

Preparing for the General Data Protection Regulation (GDPR)

The Information Commissioners office (ICO) has produced a 12 point guide to complying with the regulation.

While compliance may seem daunting much of the work described in the guide has already been carried out as part of your obligations within the NHS, particularly your obligations within the IG Toolkit.

This document will go through the 12 preparation points one by one to give a current appraisal of where your Practice is likely to be at the moment.

Further guidance will be provided as further clarification becomes available from the Information Governance Association, the Information Commissioners Office and the Government.

The contract that is in place between NHS England and CSUs is to provide IG Support at a specific level to Independent Contractors. It does not include specific support for the implementation of GDPR.

SCW CSU would be happy to provide a service catalogue which would offer additional levels of support to individual GP practices at an agreed additional cost.



1. **Awareness - PARTIALLY COMPLIANT**

A GDPR communication was included in the recent Wire newsletter to make you aware of the regulation change. Further communications will be coming out from SCW providing additional GDPR updates. This document is to help you raise awareness with the practice partners/senior managers that this is happening.

GDPR affects all parts of the public and private sector. As a data controller, your practice will be accountable under GDPR and you will need to be able to evidence compliance.

*Further action: Discuss GDPR with your Caldicott Guardian and add to the agenda of your next Practice Senior Managers meeting to ensure that decision makers and key people in your organisation are aware that the law is changing to the GDPR.*

1. **Information you hold - PARTIALLY COMPLIANT**

As part of completing the IG toolkit your practice is obliged to compile an asset register and complete a list of data flows. The asset register details where data is held and who takes responsibility for it. The data flows should detail where data is coming from / going to and will also now need to reflect the legal basis for sharing and details of the data processor.

*Further action: Asset register and data flows should be reviewed to ensure that these are both up to date (SCW will provide guidance on how to do this).*

1. **Communicating Privacy Information – PARTIALLY COMPLIANT**

Your practice already publishes a Fair Processing Notice/Privacy Notice which details what your organisation does with the personal data it holds.

This may need to be “tweaked” to ensure it remains compliant.

*Further action: Review and update your Privacy Notice (SCW will provide an updated template). Ensure it is readily assessable to patients (e.g. from the homepage of your practice website and via reception)*

1. **Individuals’ rights - PARTIALLY COMPLIANT**

Individuals’ rights are generally covered already as part of the present Data Protection regime.

Consent, the new “right to be forgotten”[[1]](#footnote-1) and data portability[[2]](#footnote-2) may be an issue and may have to be factored in.

*Further Action: Further guidance regarding consent, the* “*right to be forgotten” and data portability is awaited. Areas where consent is used for processing need to be identified and checked to see whether they remain compliant.*

1. **Subject Access Requests - PARTIALLY COMPLIANT**

Subject Access Requests (SAR) will now have to be completed within one month, a reduction from the current 40 days. It is anticipated that the current requirement for the NHS to respond within 21 days will remain. More information will have to be provided to an individual about why their information is being processed. No charge can be levied for a standard request. However you may charge a ‘reasonable fee’ to cover administration costs if a request is ‘manifestly unfounded or excessive’.[[3]](#footnote-3)

*Further action: Review and update your SAR processes /procedures and your Privacy Notice.*

1. **Lawful basis for processing personal data- PARTIALLY COMPLIANT**

There should be a lawful basis identified for all data processing and this should be added to your privacy notice to explain it.

This again is already largely done. Your Practice has a privacy notice which should identify the legal basis for any data flow.

*Further action: Review the data flows in your privacy notice and update where required*

1. **Consent – PARTIALLY COMPLIANT**

There is a greater emphasis on the unambiguous methods of gaining consent from individuals. Under GDPR, consent will need to be explicit. The methods of seeking, obtaining and recording consent should be checked to see if they meet the new standards. This will include reviewing and refreshing all forms used by your Practice where required to ensure the validity of consent.

*Further action: An audit should be undertaken to ensure areas of consent are identified and refreshed where required.*

1. **Children – PARTIALLY COMPLIANT**

There is an increased focus on the processing of children’s data.  The use of data from people who do not have the capacity toconsent is very important.

Your Practice should look at how consent is obtained from a parent or guardian and how you apply the Fraser guidelines/Gillick competence.

Your Practice is already well aware of its responsibilities in this area.

*Further action: You should identify and review procedures to ensure consent is properly obtained for processing children’s data.  You should also review and update your privacy notice if required.*

1. **Data Breaches - PARTIALLY COMPLIANT**

Your practice should already have robust incident reporting procedures in operation. All staff should know how to report a data breach. Under GDPR all personal data breaches must be reported to the ICO through the IG Toolkit incident reporting tool within 72 hours.

*Further action: Ensure you have the right procedures in place to detect, report and investigate a personal data breach. Ensure staff know who to report a data breach to.*

1. **Data Protection by design and data protection impact assessments – PARTIALLY COMPLIANT**

Both these elements are designed to show that you have thought about data protection whenever you start a new project, take on a new supplier or change existing work practices.

Currently your practice is required to carry out a risk assessment before introducing a new system or supplier. GDPR requires the completion of Data Protection Impact Assessments (DPIAs) to anticipate and address the likely impact of a new initiative on an individuals’ privacy. Further advice should be sought from the ICO[[4]](#footnote-4) where processing is considered ‘high risk’. SCW is collaborating with NHSE to develop a national DPIA template.

*Further action: Introduce use of DPIAs for any new activities initiated by your practice[[5]](#footnote-5) that involve processing or sharing patient information.*

1. **Data Protection Officer – PARTIALLY COMPLIANT**

Public Authorities and organisations that carry out large scale processing are required to appoint a designated Data Protection Officer (DPO) who has a good understanding of the organisation’s business and how it processes personal data. This role may be shared by multiple organisations depending on their organisational structure and size and must be undertaken by an individual where there is no conflict of interest. Further clarification is awaited on what this means for GP practices.

All organisations need someone who takes responsibility for data protection matters, even if they are not formally required to designate a DPO.

*Further action: Identify who takes responsibility for data protection in your Practice. This could be your IG Lead or IT Manager. Await further guidance regarding the requirement to designate a DPO.*

1. **International - PARTIALLY COMPLIANT**

This may impact on your Practice if any data is processed outside of the European Economic Area (EEA).

*Further action: Review all data flows to determine if any data is processed outside of the EEA.*

1. *https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-to-erasure/* [↑](#footnote-ref-1)
2. *https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-to-data-portability/* [↑](#footnote-ref-2)
3. *https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-of-access/* [↑](#footnote-ref-3)
4. *Information Commission Officer https://ico.org.uk/global/contact-us/* [↑](#footnote-ref-4)
5. *Privacy Impact Assessments are already carried out for CCG/SCW CSU led initiatives as part of existing project management processes* [↑](#footnote-ref-5)