Are you ready for the GDPR new format for data protection on 25th May 2018?

Now is the time to start preparing for the new GDPR act that will supersede the current DPA legislation.

The act although European in birth will continue with its tougher rules on data protection post Brexit Transition as it is being brought into force under the new British Data Protection Bill.

Applying for registration with the ICO and spending £35 in doing so does not complete your necessary task in compliance.

The new act puts teeth on the old act and creates a requirement for everyone keeping data to provide proof of compliance and as well as naming a designated data controller requires those processing data to be counted as data processors with responsibilities.

Those failing compliance and receiving complaints about data breaches can face considerable fines of up to 20 million euros or up to 4% of their worldwide turnover.

Many of the current DPA rules continue but there are many changes that affect health care practitioners especially.

Whether you are a corporate, sole trader or self-employed locum (with the ability to control and take your px list with you), you will be treated as requiring registration with the ICO and as a key member in a practice will be regarded as the data controller.

Your staff processing data will for the first time be regarded in law as data processors and will also be responsible for their actions.

You therefore need to assess the effects of the new law on your business, your data collection processes and the education and awareness you provide to all your staff. This will require their involvement, understanding and a “signing off” of the acceptance of their roles.

Each practice will need to assign a key and senior member of staff to be the data controller. There will need to be policy and procedures in place, and visible to staff and customers in writing and on your website.

Training

With the inclusion of all staff involved in data processing you will need to put in place a written record to ensure you are and have :

Training Induction process Retrain over time or after changes Refresh

Policy decisions

Decisions will need to be made on what information it is appropriate to retain, its life span and retention and its updating, back up and security.

Under GDPR information such as ip addresses genetic and biometric data will be included.

Remember it is your duty from May 25th 2018 onwards to prove that you are complying with the law.

Transmission of data can be verbal, electronic and in paper and you will need to assess who you are sharing this information with if it is not to the individual whose data it is.

Inadvertent disclosure verbally, or from printers or screens to others not mandated to receive it ie non staff or staff not considered to be of a correct level of seniority is an offense.

So you will need to write a plan that is easily understood by all staff that encompasses continued learning, induction training, security levels and password provision.

What information you need to keep and or how long. Rules on its security and transmission, including practice security.

Security

These activities are legally essential and not just advice. Failure to carry them out will cause a punitive fine where a breach has been reported.

So screens should have auto locking, printers should be pin coded and no written or printed documentation should be left in view. Each staff member should be allotted a secret password which is frequently changed and never disclosed amongst other staff members and provides the level of entry into data appropriate for that staff member's seniority, knowledge and need to know.

Remember to remove leavers from the password system.

All electronic equipment should be pass-worded and encrypted and only USB keys that are encrypted should ever be used.

All firewalls should be in place and kept up to date. Regular malware scanning is essential.

Patches must be applied immediately.

Up to date malware must be active, check back up procedures with any discs kept in a different and safe place. All USB sticks must be encrypted and mobile laptop drives disabled.

If using storage facilities, you will need a contract in place for its security including fire and flood from the provider and physically inspect the premises.

Screens should be out of view from non-authorised visitors, and care should be taken not to mention personal details across the floor of the practice.

Paper documentation should be under lock and key and keys should be held in a lockable key cupboard with a key held by the designated controller or his deputy during holidays and not left in a desk drawer.

When discarding IT equipment, you need the hard drives professionally cleaned, deleting files doesn't work

Home Working.

Carries all the same requirements as in office but the risks increase with stolen laptops, smart phones and tablets, as well as records and paperwork carried to and from engagements i.e. domiciliary visits.

Never leave anything in a locked car or boot. Keep it with you at all times in a locked case.

Log onto all mobile devices and use VPN to access office info.

Disclosure of information.

If requested by the owner of the data, you have a requirement to disclose all the information directly to the owner of the data on direct request. You can ask them to be specific on what they require but if they want the complete information you hold about them you must give it, currently within 40 days but after GDPR day this will reduce to 1 month.

The request must be in writing where email and fax is acceptable. As long as there is valid proof of identity.

To track the request, it is useful to create an "Access Info Request Form" suitably dated with information of the info requested and dates and type of transfer made, plus proof taken of identity.

You cannot alter or amend any record or documentation after a request has been made.

The clock starts ticking as soon as a request is received unless from a 3rd party e.g. a carer, relative with power of attorney, solicitor or another professional. You must verify the 3rd party as to who they are by a reasonable request for proof. You can also clarify what information is required by a 3rd party and whether it is relevant and timely. Past history of symptoms and history of problems passed or cleared up is not regarded as relevant.

If for example a patient cancels his appointment and his partner rings supposedly on his behalf trying to contact him it's not appropriate to inform the partner of his activity or the cancellation within the practice.

The transmission of information should be secure and if you have to use fax or email or SMS, the patient should have consented to this. If sending to a verified 3rd party you must ensure the verified receiver is standing by a fax machine before transmission.

When sending records to a 3rd party professional it is not appropriate to send more information than needed that might put the data owner at a disadvantage.

Records should not be retyped from for example a badly written record, they should be photocopied.

Up until new rules apply in May 2018 you can charge £10 for electronic information and where paper records involved up to £50. After the new rules apply you must not charge.

You do not have to respond to excessive repeated requests

It is useful to have a designated member of staff who deals with requests and the follow through.

Where possible the new GDPR will suggest that a request can be made remotely into the record data.

Security Breach

What to do:

Collect the facts

Ascertain what has gone wrong

Report breach to ICO by phone helpline for advice within 72 hours.

Take the necessary steps dependent on seriousness

Learn from Mistakes

Share Knowledge

Notify all possible victims

Apologise (Duty of Candour)

Reassess policy

Tips on preparation for GDPR May 25th 2018

AWARENESS choose key people with seniority to champion and educate.

Look at what you hold in data, whether relevant and where you hold it.

INFORMATION create an asset table and the risks around them.

RETENTION How long do you have to keep data

COMMUNICATION Create a privacy notice in print and online for all to see, to include etention times and what you are holding.

INDIVIDUALS RIGHTS. You cannot delete or amend data after a request is made.

CHILDREN likely to have greater rights. Children at present assumed to be 13 years or below but this might be changed.

DATA Breach require a process written down to deal with event

MAKING CHANGES Need to assess risk in making data collection and holding changes. Create a Protection Impact Assessment PIA.

Simple examples of errors in the past.

Files in bin bags for inappropriate disposal methods

Stolen briefcases, Px records, staff wage details and personal information.

Uploaded files using Google platform accidently posted on public pages

Left files after relocation of premises in old cupboard new tenant disallowing entry

Shared email addresses

SMS Text read by another

If you share data with another controller you must have a contractual agreement that you both are compliant.

Sending texts, eblasts and paper marketing and recall must be pre-consented. Consider recall letters and especially using open post cards which expose information to all do you have proof of consent?.

Useful Contacts

www.dpreform.org.uk

https://iconewsblog.wordpress.com

Security Breach Helpline 0303 123 1113.

This briefing was designed and written by the Primary Health Net Team after extensive investigation and meetings with ICO.

18.10.17