**Get GDPR Ready - Get (Sort of) GDPR Confident!**

**Adrian Poole, The Canalside Conference Centre, Bridgwater 28th February 2018**

Adrian Poole told an audience largely composed of practice managers that he would set out the law and principles before talking specifically about the implications for health. He said that that owing to the lack of guidance and the fact that the Data Protection Bill could not pass through Parliament until Autumn there could be no true confidence. We have to learn to love GDPR because it was here to stay, will be the law and that the DPA was now outdated. The new rules will apply to all contracts from 25th May although the chance of "UK PLC" being compliant by then was nil. Many key data protection principles will remain the same although be expressed differently and some will become enhanced and amended. There will be some new requirements to formalise established best practice such as "Privacy by Design", Data Privacy Impact Assessments. He advised that data should be regarded in the same way as "Health & Safety." Actions then might not be different but they would be formalised. There would, inevitably, then be more stringent sanctions applied.

Some definitions - a data controller was anyone with control over the data in question. A data processor was anyone who does anything with the data - these were not mutually exclusive. Personal data is that which enables identification, even indirectly. Special categories of personal data includes health, racial or ethnic, political opinion, religious, sexual orientation and genetic and biological data.

The law is, then, trying to catch up with rapid progress in digital information handling.

Cultural approaches included needing to be prepared to give people more information about their data, to limit the purpose for which data was used and data minimalisation to allow collection of what was needed. This would push back against the commodification of data collection. Every reasonable step needed to be made to make sure the data was accurate. Data should only be stored for as long as necessary for the original purpose. There must clear processes to protect data and accountability for when things have gone wrong and being able to demonstrate compliance with the data protection principles.

There is an exemption for organisations with fewer than 250 employees but as practices deal with "special categories" of data this will not apply.

Key points are to need to be audit ready and to "live" data protection.

Control of data is fundamental - no more liassez faire. As well as how data is held, handled and transferred relationships with third parties need to be reviewed with evidence available such as confidentiality clauses in contracts, data protection policies, information governance and security policies, privacy notices, records of processing and breaches and any commercial terms and conditions. Existing data sharing agreements would have to be tested to make sure recipients were GDPR compliant.

Data protection impact assessments are a requirement under the GDPR.

Privacy notices must be in clear, concise, intelligible language and be readily accessible. This information must be provided at the time of collection if from an individual or within a maximum of a month if gathered otherwise. A privacy notice must contain the data controller details, purposes and basis for processing, the right to withdraw consent, categories of data, source of data including public sources, whether data is a contractual or statutory requirement, whether there will be any automated decision making or processing, the data retention period, recipients of data if it will be shared, details of any transfers outside Europe, the individual's rights to object to marketing, to be forgotten and so on.

An expert in data protection law should be appointed to be the Data Protection Officer and this will be a very hard requirement for practices to achieve. This could be shared amongst organisations. Adrian Poole suggested that the LMC might provide such a person but your correspondent soon countered this. The GPC view is that the TPO should be a CCG role.

Conditions for processing special category data include that consent must be explicit. There is an argument that data collection necessary for compliance with GMS contracts does not apply to patients who are not party to the contract but equally they could say to be so by dint of what is necessary for the patient's care. It will be necessary to protect vital interests when consent cannot be given or when necessary for public interest or for the controller to carry out its legal obligations such as those of the practice to the CQC. The legitimate interests of the data controller can also be taken into account those that are necessary for public interests based in law (such as seeking a DBS check on an employee), connected with healthcare, pharmaceutical or social care purposes (!) or based on archiving, scientific or historical research purposes (which remains vague). So consent is important and should be sought but not absolute. The review of consent is fraught - if the data is wrong by then then attempting contacting the patient at the by then wrong address could be a data breach!

Implied consent will no longer exist. It must be a freely given, specific, informed and unambiguous indication of the individual's wishes. That said vital interests of the subject such as matters of life and death, processing that cannot be consented can be exceptions. Also when a task is in the public interest or the data controller's legitimate interests. Subjects of data have the right to challenge and access the data held, to withdraw that consent, restrict data processing to storage (particularly if of disputed accuracy, the right to erasure after withdrawal of consent and the right to challenge compliance with the GDPR. This could well lead to a new claims culture as people "have a go" to see if breaches can found or lack of compliance cannot be demonstrated. There will be a new right for data to be transported ("ported") to another provider.

Subject Access Requests (SARs) will mean that no fee will be chargeable and the time limit is reduced from the maximum of two months to one month. It seems likely that insurers and lawyers will now be asking clients to get information themselves under an SAR.

Children under 13 can never give valid consent under the GDPR. Privacy notices will have to be couched in terms understandable to the 13-15 year olds.

Data breaches are widely defined and must be reported within 72 hours to the ICO (including weekends) unless the breach is unlikely to affect rights and freedoms, the controller has taken measures to protect the data (encryption) or the notification will take "disproportionate effort" in which case a public communication (newspaper, website) should be used. This also seems a good opportunity for claims companies to "have a go."

Sanctions under the GDPR can be a fine of up to 4% of worldwide turnover or 20m Euros whichever is the greater. Individuals will also have the right to seek damages for material and non-material losses such as distressed caused.

On a practical note, the important thing for practices is to concentrate on basic things first such as conversations across the reception counter, who can overhear phone calls, access to computer and paper records, and so on. Note that a risk assessment to make sure that existing safeguards are reasonable and that "reasonable steps have been taken" to show that privacy has been designed into processes should generally satisfy the GDPR. It's as if one now need to be able to "prove one's innocence" as practices are caught in the crossfire of legislation designed for quite another purpose. Otherwise it is beholden on data holders and processors to notify the IPO and individuals concerned as defend in the regulations.

We then moved on to specific health and social care considerations and this will also include staff HR information. This information will be of high risk with more general rights of access. The problem with consent in this field is that "people can be odd" and will question the legitimacy of their consent or withdraw it to make doing one's job difficult. However recall that acting in their vital interests if consent cannot be given, legal requirements (such as being able to defend a subsequent claim), substantial public interests and the "get of jail card" of the HEALTH & SOCIAL CARE EXEMPTION can be referred to as a genuine opt out where proper consent cannot be obtained after it being attempted. The GDPR was designed to defend individuals against the likes of Amazon, not GPs. THE PUBLIC SERVICE EXEMPTION can also be used for health care data - caveat the Bill provisions are not fully known.

There are limitations to the GDPR - it does not apply to existing laws of consent to care and treatment, confidentiality or to the Caldicott concept of implied consent. The FoIA is also not affected.

Conditions for the processing of data include the provision of health care or treatment etc. Substantial public interest conditions also include purposes of preventing and detecting crime, counselling, pensions, political parties, elected representatives and anti-doping in sport. Exemptions include crime and taxation, immigration, disclosure required by law, protection of the public against malpractice or risks to health and safety and information demanded by regulatory bodies.

The rights of data subjects on SARS must be adhered to but be careful of revealing "too much" including third party data without consent. Disclosure to third party organisation's where getting consent would prejudice the purpose for which the information is required such as by the police, the court or HMRC.

The rights of data subjects to obtain rectification or erasure of inaccurate personal data but no explanation need be made if the data is necessary for the performance of a public interest task or exercise of official authority or to make or defend a legal claim. Any refusal must be accompanied with an explanation. When a subject raises an objection data processing must stop unless: there are compelling legitimate grounds overriding the data subject's rights or it is necessary for the making or defending of a claim. Processing must be restricted whilst dealing with any rectifications requested, dealing with objections, where the process is unlawful but erasure is opposed and where the data is otherwise not needed but the subject requires it to pursue legal rights.

This was an excellent session with a knowledgeable and engaging speaker. It seems to be that the intentions of the Regulations are honourable but they do present risks for practices trying to deliver health and social care with scope for fishing expeditions by lawyers and claims firms as well as genuine risks to the unwary that do no not address basic matters such as being able to justify actions and compliance. Other matters like the names of patients announced to waiting rooms and the provision of staff information to external payroll providers need to be considered. There was an interesting question about staff biographies on practice websites now requiring informed consent from the individuals concerned. There will be no more charges for viewing records or releasing records to individuals.

What is necessary that practices should conduct a data audit promptly, purging old, extraneous information still being held on staff files for instance. The important thing is to be able to justify actions and policies.