What's new in GDPR and Actions for your practice

Heading	What's Changed?	Notes	Action
Individual Rights			
The right to be informed	The GDPR sets out the information that you should supply and when individuals should be informed. Emphasis on transparency	Further guidance for organisations on the right to be informed is provided in the ICO privacy notices code of practice.	Publish Fair Processing Notice (*see template in guidance pack*) Display poster in reception (*see template in guidance pack*)
The right of access	Was 40 calendar days – now must provide WITHIN ONE MONTH. Was able to charge up to £50 for medical records – now FREE OF CHARGE.	You must provide a copy of the information **free of charge**. However, you can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive. You may also charge a reasonable fee to comply with requests for further copies of the same information. The fee must be based on the administrative cost of providing the information.	Ensure procedure for dealing with access requests is in place. Inform patients how to make a request through your Fair processing notice. You may have a web form to submit a request. Check if you can give online access and promote this to patients. Decide what is reasonable fee (e.g. cost per sheet of printing/copying or hourly cost of staff) Have template letter to send to individual if insurance company has requested full record (*BMA guidance on SARs for insurance purposes*).

The right to rectification	Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. If you have disclosed the personal data in question to others, you must contact each recipient and inform them of the rectification - unless this proves impossible or involves disproportionate effort. If asked to, you must also inform the individuals about these recipients.	Changing information on the GP system means the spine will be automatically updated. Any organization taking information from the spine will have the new details. Where you are not taking action in response to a request for rectification, you must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy.	Healthcare record –maintain the incorrect data, clearly indicating what is incorrect and what is now correct, so full picture is available. Other records – have process for review and process for updating (e.g. check home address and email when contacted by patient).
The right to erasure	Right applies where: • Data is no longer needed • Consent is withdrawn • Subject objects and no overriding legitimate grounds to continue • Data has been unlawfully processed But does not apply: • Where legally obliged to process, carried out in the public interest or the 'exercise of official authority vested in the data controller'	Can retain the data in the health record for continuing provision of healthcare. Where you are not taking action in response to a request for rectification, you must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy.	Assess each request on its merits. Write to the individual of your decision.
The right to restrict processing	Individuals have a right to 'block' or suppress processing of personal data. When processing is restricted, you are permitted to store the personal data, but not further process it.	Where a patient is known to staff (e.g. a relative or colleague) it may be logical to restrict access to confidential information to nominated clinicians	You may need to review procedures to ensure you are able to determine where you may be required to restrict the processing of personal data. Inform individual of right to restrict (object to) processing beyond the practice and related risk.

The right to data portability	The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.	The right to data portability only applies: • to personal data an individual has provided to a controller; • where the processing is based on the individual's consent or for the performance of a contract; and when processing is carried out by automated means.	This is covered by GP2GP process when a patient changes surgery.
The right to object	This right applies regardless of which legal basis for processing is relied on. You must stop processing the personal data unless: you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or the processing is for the establishment, exercise or defence of legal claims.	You must inform individuals of their right to object "at the point of first communication" and in your privacy notice. National data opt-out programme applies. NHS Digital is developing a new system which will allow patients to make an informed choice about whether they wish their personally identifiable data to be used just for their individual care and treatment (Type 1 opt-out) or also used for research and planning purposes (Type 2). NHS Digital will launch the new national opt-out programme to the public in May 2018. Clinical research will still require valid consent.	You must inform individuals of their right to object "at the point of first communication" (e.g. registration) and in your fair processing notice. Inform individual of the related risk to their health if information is not shared for their care. Sign up for news about the national opt-out programme at: https://digital.nhs.uk/national-data-opt-out

Rights in relation to automated decision making and profiling.	The GDPR applies to all automated individual decision-making and profiling. You can only carry out this type of decision-making where the decision is: • necessary for the entry into or performance of a contract; or • authorised by Union or Member state law applicable to the controller; or • based on the individual's explicit consent.	For healthcare, this includes risk stratification.	Continue with current Type 1 and Type 2 opt-out measures. Awaiting further guidance from Department of Health on profiling for risk stratification. Risk stratification is lawful processing. If you are sharing data for risk stratification, ensure it is included in your fair processing notice.
Consent			
	GDPR builds on the DPA standard of consent. Under the GDPR, "consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement." The GDPR therefore does not recognise implied consent. Note that the common law of confidentiality still does.	If consent is a precondition of a service, it is unlikely to be the most appropriate lawful basis. Much of clinical care has traditionally been conducted on the basis of implied consent. However, consent is not necessarily the best basis for sharing data for direct patient care. For healthcare, other legal basis is available. See: *Information Sharing Guidance*  SharingGuidance2018v1.0.docx for further detail.	Check your legal basis for all processing on your data flow map (*see template*). Establish where Consent is the most appropriate legal basis. Review your forms to ensure consent will be valid under GDPR (*see guidance*). You must keep clear records to demonstrate consent – your GP systems implement preference for sharing. How do you capture evidence of individual's decision? Keep consents under review and refresh them if anything changes. Build regular consent reviews into your

		ICO guidance on consent is under review and will be updated. Guidance is available on the ICO website at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/	business processes. See guidance pack for consent checklist.
Accountability and Governance			
	Maintaining records of 'processing activities'	Must be able to evidence aspects of data processing: What, why, when, how, and who with.	Complete and maintain both: • Information Asset Register • Data Flow Map
	Implement appropriate technical and organisational measures that ensure and **demonstrate** that you comply.	Maintain information governance policies, staff training records, audits of processing activities, and regular review of policy and processes	IG Policies which take account of 'all relevant legislation' mean you do not need a separate GDPR policy. New Data Protection Act expected May 2018. Update policies with reference to applicable legislation once new DPA and applicable legislation confirmed. Further updates will be sent out by your GP IG manager during April and May. Implement new national data guardian data security requirements (see guidance pack).

Appointment of a Data Protection Officer	You currently have an IG lead and/or Caldicott Guardian. GDPR requires that public authorities appoint a Data Protection Officer. The Data Protection Officer (DPO) is key to ensuring organisations comply and can demonstrate GDPR compliance.	You should designate someone to take responsibility for data protection compliance and where this role will sit within your organisation's structure IGA guidance on the Role of the Data Protection officer is available at: https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance	Consider how your practice will fulfil the Data Protection Officer role. • External Resource • Shared Resource with other practices • Attachment of DPO responsibilities to another role • Appointment of dedicated DPO for your practice/ federation Further clarification on responsibility for appointing a DPO is awaited
	All personal data breaches must be reported within 72 hours on the NHS SIRI reporting Tool https://nww.igt.hscic.gov.uk/	You need to have the right procedures in place to detect, report and investigate a personal data breach	Update your incident reporting procedure Ensure your staff know how to recognise a breach and are aware of reporting requirements
Privacy by Design			
	Implement measures that meet the principles of data protection by design and data protection by default. Requiring a risk management approach to ensure measures are proportionate to the level of risk. Mandatory to complete a Data Protection Impact Assessment (DPIA).	You are not required to complete a DPIA retrospectively, but should complete one for all new processing. DPIAs are undertaken for new processing by SCW for SCW led projects	Anonymise or pseudonymise data whenever possible, and minimise use of personal data. Complete a Data Protection Privacy Impact Assessment for all new processing (see template and guidance).