp; protection requirements, including appropriate content filtering.</li> <li>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.</li> <li>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.</li> </ul>
Primary Care At-Scale	Online Consultations duplicates this requirement	<p>Remove Requirement:</p> <p>e-consultations &amp; e-triage</p>
Online Consultations	Online Consultations	<p>Additional Requirement:</p> <p>Online Consultations (enhanced GP IT)</p> <p>Description: An online consultation solution which supports registered patients and their General Practice. CCGs and practices are advised to follow the Online Consultation good practice procurement &amp; specification guidance.</p>
Patient Facing Digital Services	Wi-Fi in General Practice – GP Forward View replaces this	<p>Remove Requirement:</p> <p>Public facing Wi-Fi in GP - (managed and secured separately from any clinical Wi-Fi services and N3)</p>
Information Governance Service	National Data Security Standards for	<p>Core IG support services: Additional Requirement:</p> <p>IG advice and support</p>

Service name	Change Reason	Changes
	Health and Social Care / Cyber Security EU General Data Protection Regulation	<p>A review at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security. This may for example be a facilitated workshop at CCG level which would encourage shared learning. (NDG Standard 5).</p> <p>Advice to support General 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.</p> <p>Data Protection Officer (DPO) Support A Data Protection Officer Advice and Support function will be available to support General Practice designated Data Protection Officers. (GDPR Requirement). The service will include:</p> <ul style="list-style-type: none"> <li>• Access for General Practices during normal service hours to specialist qualified advice on GDPR matters.</li> <li>• Advice on compliance with GDPR obligations, including those outlined in paragraph 1 of Figure 7 in this document</li> <li>• Advice reflecting national guidance on GDPR compliance as it is published.</li> </ul> <p>Advice to support General Practices comply 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.</p>
Registration Authority	National Data Security Standards for Health and Social Care / Cyber Security	<p>Additional Requirement: Provide practices with a facility to notify the GP IT Delivery Partner when 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. (NDG Standard 4)</p>
NHS Mail Administration	National Data Security Standards for Health and Social Care / Cyber Security	<p>Additional Requirement: Provide practices with a facility to notify the GP IT Delivery Partner when staff leave the practice organisation or no longer require NHS Mail access, and ensure access is removed within the agreed performance standards for user account management. (NDG Standard 4)</p>

## 5 Appendix 3: Detailed Changes to Figures and Tables

### 5.1 Figure 7: Information Governance, Data & Cyber Security accountabilities and responsibilities

The following changes and additions are made to **replace** the **Figure 7 Key Information Governance, Data & Cyber Security accountabilities and responsibilities** within the GP IT Operating Model, Securing Excellence in GP IT Services, 2016-18, 3rd Edition:

*Note: References to NDG standards and GP IGT (v14.1) are shown in brackets)*

	Information Governance, Data & Cyber Security Requirements	Accountability	Responsibilities
<b>1</b>	<b>GDPR Obligations</b>		
1.1	<p>As data controllers practices must comply with data protection reform, i.e. GDPR and further the Data Protection Act 2018 (upon receiving Royal Assent and coming into force). To include:</p> <p>General Practices must designate a Data Protection Officer (DPO).</p> <p>A DPO advice and support function will be available to support General Practice designated Data Protection Officers as part of the commissioned IG support service. (GPIGT 114,115)</p> <p>Raise awareness of the GDPR with senior partners/board, staff and contractors. (GPIGT 114,115)</p> <p>Keep records of data processing activities</p> <p>Ensure there is a comprehensive understanding of the information held and how it is used. (GPIGT 316)</p> <p>Identify the legal basis for processing personal information. Document a legal basis for each processing activity identified through audit and flow mapping (GPIGT 316)</p> <p>Compliance with consent requirements – taking into account national guidance on the GDPR and consent. (NDG 8-point model)</p> <p>Comply with stringent transparency and fair processing requirements. (GPIGT 212, 213)</p> <p>Where practices offer paid for online services to any child under 13 a parent or guardian's consent in order to process their personal data lawfully is required. (Note national guidance on the applicability of this requirement).</p> <p>Practices should support individuals to exercise rights of rectification, erasure (the right to be forgotten), restriction, data portability and, objection to processing – where these apply, taking into account national guidance. (NDG 8-point data sharing opt-out model) (GPIGT 213)</p> <p>Manage subject access requests to provide individuals with access to their personal information normally within one month and at no charge. (GPIGT 213)</p> <p>Detect, report and investigate personal data breaches complying with the requirement to report specific breaches to the ICO within 72 hours of becoming aware of such a breach. (GPIGT 320)</p> <p>Data Protection Impact Assessments (DPIA) are carried out where processing is likely to result in high risk to the rights and freedoms of individuals.</p> <p>Implement data protection by design and by default. Ensure</p>	Individual Practices	<p>Individual Practices</p> <p>Multiple practices may designate a single named DPO.</p> <p>CCG commissions specialist DPO advice and support for practices as part of commissioned IG services.</p>



	Information Governance, Data & Cyber Security Requirements	Accountability	Responsibilities
	<p>all current and proposed processing activities have data protection compliant technical and organisational controls in place.</p> <p>This is not an exhaustive list of obligations arising under GDPR and General Practices, as data controllers, must ensure they achieve and can demonstrate compliance with all such requirements.</p>		
<b>2</b>	<b>N.D.G. Standards: Leadership Obligation: 1. People:</b>		
2.1	<p>Practices must have a named senior partner, board member or equivalent senior employee to be responsible for data and cyber security in the practice at partner/board level. This requirement further defines existing practice obligations to <i>identify the person with lead responsibility for IT matters in the Practice</i> (CCG-Practice Agreement - 5.3). (Standards 1,2) (IGT 114,115)</p> <p>CCGs must ensure their commissioned GP IT Delivery Partner has allocated equivalent senior level responsibility for data and cyber security within their organisation.</p> <p>CCGs, as responsible commissioners of GP IT services, should have board level awareness of cyber security, including undertaking nationally recommended cyber security training.</p>	<p>Individual practices</p> <p>CCGs</p>	<p>Individual practices or federation arrangements</p> <p>CCG as commissioner will provide specialist advice and support to this role.</p> <p>Commissioned GP IT Delivery Partner</p>
2.2	Each practice completes the GP Information Governance Toolkit v14.1 with a recommendation that practices attain level two as a minimum. From April 2018 this is replaced by the Data Security and Protection Toolkit (DSPT) to measure progress against the 10 data security standards & GDPR. (Standards 1,2)	Individual Practices	Individual Practices CCG commissions specialist advice and support service
2.3	<p>A local Information Governance advice and support service as outlined in the GP IT Commissioning Specification Support Pack.</p> <p>This will include (core)</p> <ul style="list-style-type: none"> <li>IG policy support</li> <li>IG Advice and Support</li> <li>DPO Advice and Support</li> <li>IG Training</li> <li>IG/DSP Toolkit Compliance Advice</li> <li>Incident management and investigations</li> <li>Project Support</li> </ul>	<p>NHS England/CCGs are accountable as the commissioner of GP Services to seek assurance that patient information is handled appropriately and legitimately.</p> <p>General Practices are accountable for their compliance with all necessary laws and IG standards. In part, this can be demonstrated through attaining level 2 demonstrating satisfactory compliance as defined in the NHS Information Governance Toolkit (or any successor framework). From 2018/19 this will be the Data Security and Protection Toolkit.</p>	<p>NHS England/CCGs are responsible as the commissioner of GP services to ensure GP Practices handle patient records in an appropriate manner by adhering to standards and specifications and that GPs investigate and take appropriate action relating to all serious incidents.</p> <p>Commissioned GP IG Service Delivery partner is responsible for service delivery.</p>

	Information Governance, Data & Cyber Security Requirements	Accountability	Responsibilities
		CCGs are accountable for commissioning a local IG support service (from 1 <sup>st</sup> April 2018)	
2.4	All staff must complete appropriate annual data and cyber security training. (Standard 3) (GP IGT 117)	Individual Practices	Individual Practices
<b>3</b>	<b>N.D.G. Standards: Leadership Obligation: 2. Processes:</b>		
3.1	Staff access to all systems processing patient identifiable data is regularly reviewed and updated by the practice using the NHS RA service or local practice access controls. Practices are provided with a facility to notify the GP IT Delivery Partner when staff leave the practice organisation or no longer require RA access to the practice or NHS Mail access. (Standard 4) (GPIGT 304)	Individual Practices  CCGs as Commissioner of RA & NHS Mail Admin services	Individual Practices  GP IT Delivery Partner acts on access control change requests within contracted performance standards.
3.2	GPSoc systems & National systems provide practices with facilities to identify dormant user accounts. Locally commissioned (non-GPSoc) systems processing patient identifiable data provide practice with facilities to identify dormant user accounts (Standard 4)	NHS Digital as commissioner  Individual practices or CCG as local commissioner	Individual Practices  Systems Suppliers
3.2	Practices are required to regularly review processes. As part of the local IG Support service a review at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security. This may for example be a facilitated workshop at CCG level which would encourage shared learning. (Standard 5).	Individual Practices  CCGs as commissioner of IG Services	Commissioned IG Service Delivery partner is responsible for service delivery. General Practices will fully support such process reviews and recommendations.
3.4	Acting on CareCERT advisories: Organisations must: Act on CareCERT advisories in line with suggested timescales, and evidence this through CareCERT Collect. Confirm within 48 hours that plans are in place to act on critical CareCERT advisories. Identify a primary point of contact for your organisation to receive and coordinate your organisation's response to CareCERT advisories. (Standard 6) (GPIGT 320)	CCG as commissioner	GP IT Delivery Partners
3.5	Practices report cyber and data security incidents and near misses when they become aware in line with national incident reporting guidance and legal requirements. (Standard 6) (GPIGT 320) CCGs report cyber security incidents and near misses when they become aware in line with national incident reporting guidance and legal requirements (standard 6) Practices will have access to specialist support through the commissioned GP IT services in the reporting and managing of incidents.	Individual Practices CCG as commissioner	Individual Practices CCGs The commissioned GP IT Delivery Partner(s) as provider
3.6	Each practice must maintain a business continuity plan which will include the response to data and cyber security incidents. (Standard 7) (GPIGT 319) (CCG-Practice Agreement)	Individual Practices	Individual Practices
3.7	Commissioned GP IT delivery partner(s) will be required to maintain disaster recovery and business continuity plans for services provided to General Practices which will include responses to data and cyber security incidents. (Standard 7) (GPIGT 319). These plans should be based on a Recovery	CCG as commissioner	GP IT Delivery Partners are contractually responsible for own compliance.

	Information Governance, Data & Cyber Security Requirements	Accountability	Responsibilities
	Time Objective (RTO) for essential GP IT services of no more than 48 hours.		
<b>4</b>	<b>N.D.G. Standards: Leadership Obligation: 3. Technology:</b>		
4.1	On-Site Assessments: CCGS will ensure all General Practices are registered to undertake an on-site data and cyber security assessment through NHS Digital's Data Security Assessment programme. General Practices must fully cooperate with the above assessments and the implementation of any applicable recommendations. (Standards 8,9)	CCG as commissioner	The commissioned GP IT delivery partner.  General Practices will fully cooperate with such assessments
4.2	Locally commissioned GP IT Delivery partner(s) will be contractually required to demonstrate satisfactory compliance as defined in the NHS Information Governance Toolkit current version or the Data Security and Protection Toolkit (DSPT) from April 2018, for their organisation and the services delivered under the GP IT services contract. (Standard 10)	CCG is accountable for ensuring contractually GP IT Delivery Partner is compliant All GP IT Systems and services suppliers, including GP IT Delivery Partners and GPSoC system suppliers will be accountable for their organisation GDPR compliance (including data processing obligations).	GP IT Delivery Partners are contractually responsible for compliance, including conforming to the rules around offshoring. GP IT delivery partners are responsible for ensuring their systems conform to information standards and that they are compliant with GDPR.  All GP IT Systems and services suppliers, including GP IT Delivery Partners and GPSoC system suppliers are responsible for ensuring their systems conform to information standards.
4.3	For all systems and IT Infrastructure processing patient identifiable data in General Practices the responsible IT Supplier must have the appropriate accreditation. (Standard 10)	Individual practices as data controllers  CCG as commissioner  DH as commissioner of GPSoC systems  Individual practices or other parties who commission/procure systems and IT infrastructure outside the scope of the commissioned GP	All contracted suppliers of GP IT systems, GPSoC systems, GP IT infrastructure and GP IT support services.  Practices comply with agreed action plans which meet their responsibilities described in the CCG – Practice Agreement.  Commissioners

	Information Governance, Data & Cyber Security Requirements	Accountability	Responsibilities
		IT delivery service or GPSoC and which processing person identifiable data.	and Suppliers to provide practices with assurance that this requirement has been met.

## 5.2 Figure 8: Detailed IG Responsibilities

The following **changes** are made to **Figure 8 Detailed IG Responsibilities** within the GP IT Operating Model, Securing Excellence in GP IT Services, 2016-18, 3rd Edition:

Process	NHS England and NHS Digital CareCERT	NHS England Regional DCO Teams	CCGs	Practices
<b>Reporting IG Serious Incidents Requiring Investigation (SIRIs)</b>	Set operational policies and procedures relating to SIRIs, develop SIRI reporting requirements in the IG toolkit, CareCERT and STEIS and on the governance of SIRIs.	Support practice investigation into SIRIs with advice and guidance from NHS England	Report any misuse of clinical systems in breach of local or national policy in line with national reporting guidance and legal requirements.  Report cyber incidents when aware in line with national reporting guidance and legal requirements.  Provide incident management support (through commissioned services).	Report any IG breaches and near misses, in line with national reporting guidance and legal requirements.
<b>IG/DSP Toolkit</b>	Set requirements to be included within the IG Toolkit/DSPT which is delivered by NHS Digital.	Monitor compliance with GP IG Toolkit/DSPT.	Provide compliance advice for GP IGT/DSPT.	Complete the GP view of the current IG Toolkit and demonstrate satisfactory compliance as defined in the NHS Information Governance Toolkit. From 2018/19 this will be the Data Security and Protection Toolkit.
<b>IG support services</b>	Will scope the minimum IG support services that GP practices require.		Provide IG support services for General Practice.	Uses the IG support service appropriately and follows advice provided.

## 5.3 Figure 11: Detailed responsibilities for Primary Care IT Enabling Services

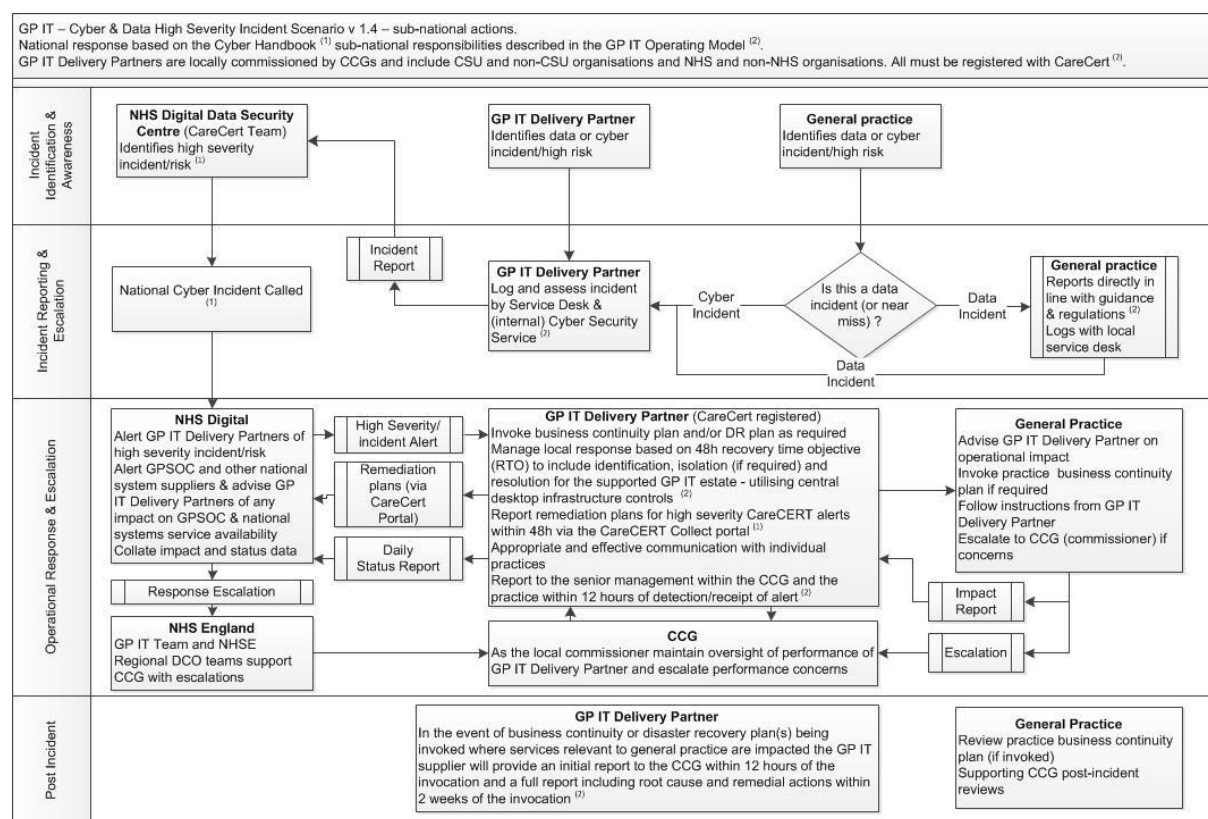
The following **changes** are made to **Figure 11 Detailed responsibilities for Primary Care IT Enabling Services** within the GP IT Operating Model, Securing Excellence in GP IT Services, 2016-18, 3rd Edition:

Process	NHS England	NHS England regional DCO teams	CCGs	NHS Digital	GP Practices	GP IT Delivery Partner
Information Governance Support Service	The Data Sharing and Privacy Unit is responsible for developing IG guidance (including GDPR compliance) in collaboration with the Information Governance Alliance.	Assures that other primary care contractors (not GPs) who have access to and are using national clinical IT systems have made adequate provision to meet the requirements for IG, IGT/DSPT, GDPR and NDG Standards.	Provides an IG service (to include Data Protection Officer (DPO) Support Service) in line with operating guidance and standards for contractors (GPs) providing primary care essential services to a registered patient list.	Maintains the Information Governance Toolkit. From 2018/19 this will be the Data Security and Protection Toolkit.	As a Data Controller complies with GDPR. Designates named DPO (multiple practices may designate a single DPO).  Completion of GP Information Governance Toolkit / DSPT from April 2018. Report incidents in line with national guidance and legal requirements.	Delivery of IG service which includes DPO support, IG Toolkit/DSPT compliance advice and IG Support and Advice for General Practice to minimum specification compliant with core IG requirements. Support practices in the reporting and management of incidents.
Registration Authorities (RA) service	Provides strategic leadership for the local operating model and service level agreement to ensure NHS England is achieving best value for money.	Assures that other primary care contractors (not GPs) who have access to and are using national clinical IT systems have made adequate provision to meet the requirements for RA Services.	Provides the service in line with national standards and sets service level agreements for an RA service for all contractors (GPs) providing primary care essential services to a registered patient list.	Sets standards for suppliers, including the RA service schedule. Maintains and publishes RA policy and process guidance. Maintains and publishes the National Role Based Access Control Database (NRD).	Adherence to NHS Digital RA policies and process guidance. GP practices approve the issue, revocation and management of smartcards for any access by individuals working in their practice to the clinical system.	Delivery of service including configuration, issuing and management of smartcards. Adherence to NHS Digital RA policy. Maintain local RA policy and processes aligned to NHS Digital RA policy and process guidance.  Assurance of GP practices' adherence to RA Policy and processes. If assurance cannot be obtained, then the issue is

Process	NHS England	NHS England regional DCO teams	CCGs	NHS Digital	GP Practices	GP IT Delivery Partner
						passed to the NHS England to resolve.
NHSmal administration and support service	Provides strategic leadership for the local operating model and service level agreement to ensure NHS England is achieving best value for money.	Assures that other primary care contractors (not GPs) who have access to and are using national clinical IT systems have made adequate provision to meet the requirements for NHS Mail Support..	Provides the service in line with national standards and sets service level agreements for an NHS Mail Admin service for all contractors (GPs) providing primary care essential services to a registered patient list. Authorises IT delivery partner to manage on its behalf.	Sets standards for suppliers.	Use of NHSmal service in line with IT security policies.  Use of NHS Mail as the primary email system for the practice.	Delivery of service in accordance with national standards and service level agreements.
Clinical safety assurance service	Sets the standards and the assurance process for local commissioners .	Assures that other primary care contractors (not GPs) who have access to and are using national clinical IT systems have made adequate provision to meet the requirements for Clinical Safety.	Provides the clinical safety and assurance service required to comply with SCCI0160 for all contractors (GPs) providing primary care essential services to a registered patient list.	Responsible for ensuring clinical system supplier (GPSOC & National Systems) compliance with SCCI0129 for manufacturing of health IT systems (or MHRA registration for clinical systems classified as medical devices). Includes any incorporated third party products.	Responsible for compliance with SCCI0160 governing implementation and safe use of health IT systems.	Delivery of clinical safety assurance service. If assurance cannot be obtained, then the issue is passed to NHS England to resolve. Compliance with SCCI0160 governing implementation and safe use of health IT systems for core and mandated GP IT, enhanced and transformational primary care IT services.

## Cybersecurity Incident Flow Diagram

The following additional figure is added



## 6 Appendix 4: Digital Primary Care Maturity Assurance Indicators

The following revised table replaces Appendix 4: Digital Primary Care Maturity Assurance Indicators within the GP IT Operating Model, Securing Excellence in GP IT Services, 2016-18, 3rd Edition:

New DMA Ref	Old DMA Ref*	Status**	Digital Primary Care Maturity Indicator	Digital Primary Care Maturity Assurance Level	Reference (where appropriate)
IND3.0	3	Change Source (2017)	Enriched Summary Care Records	Enhanced GP IT	
IND5.0	5	Retired	GPSOC accredited principal computer system	Core GP IT & Centrally Mandated Requirements	GP IT operating model CCG-Practice Agreement GMS contract



New DMA Ref	Old DMA Ref*	Status**	Digital Primary Care Maturity Indicator	Digital Primary Care Maturity Assurance Level	Reference (where appropriate)
IND17.0	17	Retired	Practice uses GP2GP to transfer records	Core GP IT & Centrally Mandated Requirements	GMS contract
IND18.0	18	Retired	Integrate GP2GP records within 3 days	Core GP IT & Centrally Mandated Requirements	GPSOC contract
IND19.0	19	Retired	Summary Care Record Uploads	Core GP IT & Centrally Mandated Requirements	GMS Contract
IND23.0	23	Retired-updated	Patients can view test results online	Enhanced GP IT	
IND27.0	27	Retired-updated	Patients can view GP Letters online	Enhanced GP IT	
IND43.0	43	Retired	The practice has a protocol to allow patients access to their records on request	Core GP IT & Centrally Mandated Requirements	( Data Protection Act 1998 and GMS Schedule 6 Part 9,PMS Schedule 5 part 9)
IND44.0	44	Retired	The practice has a designated individual responsible for confidentiality of personal data	Core GP IT & Centrally Mandated Requirements	(GMS Schedule 6 Part 5,PMS Schedule 5 part 5)
IND45.0	45	Retired-updated	Patients offered online access to detailed (coded) medical record.	Core GP IT & Centrally Mandated Requirements	GMS Contract
IND45.1	45	Update	Practice System able to support patient online access to detailed (coded) record.	Core GP IT & Centrally Mandated Requirements	GMS Contract
IND45.2	45	Update	At least 10% Patients registered for patient online access to detailed (coded) record.	Enhanced GP IT	
IND45.3	45	Update	At least 20% Patients registered for patient online access to detailed (coded) record.	Enhanced GP IT	

<b>New DMA Ref</b>	<b>Old DMA Ref*</b>	<b>Status**</b>	<b>Digital Primary Care Maturity Indicator</b>	<b>Digital Primary Care Maturity Assurance Level</b>	<b>Reference (where appropriate)</b>
IND48.1	48	Retired-updated	Local acute trust discharge letters/summaries received by practice electronically	Core GP IT & Centrally Mandated Requirements	NHS Standard provider contract Everyone Counts: Planning for Patients 2014/15 to 2018/19
IND48.3	48	Update	Local acute trust inpatient discharge letters/summaries received by practice electronically	Core GP IT & Centrally Mandated Requirements	NHS Standard provider contract Everyone Counts: Planning for Patients 2014/15 to 2018/19
IND48.4	48	Update	Local acute trust outpatient discharge letters/summaries received by practice electronically	Core GP IT & Centrally Mandated Requirements	NHS Standard provider contract Everyone Counts: Planning for Patients 2014/15 to 2018/19
IND52.1	52	Retired-updated	Patients can book appointments online.	Core GP IT & Centrally Mandated Requirements	GMS Contract (GMS Schedule 6, part 5, new paragraph 74C, PMS Schedule 5, part 5, paragraph 70D)
IND52.2	52	Update	Practice system able to support patients book/cancel appointments online.	Core GP IT & Centrally Mandated Requirements	GMS Contract (GMS Schedule 6, part 5, new paragraph 74C, PMS Schedule 5, part 5, paragraph 70D)

New DMA Ref	Old DMA Ref*	Status**	Digital Primary Care Maturity Indicator	Digital Primary Care Maturity Assurance Level	Reference (where appropriate)
IND52.3	52	Update	At least 10% Patients registered for patient online access appointment booking	Enhanced GP IT	GMS Contract (GMS Schedule 6, part 5, new paragraph 74C, PMS Schedule 5, part 5, paragraph 70D)
IND52.4	52	Update	At least 20% Patients registered for patient online access appointment booking	Enhanced GP IT	
IND56.0	56	Retired	At least 80% of elective referrals are made using the NHS E-referral system	Core GP IT & Centrally Mandated Requirements	GMS contract 2015/16 review letter
IND61.0	61	Retired-updated	WiFi for GPs and practice staff	Enhanced GP IT	
IND65.0	65	Retired	The practice is registered under the Data Protection Act	Core GP IT & Centrally Mandated Requirements	(GMS Schedule 6 Part 9,PMS Schedule 5 part 9)
IND88.1	88	Retired-updated	The practice promotes and offers e-consultations for Practice patients	Enhanced GP IT	
IND88.10	88	Update	The practice promotes and offers telephone consultations for Nursing Homes	Enhanced GP IT	
IND88.11	88	Update	The practice promotes and offers online consultations for Nursing Homes	Enhanced GP IT	
IND88.12	88	Update	The practice promotes and offers email consultations for Residential Homes	Enhanced GP IT	
IND88.13	88	Update	The practice promotes and offers video consultations for Residential Homes	Enhanced GP IT	
IND88.14	88	Update	The practice promotes and offers telephone consultations for Residential Homes	Enhanced GP IT	
IND88.15	88	Update	The practice promotes and offers online consultations for Residential Homes	Enhanced GP IT	

<b>New DMA Ref</b>	<b>Old DMA Ref*</b>	<b>Status**</b>	<b>Digital Primary Care Maturity Indicator</b>	<b>Digital Primary Care Maturity Assurance Level</b>	<b>Reference (where appropriate)</b>
IND88.2	88	Retired-updated	The practice promotes and offers e-consultations for nursing homes	Enhanced GP IT	
IND88.3	88	Retired-updated	The practice promotes and offers e-consultations for residential homes	Enhanced GP IT	
IND88.4	88	Update	The practice promotes and offers email consultations for Practice patients	Enhanced GP IT	
IND88.5	88	Update	The practice promotes and offers video consultations for Practice patients	Enhanced GP IT	
IND88.6	88	Update	The practice promotes and offers telephone consultations for Practice patients	Enhanced GP IT	
IND88.7	88	Update	The practice promotes and offers online consultations for Practice patients	Enhanced GP IT	
IND88.8	88	Update	The practice promotes and offers email consultations for Nursing Homes	Enhanced GP IT	
IND88.9	88	Update	The practice promotes and offers video consultations for Nursing Homes	Enhanced GP IT	
IND92.0	92	Retired-updated	Patients can order repeat prescriptions online.	Core GP IT & Centrally Mandated Requirements	GMS Contract
IND92.1	92	Update	Practice system able to support patient online ordering repeat prescriptions.	Core GP IT & Centrally Mandated Requirements	GMS Contract (GMS Schedule 6, part 5, new paragraph 74C, PMS Schedule 5, part 5, paragraph 70D)
IND92.2	92	Update	At least 10% Patients registered for patient online repeat prescription ordering.	Enhanced GP IT	GMS Contract (GMS Schedule 6, part 5, new paragraph 74C, PMS Schedule 5, part 5, paragraph 70D)

New DMA Ref	Old DMA Ref*	Status**	Digital Primary Care Maturity Indicator	Digital Primary Care Maturity Assurance Level	Reference (where appropriate)
IND92.3	92	Update	At least 20% Patients registered for patient online repeat prescription ordering.	Enhanced GP IT	
IND163.0	163	Retired	GPIT commissioned services service specification	Core GP IT & Centrally Mandated Requirements	GP-IT operating model CCG- Practice agreement
IND169.0	169	Retired-updated	10% of registered patients to be using one or more online service	Core GP IT & Centrally Mandated Requirements	
IND170.0	170	Retired	80% repeat prescriptions transmitted using EPS	Core GP IT & Centrally Mandated Requirements	
IND171.0	171	Update	WiFi services for GP staff, Guests and Public use	Core GP IT & Centrally Mandated Requirements	NHS England letter June 2017
IND172.0	172	New	Assurance on critical CareCERT recommendations	Core GP IT & Centrally Mandated Requirements	National Data Guardian Standards 2017
IND173.0	173	New	Regular review of cyber security measures with GPIT delivery partner(s)	Core GP IT & Centrally Mandated Requirements	National Data Guardian Standards 2017
IND174.0	174	New	Governance for GPIT with STP/ICS/ACO models	Transformation	
IND175.0	175	New	The Practice has been approached regarding the use of SNOMED-CT and is engaged in the process	Core GP IT & Centrally Mandated Requirements	2017-18 GMS Digital Guidance
IND176.0	176	New	As the commissioner of GP IT services, the CCG ensures that the GP IT delivery partner(s) and the GP work together to remove, replace or mitigate and actively manage the risks associated with unsupported systems.	Core GP IT & Centrally Mandated Requirements	National Data Guardian Standards 2017
IND177.0	177	New	Snomed CT Support as part of Data Quality Service	Core GP IT & Centrally Mandated Requirements	SCCI Notice SCCI0034

<b>New DMA Ref</b>	<b>Old DMA Ref*</b>	<b>Status**</b>	<b>Digital Primary Care Maturity Indicator</b>	<b>Digital Primary Care Maturity Assurance Level</b>	<b>Reference (where appropriate)</b>
IND178.0	178	Update	Plan for 20% Patient access to their online record	Core GP IT & Centrally Mandated Requirements	2017-18 GMS Digital Guidance

\*From GP IT Operating Model 3<sup>rd</sup> ed 2016-18

\*\*"New"-no comparable indicator from GP IT Operating Model 3<sup>rd</sup> ed 2016-18, "Retired-Updated"-the old indicator number is retired but an updated indicator is introduced, "Update"-a previous indicator is refreshed, "Retired"-indicator is no longer in use. Note: Some of the indicators rely on published datasets whose presentation may be subject to change.

## **7 Appendix 5: GP IT Commissioning Specification 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 revisions to the GP IT Operating Model outlined within this addendum.

The pack (this appendix) consists of two separate documents

1. GPIT Specification Support Pack v2.3.docx
2. GPIT Data Capture Service Schedule v2.3.xlsm \*

(\* note this is a macro enabled excel spreadsheet)