Software risk Management in GP practices

February 2025

Joining the dots across health and care

The purpose of this paper

Context

This is one of two discovery projects commissioned by NHSE SE Region to help understand the potential of automation in primary care to respond to escalating costs and increasing demands that are putting pressure on primary care systems to meet ever more complex healthcare needs and support safe working.

This project focuses on Software risk management. In most places, information governance (IG) and clinical safety (CS) are the responsibility of individual GP practices. Practices should understand and risk assess processes and have documentation to demonstrate the steps they have taken to protect their patients and their information and have met their legal requirements. Many of these activities require specialised skillsets to assess and therefore there are a range of services outlined who can provide such support to GP Practices. Ultimately, however, the GP practice will hold the IG and CS risk and must balance the risk pointed out by these specialists against the potential benefits to patients of deploying new technologies.

Objectives of the work

1. Outline existing, and additional, support for ICBs and practices seeking to deploy new software.
2. Better define the roles and responsibilities at national, regional, system and provider levels for effective improvement.
3. Improve transparency over software in use versus levels of assurance and educate GP practices on their accountabilities.
4. Improve support currently commissioned to help GP practices meet responsibilities through reducing bureaucracy and streamlining processes.
5. Develop checklist / toolkit of National requirements to adhere to e.g. DCB0160 Clinical Risk Management: Data controller applying GDPR etc. to help support practices to better understand implications when integrating a new tool into general practice.

Note that for objectives 3&4, this discovery work will propose improvements, actioning changes to the system is beyond the scope.

Caveats

1. This work was conducted as a rapid discovery piece with limited timeframe and budget. The baselining effort consequently focused on SCW services as the majority provider of GPIT service delivery for the South East Region and with easier access to individuals within the organisation.
2. This is a rapidly changing landscape and while every effort has been made to represent the facts fairly, we are already aware of planned changes so this report may quickly fall out of date and require updating.

SCW response

SCW are ourselves the majority provider for most of the relevant services described in this report, we are keen to respond to issues raised and opportunities for improvement and have included a short term response at the end of this document with a commitment to a formal response by February 2025

The Benefits of getting this right (improving software compliance and compliance processes for GP practices)

- Reduced clinical safety risk
- Reduced information governance risk
  - Reduced risk of inappropriate disclosure of patient data
  - Reduced risk of cyber security incident that might affect business continuity
  - Improved confidence, acceptance and adoption of digital solutions
- Faster deployment times for new technology
  - Improve digital maturity
  - Increased innovation in the market
  - Improve benefits realisation for available software e.g. productivity/efficiency
- Reduced admin time for practices
  - Reduced burden of CS and IG assurance
  - Reduced need for local IT interventions (e.g. less time installing/reinstalling software)
- Improved value for money from expenditure on software
  - Software licenses not in use can be decommissioned
  - Greater transparency over software assets could lead to greater utilisation

While not a benefit per se, IG is regulated by Information Commissioner's Office (ICO) and digital clinical safety falls into the Care Quality Commission (CQC)'s remit so compliance will also mitigate risk of regulatory action

Roles and responsibilities

Body	Responsibilities
NHS England national	• Maintaining national standards – DTAC (Digital Technology and Assessment Criteria) and DSP Toolkit (Data Security and Protection) • Publishing and updating GPIT Operating model – this is a commissioning framework for a range of services provided to GP Practices (but not a detailed specification that could be used as the basis for a provider contract) • Delivery of Digital Services to GP practices - delegated to ICBs through the GPIT operating model
NHS England Regions	• NHS England is currently exploring a role for assurance over ICB commissioning of the GPIT operating model
ICBs	• Responsible for ensuring availability and procurement of digital services in line with the GPIT Operating model and receive funding specifically intended to meet these statutory responsibilities for core requirements • Responsible for health and care services for the population more generally as a commissioner
GP practices	• GP Practice may commission hardware/software independently however through GPIT practice agreements, GP practices are responsible for notifying the ICB of any additional hardware/software in use not supplied by the ICB • GP Practices retain risk as data controllers and for clinical safety and need to comply with data protection legislation and the Health and Care act 2012 respectively • GP Practices are subject to regulation by Information Commissioners office (ICO) and CQC who will regulate for data protection and safety respectively
Service Providers (IT, IG and CS) e.g. SCW	• Delivering services in line with Service specifications, Service level agreements and agreed Key Performance indicators (KPIs) • Complying with data protection legislation where relevant

Accountability/responsibility for different tasks is ambiguous. We suggest that ICBs should clarify expectations locally (example below)

There are references to accountability/responsibility in national documentation, however, there is no single source of clarity on all tasks. We propose that this is necessary to tightly manage end to end software deployment. ICBs may make local decisions about service levels and therefore we recommend that ICBs review this and embed it within local ICB-practice agreements

A = Accountable, R = Responsible, R^{SP} = Responsible for managing service provider to do this - = No accountability/responsibility ? = ambiguous

Service	Task (for a specific software deployment)	ICB led procurement		Practice led procurement	
		ICB	Practice	ICB	Practice
Information governance	Commissioning of IG support service	A/R	-	A/R	-
	Creation/sourcing of DPIA/DPA documentation	A/R	-	-	A/R
	Data Protection Officer (DPO) review of documentation	A/R^{SP}	-	A[1]/R^{SP}	A[1]
	Practice review and sign off of documentation	R	A/R	-	A/R
Clinical Safety	Commissioning of Clinical assurance service	A/R	-	A/R	-
	Creation/sourcing of practice level DCB0160	A/R	-	-	A/R
	Clinical Safety Officer (CSO) review of documentation	A/R^{SP}	-	?	A/?
	Practice review and sign off of documentation	R	A/R	-	A/R
	Actioning practice level mitigations	-	A/R	-	A/R
IT	Commissioning of Core IT service	A/R	-	A/R	-
	Notifying ICB of intention to install new software in line with ICB – Practice agreement	-	-	-	A/R
	Notifying IT service of new software to commence cyber security and support level assessment	A/R	-	-	A/R
	Completion of cyber security and support level assessment	A/R^{SP}	-	A/R^{SP}	-
Contracting	Sourcing appropriate contract	A/R	-	-	A/R
	Review and sign off of contract	A/R	-	-	A/R

[1] This is an area of overlapping accountability – ICBs are accountable to provide a DPO service through GPIT model, practices are accountable through law to have a DPO

Software deployment process practice checklist

Important guidance

- *Ideally risk assessment and compliance is undertaken DURING purchase of a solution to ensure that a non-compliant solution is not purchased*
- *This checklist should be followed even where products are offered free of charge - it is always good practice to shop around and nothing is truly free in the long term, either charges will come once you are reliant on a product, or you may be paying for it with access to your patient data!*
- *The process to be followed is the same for the first installation of a new product, or installation of a product already in use. However, in the latter there will be example template documents e.g. DPIAs that can be used/modified - First installations will require more initial work to create documents and support services may have no prior knowledge of the product*

Steps (*documentation required covered in more detail on next slide*)

1. **Outline requirement** – Describe what you are trying to achieve in terms of product or service, what benefits you are looking to realise, how you would assess quality and desired balance between quality and price (e.g. 60/40 quality/price weighting)
2. **Identify procurement route** e.g. Direct award or buying through a commercial framework.

   GP Practices often don't use commercial frameworks, but these usually give access to a template contract – the alternative is usually a contract written by a supplier which may not provide the same level of protection. NB. Many frameworks charge a small amount for use, often cheaper than legal advice to review a contract or in the event something happens.

   To find available commercial frameworks, contact your ICB who will have knowledge and tools for this (you can also search yourself at find-tender.service.gov.uk)
3. **Longlist, shortlist and evaluate suppliers** based on requirements. Longlisting lists available suppliers, shortlisting may involve eliminating based on pass/fail tests, evaluation should assess quality and price and check supplier accreditations
4. **Commence compliance risk assessment of preferred solution**, *these five processes should be initiated and commenced in parallel*
   a) Request DTAC (Digital Technology Assessment Criteria) from supplier - this contains several documents from the supplier which can be used across all other risk assessments
   b) Information governance risk assessment (where relevant). Contact your local IG consultant/DPO (Data Protection Officer) for support, practices will need to find existing templates or write a DPIA (Data Protection Impact Assessment) and DPA (Data Processing Agreement) before signing these – *IG risk assessment is to ensure compliance with data protection laws, demonstrate that protection of individual's data has been considered and that a proportionate approach has been taken to mitigation of any risks*
   c) Clinical safety assessment (where relevant). Contact your local Clinical safety assurance function, practices will need to complete and sign DCB0160 (Clinical risk management standard) form, if solution is medical device, need to ensure it has CE mark and registered with MHRA (Medicines & Healthcare Products Regulation Agency) – *Clinical safety assessment is a requirement of the health and social care act 2012 and ensures that services continue to be safe for patients which is regulated by the CQC*
   d) IT provider risk assessment. Contact local IT service provider, as process will vary
   e) Seek permission from the ICB to install a solution following the locally agreed process as described in your GPIT Operating model practice agreement
5. **Purchase completed** through signature of contracts, inserting a break clause after 6 months is good practice and allows flexibility to exit a contract without financial penalty if not satisfied with product/service
6. **Standing IG documentation updated** – Update ROPA (Record of Processing Activities) and Privacy notice (these are both elements of the Data Security & Protection toolkit which must be completed annually in any case)
7. **Deployment and implementation**. You may be able to access support with this either from the supplier, the ICB or potentially through national support offers (if any)
8. **Periodic review**. Most of the compliance documents should contain a review date that should be diarised

Documentation list and actions

🟪 Legal requirement
🟩 Other requirement

Document name	When required?	Purpose of document	Actions required by GP Practices
🟩 DTAC (Digital Technology Assessment Criteria)	All Digital health technology	Supplier provides evidence of meeting clinical safety and IG (inc cyber security) standards. This includes DCB0129 which is a supplier assessment of clinical safety	Request DTAC from supplier, send to IG, CS, and IT
🟪 DCB0160 Clinical safety standard	Clinical solutions	Ensure application of effective clinical risk management by healthcare provider organisations using the software (*Note: NHS England has started a review of digital clinical standards DCB0129 and DCB0160 to ensure they remain up-to-date, practical and aligned with the latest advancements in healthcare technology and clinical practice.*	*Template document may already exist, ask supplier and Clinical Safety Officer (CSO)* identifying hazards and risk mitigation considerations (at individual GP practice level)
🟪 Data Processing Impact Assessment (DPIA)	Data processing solutions	For the controller (Practice) to demonstrate that where data is to be processed, it has met the legal requirements applicable to the processing activity and has reduced risk as far as possible.	*Template document may already exist, ask supplier and Data Protection Officer (DPO)* Data controller should review and pass to DPO for review, then sign if agree with impact assessment.
🟪 Data Processing Agreement (DPA) –If required (check with DPO if unsure)	Data processing solutions	Define in a legally binding contract the arrangements between controller (Practice) and processor (supplier) for the processing of data and assurance to the controller that the processor is sufficiently competent to comply with the law.	*Template document may already exist, ask supplier and DPO* Assuming this reflects the DPIA and this has been reviewed and signed, this document should then be signed by the data controller
🟪 ROPA (Record of processing activities) and Privacy notice	Data processing solutions	Clear record of all data processing by the organisation. This forms part of the Data Security and Protection (DSP) Toolkit that all organisations must complete annually	Update ROPA and privacy notices to reflect change in data processing (advice can be provided by IG consultant/ DPO)
🟩 Local IT provider documentation	All software	Understand: • Implications for infrastructure: Compatibility/ burden/ cybersecurity risk (crossover with IG) • Any support requirements • Level of business continuity	Complete any elements needed by healthcare provider Pass documentation to supplier for any supplier elements

This is a core set of documents and is not exhaustive, further documents may be necessary locally

Service baseline – GPIT operating model

ICB	Core GPIT	GPIG services		Clinical safety Assurance	GPIT training
		DPO	IG		
BOB	SCW	SCW	SCW	Limited service*	SCW
Frimley: E&W Berks	SCW	SCW	SCW	Limited service*	SCW
Frimley: SH, NEHF	TTP	SCW	SCW	Limited service*	SCW
HIOW	TTP	AGEM	AGEM	Limited service*	AGEM
Kent & Medway	SCW	In-house	In-house	Limited service*	SCW
Surrey	SCW	In-house	SCW	Limited service*	SCW
Sussex	SCW	SCW	SCW	Limited service*	SCW

*This has been assumed. SCW does not supply an ongoing service that would meet the clinical safety assurance guidance and support specification as laid out in the GPIT Operating Model service standard (support is provided on a consultancy basis). The discovery project has highlighted that none of the ICB's has an in house service that they advertise to their GP practices that would provide the full level of support for all software implementations across the entire GP estate. However we are aware of at least one ICB planning to increase the level of service

*GP practices who are independently procuring a software product may be required to buy in a Clinical safety assurance service if the ICB are not able to provide it

GP Practice baseline metrics of interest

	Software estate[1]		Information governance (activity) 23/24		
ICB	**Number of Unique Software names[2]**	**Local RBAC/ administrator rights position[3]**	**DSP Toolkit compliance**	**Number of DPIAs reviewed[4]**	**Number of incident responses[5]**
BOB	3,286	Local RBAC remains	100%	71	28
Frimley	3,408	Local RBAC remains, removal project commenced	100%	32	36
HIOW	Not held by SCW	Not held by SCW	Not held by SCW	Not held by SCW	Not held by SCW
Kent & Medway	2,527	Local RBAC being removed scheduled to finish **August 2025**	Not held by SCW	Not held by SCW	Not held by SCW
Surrey	2,488	Local (RBAC) remains	100%	Not held by SCW	Not held by SCW
Sussex	2,127	Local RBAC removed from **November 2021**	100%	114	31

1. As well as identifying local RBAC/ admin rights remaining, gaps in capability that are known to affect SCW provided services (all ICBs other than HIOW) are lack of control over user installed software and lack of inspection of uploaded data through web browsers.
2. Unique software names have not been cleansed, some manufacturers include patch numbers, dates etc. which likely cause duplicates and overstate this position. At present SCW do not have access to a tool which would provide a level of automated identification of commercially available software in each ICB.
3. Local RBAC means that individual practices may have administrator rights so they could bypass technical assessment by the IT provider.
4. Data Protection Impact Assessments (DPIAs) are fluid documents which can often require lengthy back and forth conversations between the IG team and the practice in order to ensure the information they contain is accurate and informative.
5. A proportion of these incidents will be recommended to be reported to ICO.

Medium to long term potential opportunities for improvement

Most of these opportunities would need to be explored jointly between commissioners (ICBs) and service providers. Many would benefit from ICBs working together collectively defining once for all solutions where possible.

Improving transparency	• Ensure KPIs, reporting and technical assessment cover all software installed on the GP practice estate in line with GPIT Operating model. This will likely require new software identification capabilities and addressing a backlog of unassessed software. • Proactively address current gaps in application monitoring and control capability, namely removal of local RBAC rights, control over user installed software and inspection of uploaded data through web browsers. • Document end to end deployment process and update regularly as improvements are made. • Extend reporting to GP practices to facilitate transparency of services. As well as improving understanding of compliance position, this may prompt consideration of use of software licenses leading to return of unused licenses and a financial saving as well as improved utilisation of retained licenses. • Explore potential to build “Compliance mesh” to support GP practices, this could be a software system that pulled a list of software in use in each GP practice to allow them to use this information to populate an information asset register. Then a documentation management solution could be used for IG and CS documentation that could link to the information asset register.
Ensuring sufficient support is in place	• Conduct an independent review of the GPIT operating model and service specification against user needs and/or user research. This could include benchmarking against other industries. • Explore commissioning of Clinical safety assurance advice and support service in line with GPIT Operating model. • Uplift KPIs to move toward customer service output and outcome measures for areas where there are currently activity and input KPIs.
Streamlining processes	• A sufficiently robust process that would facilitate systematic join up and hand off between teams including between different providers likely needs to be supported by a Kanban board (i.e. all software currently being worked on by different teams is represented and moved through the process). The design process for this may also identify gaps and duplication. This should ensure the different processes for deployment are commenced in parallel, deployment times are reduced, and transparency is improved. • Single user portal for GP practices for all business services received. • Link CS, IG and IT training potentially in the same platform. Potentially also link this to statutory and mandatory training. • Self serve software installation should be explored. • Build libraries of draft compliance documentation for different suppliers and solutions. • Explore using AI to produce first draft documentation where no existing template documentation exists. • Explore rationalisation of existing compliance documentation to reduce burden of periodic review.

SCW response to this work

SCW are ourselves the majority provider for most of the relevant services described in this report, we are keen to respond to issues raised and opportunities for improvement.

Short term changes
At no extra cost to customers, we commit to making the following changes:

1. Onboarding IG team to our Topdesk solution, this will include:
   - Tracking handling of all customer requests
   - Building workflows that robustly will link IG and IT from a deployment perspective
   - Creation of new KPIs and flow of KPIs through into the existing ICB reports that currently cover IT

   We expect this process to take approximately 6-9 months in full
2. Exploring third party access to Topdesk (or equivalent alternative solution)
   - We already have some customers with a level of access to Topdesk, we will explore technical and internal IG feasibility of opening this up to third parties for use in tracking software deployment

   If found to be feasible, this process would follow the onboarding of our own IG team
3. Providing access to ICB KPI reporting to NHSE Regions
   - We will seek permission from individual ICBs as a matter of courtesy
   - Some reports that include personal data will be excluded due to information governance

   We expect this process to take approximately 2-4 months, assuming that permission is provided

Full response

- Many of the potential issues/opportunities require development of options and estimation of cost before decisions can be made
- Our approach internally to ensure effective prioritisation of resources is to translate this document into a risk log with mitigating actions and then choose priority work areas to be developed and costed. We will consider the option of mobilising a programme of work specifically to address the findings
- Simon Sturgeon our Chief Digital Information Officer has taken executive ownership of this work

We will commit to providing a formal response by the end of February 2025. It is unlikely full costing of all mitigations will be complete at this point

Appendix 1 – GPIT Operating model v6 requirements (relevant services)

Joining the dots across health and care

Software license Management – P88, GPIT Operating model v6

Requirement	All software and operating systems installed and operated on managed GP IT equipment will be licensed and managed.
Transactional Support Services	Availability: Standard Service Hours • In compliance with the ICB GP IT Asset Management Policy: ○ allocation and control of available licences ○ procurement of additional licences ○ maintain licence register • in compliance with the ICB-Practice Agreement support the conditions on the use of Third Party Software including assessing practice requests to use Third Party Software
Specialist Support Services	Availability: Standard Service Hours • support the ICB in the development of the ICB GP IT Asset Management Policy and the ICB GP IT Warranted Environment Specification (WES-GP) and their assurance • specialist support for Windows 10 & 11 and MDE deployments
Systems and applications	• All software (including operating systems) used on Managed GP IT Infrastructure must be approved and recorded on a software licence register which must confirm that the software is appropriately and legally licenced for such use and does not present a cyber security risk. • compliance with the ICB GP IT Asset Management Policy • compliance with the ICB GP IT Warranted Environment Specification (WES-GP) • Microsoft 365 will be provided on NHS owned devices through Collaboration Licences held by the ICB.
Practice Responsibilities	The individual practice is responsible for: • compliance with ICB-Practice Agreement on use of Third Party Software requesting permission to use third party applications on Managed GP IT Infrastructure

Clinical Safety Assurance specification (1/2)- P125-6

Requirement	• Clinical safety assurance advice and support. Note this includes patient safety matters where the use of digital systems by the practice are concerned.
Out of scope	• The responsibility and burden of effort for Clinical Safety Assessment and assurance under DCB0129 rests with the system developer. This includes any third party software incorporated into the system. However when procuring digital services assurances should be secured from system suppliers that this standard, if applicable has been met. • Legal advice
Specialist Support Services	Availability - Standard Service Hours • Ensuring that the necessary standards are met for management of clinical risk in relation to the deployment and use of health software. • All practices should register with the Medicines and Healthcare products Regulatory Agency (MHRA) Central Alerting System (CAS) for both email and mobile phone text alerts. This is a web-based national cascading system for issuing patient safety alerts, important public health messages and other safety critical information and guidance to the NHS and others. **Advice and Supporting Assurance** Advise on compliance with: • Clinical Risk Management: Its application in the manufacture of health software DCB0129 as part of procurement activities • Clinical Risk Management: Its application in the deployment and use of health IT systems DCB0160 (where required): during clinical system deployment or significant reconfiguration and in business as usual activities. • Medical Device Requirements where a system/software (or part of it) is classified as a medical device **Incident Management** Supporting and advising practices in the identification of and response to digital related Patient Safety Incidents. Supporting practices reporting Patient Safety Incidents in line with national guidance through the Learn From Patient Safety Events Service (LFPSE) provided by NHS England.

Clinical Safety Assurance specification (2/2)- P125-6

Specialist Support Services

Supporting Projects & Clinical System Deployments

Advice for practices and the appointed project teams on Clinical Safety (DCB0160) where projects involve:

- change of practice Foundation Solution including data migration activities
- new initiatives involving clinical systems to support different or innovating ways of working
- reconfiguring clinical systems with the potential to bypass or deviate from internal system controls and safeguards
- new clinical systems integrating with the Foundation Solution
- decommissioning clinical systems e.g. when merging or closing practices
- deploying new digital technologies
- clinical system procurement including third party assurance

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

Support for projects beyond general advice for example preparing Clinical Risk Management Plan, Clinical Safety Case Records and Hazard Reports and supporting procurement activities should be resourced as part of the project plan.

Supporting Local Procurement

The use of the Digital Technology Assurance Criteria (DTAC) may be helpful in local procurement activities

Where ICBs or individual practices procure clinical software or medical devices which interact with the clinical software and patient record from routes other than the DSIC Catalogue assurances should be sought that the supplier has applied if applicable to the product current medical device regulations: Medical Devices (Amendment etc.) (EU Exit) Regulations 2020: and the Medicines and Medical Devices Act 2021. Users of such software and medical devices should follow manufacturer's instruction for use (IFU). Any change of use needs to be properly assured with the manufacturer's knowledge/permission as any "off label" use will mean that the user has taken on the responsibilities/liabilities of the manufacturer/developer.

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

Information governance support specification (1/3) - P120-1

Transactional Support Services	Availability: Standard Service Hours **Personal Data Breaches - Advice** A Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. Breach reporting is mandatory for all organisations. All health and care organisations, regardless of whether they are in scope of the NIS Regulations, are required to report GDPR breaches through the DSPT. This includes breaches relating to network and information systems. A network and information systems incident that disrupts the delivery of health and care, or compromises the confidentiality of health and care data, is likely to risk the rights and freedoms of individuals. Such incidents should be reported through the DSPT in line with UK-GDPR requirements even where there is not a requirement to report the incident under the NIS Regulations. Any data breach (or near miss) of practice patient personal information will require actions by one or more of the following: • the individual practice - as data controller • national NHS commissioned suppliers of GP digital services as data processor(s) • local ICB commissioned GP IT Delivery Partner - as data processor AND as specialist support service to practice • local health and social care providers where data has been shared - as data processors • any digital services supplier commissioned by the practice – as data processor • any Practice sub-contractor – as data processor ICBs will ensure practices are supported with: the provision of advice and/or support to practices on the investigation of possible information security breaches and incidents • advice on personal data breach assessment, management and reporting in line with national guidance via the incident reporting tool within the DSPT • advice on post-incident reviews and recommended actions or practice implementation • to lead or direct data breach reviews and investigations where highly specialist knowledge is required or complex multi–party issues are involved ICBs will require commissioned GP IT Delivery Partners as data processors where the breach involves data processing activities for which the GP IT Delivery Partner is responsible to take action immediately following identification of a data breach or a near miss, alerting promptly the practice as data controller and with a report made to the senior management within the ICB and the practice within 12 (working) hours of detection provide a lessons learned report (with relevant action plan as appropriate) to the ICB within 2 weeks of the recorded resolution of the incident on the service desk

Information governance support specification (2/3) - P121-2

Specialist Support Services	Availability: Standard Service Hours **IG policy support** Support for the production and maintenance of local information governance policies and procedures for practices. Provision of advice and support to practices on approval, ratification and adoption of the policies for their organisation. **Support for DSPT compliance** Provide advice and guidance to practices on how to complete the DSPT, including the collection and collation of evidence in support of DSPT submissions and resolving failure to meet DSPT standards. Provide practices with evidence required for DSPT where this is held by the ICB or its commissioned GP IT Delivery Partner(s). **IG consultancy and support** Provision of advice, guidance and support on IG related issues, including existing operational processes and procedures or new business initiatives. Advice and guidance on personal data access (but not extending to legal advice). **IG advice and Data Protection Officer (DPO) Support** Provision of advice, guidance and support on IG related issues including existing operational processes and procedures or new business initiatives to support practice designated Data Protection Officers including existing operational processes and procedures or new business initiatives. To include: • specialist advice on UK GDPR matters and compliance • advice to support practices develop and maintain best practice processes that comply with national guidance on citizen identity verification, including “Patient Online Services in Primary Care – Good Practice Guidance on Identity Verification”, that underpins the delivery of Patient Online Solutions, and assurance requirements as these are developed • advice to support practices achieve mandatory compliance with the National Data Opt-Out policy

Information governance support specification (3/3) - P122-3

Specialist Support Services

DPO Function
Availability of a named DPO, in addition to DPO support and advice for practices to designate as their Data Protection Officer. As data controllers and public authorities are legally required to designate a DPO. Practices may choose to make their own DPO arrangements, but ICBs are not expected to fund these if a DPO service has been offered by the ICB.

Reviews
Support practices & their DPO to review at least annually to identify and improve processes which have caused breaches or near misses, or which force authorised users to use workarounds which compromise data security. This may for example be a facilitated workshop at ICB level which would encourage shared learning.

Supporting Projects
Advice for practices and the appointed project teams on IG/DSP, data sharing, Data Protection Impact Assessment (DPIA) completion and cyber security considerations where projects involve:

- change of Foundation Solution for the practice (including data migration activities)
- new initiatives involving sharing patient data with third parties
- merging practices
- closing practices
- significant estate developments and new builds
- deployment of new technologies

This is not an exclusive list. Specialist support for projects beyond general advice for example preparing Data Privacy Impact Assessments should be resourced as part of the project plan.

Data Processing Activities
Data processing activities using general practice controlled personal data carried out by local ICB commissioned data processors will be identified and recorded in a data processing agreement in accordance with the digital services acquired and will be regularly reviewed.

Supporting local procurement
The use of the Digital Technology Assurance Criteria (DTAC) may be helpful in local procurement activities

Extract from template Practice agreement v3 2023

4.10 The Practice shall notify the ICB of any software and/or hardware used by the Practice, that is installed or operated on the Managed GP IT Infrastructure, but which has not been provided by the ICB. Where so notified by the Practice, the ICB may acting reasonably at its discretion decide to:

4.10.1 provide service desk support for that software and/or hardware and include this provision in the Summary of Services;

4.10.2 approve the use of the software and/or hardware but not provide service desk support;

4.10.3 prohibit the use of the software and/or hardware where there is a cyber security, data security, clinical safety or infrastructure/system performance risk to the Services provided by the ICB; or e products and services of the suppliers pursuant to the GP IT Futures Catalogue and GP IT Futures Framework including Foundation Solutions and Other Solutions.

4.10.4 prohibit the use of the software if the Practice does not have a valid licence or other required consent to operate the software

4.11 Neither party shall allow any unsupported computer operating systems, browsers or software to be installed or connected to the Managed GP IT Infrastructure.

4.12 Where, as part of the Services provided to the Practice the ICB has provided IT infrastructure for public direct use e.g. via the use of public wifi in any Supported Premises the Practice may use these services for its Practice and Practice's staff use. Such use can occur without prior agreement from the ICB, provided that the Practice ensures it and its Practice staff comply with the required conditions for use of public access to such services.

4.13 Subject to clause 4.10 the Practice shall not install any hardware or software or make changes to any hardware or software configuration that is installed or operated on the Managed GP IT Infrastructure under this Agreement unless agreed by the ICB, such agreement not to be unreasonably withheld.

4.14 The ICB shall maintain a list of software and hardware (which can be made available on request) that may be installed or operated on the Managed GP IT Infrastructure in the Practice.

4.15 The Practice shall seek the ICB's permission to participate in any testing or pilot activity which involves changes to the software or hardware configuration in the Practice, such permission not to be unreasonably withheld.

4.16 The Practice shall comply with the constraints imposed by the ICB pursuant to clauses 4.8 to 4.15 failing which, the ICB shall have no responsibility for any failure or degradation of system functionality or performance in this respect which has a business impact.

4.17 The Practice shall bear the costs (including remedial work) resulting from a failure or degradation in functionality or performance of the Managed GP IT Infrastructure relating to installing or operating software or hardware that is not approved by the ICB.

4.18 The parties acknowledge that:

4.18.1 NHS England, through its role for the DSIC Catalogue of Frameworks (or successor) (for example setting and assuring against Standards), does not assume any risk of the failure or suitability of the products and services available via the DSIC Catalogue of Frameworks (or successor), including Foundation Solutions and other Services; and

4.18.2 Clinicians at each Practice must use their own professional judgement with regards to the results generated by the products and services of the suppliers pursuant to the DSIC Catalogue of Frameworks (or successor), including Foundation Solutions and other Services

Appendix 2 – Work of interest

Joining the dots across health and care

Collection of recent difficult software deployments supplied by commissioners – timescales are notably very long

Software deployment including compliance is not currently being measured and managed as a full end to end process which is likely resulting in excessively long deployment times. Commissioners need KPIs for different service providers that enable them to effectively manage each step of the pathway as well as transparency over all steps in all deployments. This could enable the deployment process to be shortened considerably

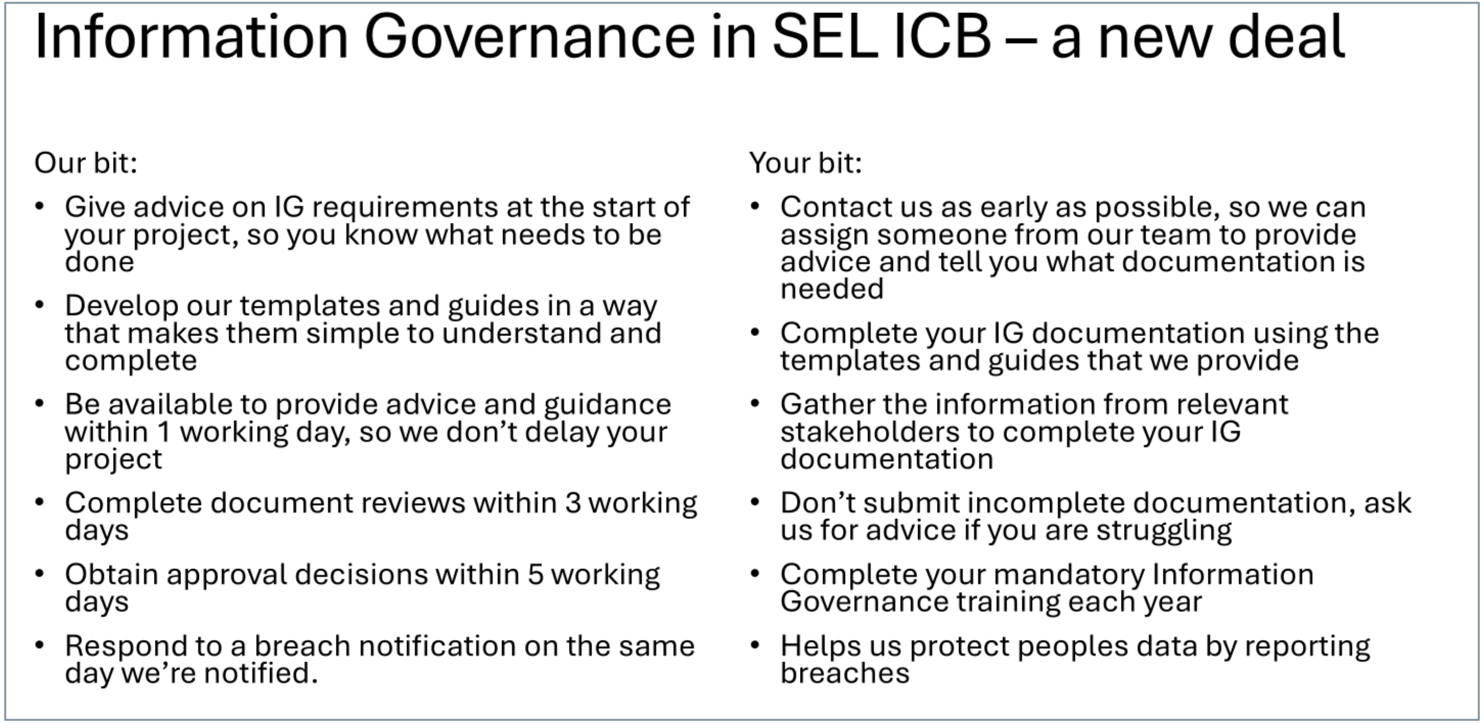
The examples below have been reviewed and processes adjusted accordingly in some instances, but this does not yet amount to provision of full transparency with appropriate KPIs

Name of Software solution	Where?	Process failures from customer perspective	End to end timescale of deployment[1]
Ardens Manager	Surrey	No DPIA template for a product already in place in >30 practices	(done in house in Sussex)
Titan PMR	Surrey	"New product" but already in place in SCW patch	>12 months
Tortus	Sussex		>9 months
JiffJaff MybotGP	Surrey	IG occurred without timely handoff to ICB or IT	>9 months

[1] This can include delays from all parties including service providers, ICBs, GP practices and suppliers. This simply serves to demonstrate the difficulty in deploying software that can potentially bring great benefits to systems and patients

Example of setting the “rules of engagement” with users for the process of deployment (IG focused but could be expanded)

- This is an example of comms produced by a London ICB for practices to support with the assurance process
- Notably there are customer facing KPIs embedded in this slide that would assist with measurement and understanding of timeframes for end to end software deployment



Information Governance in SEL ICB – a new deal

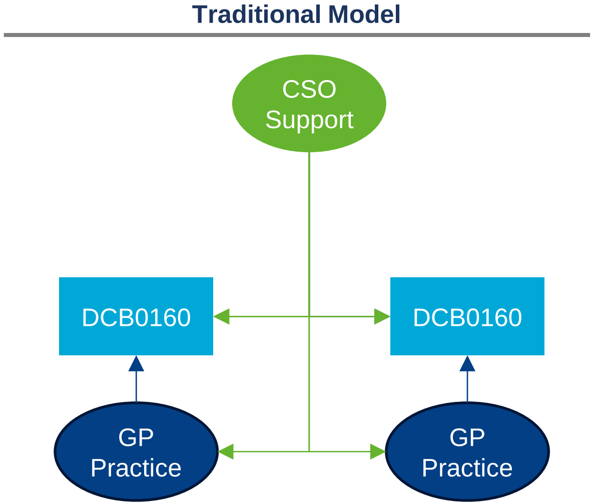
Our bit:

- Give advice on IG requirements at the start of your project, so you know what needs to be done
- Develop our templates and guides in a way that makes them simple to understand and complete
- Be available to provide advice and guidance within 1 working day, so we don’t delay your project
- Complete document reviews within 3 working days
- Obtain approval decisions within 5 working days
- Respond to a breach notification on the same day we’re notified.

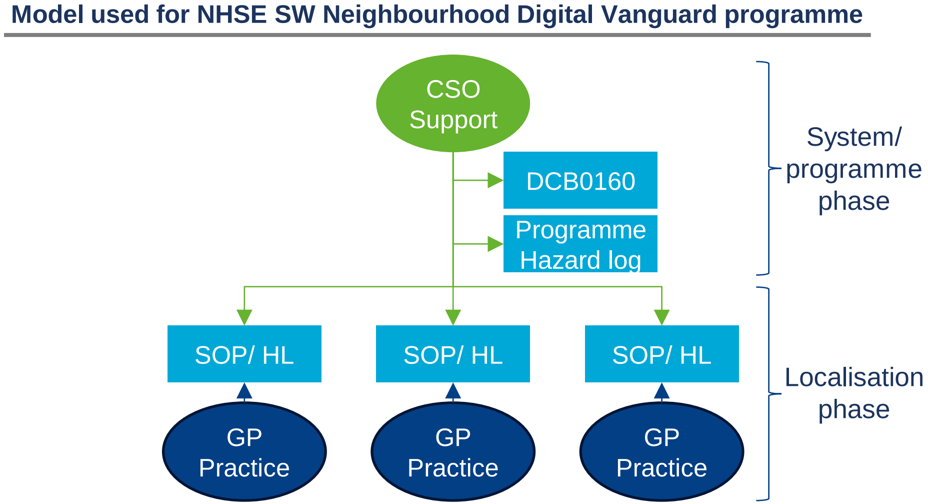
Your bit:

- Contact us as early as possible, so we can assign someone from our team to provide advice and tell you what documentation is needed
- Complete your IG documentation using the templates and guides that we provide
- Gather the information from relevant stakeholders to complete your IG documentation
- Don’t submit incomplete documentation, ask us for advice if you are struggling
- Complete your mandatory Information Governance training each year
- Helps us protect peoples data by reporting breaches

Example of Digital Clinical Safety at scale



Duplicative, expensive



This model requires MoUs to be put in place between the CSO function and GP practices. The DCB0160 is held at programme level with a programme level hazard log. Then each practice completes a standard operating procedure and localises the programme hazard log describing how they will use the software and any local mitigations to hazards that they will put in place. This reduces duplication of activities between practices