GDPR: STAFF COMPLIANCE CHECKLIST

This document is designed as a simple checklist for you to use in order to ensure that you are thinking along the right lines when you process any personal data. At the end, there's a list of stuff that you need to do or be aware of.

Registration

1. After 25th May 2018 you MUST be registered with the ICO if you are processing personal data, whether this is on paper or electronically. If you are registered with the ICO already for Data Protection Act purposes, then this will carry over.

2. This only applies if you are the "Data Controller" – in other words the person who keeps the data. **If you only work as an associate in someone else's practice, you don't need to register**. But, if you have your own patients, and you store their data yourself (including a locked filing cabinet in someone else's building) then you do have to register.

3. Here's where to register:

https://ico.org.uk/for-organisations/register/

Case Histories

4. You do NOT need consent to process (ie store and handle) case histories. The GDPR provides 2 reasons to process personal data:

   a. **Contract**. You have a contract with your patients to provide a service and the case history is necessary for you to fulfil your part of the bargain (and before you ask, a contract can be oral or written, and does not require money to have changed hands).

   b. **Legitimate Interest**. It is a legitimate interest for both you and the patient that you record a medical history and your treatment.

You also have a **Legal Obligation** to retain your notes for the statutory minimum of 8 years, but this is not in itself a justification for taking the notes in the first place(!).

Note that there is actually a DANGER in asking a patient to consent to your processing their data: first, giving consent implies that they can withdraw it – which they can't, because the moment you write a medical note you have to retain it (see above). Also, if you fail to notice that they did not tick the consent box and then proceed with treatment, theoretically you could find yourself in the sticky stuff. *(Thanks to Deborah Smith at Mint for pointing this one out)*

Realistically, of course, none of this is ever likely to be a problem, but we need to keep things legal, as well as simple.

Staff and Associates

5. You do NOT need consent from your staff/employees/associates to process their personal data. Again, you have a **contract** with them, and if you can't process their details they won't get paid!

Data Protection Officer

6. You do NOT need to appoint a Data Protection Officer. This is only required for large organisations. Feel free to do it if you really want to, of course.

Data Security

7. You do have to make sure that personal data is secure:

   a. It is fine to store paper case notes in locked filing cabinets, provided unauthorised persons do not have access to the keys.

   b. Filing cabinets (locked or otherwise) inside a secure building are satisfactory. The regulations simply require that reasonable steps have been taken to prevent unauthorised persons accessing the data. You do not have to remove the filing cabinet keys from locked premises – that would be ridiculous! Just make sure that the cleaning lady or the electrician can't get hold of the keys and access all your notes- ie don't leave them in an obvious place.

   c. It is fine to store data on a password-protected computer, provided reasonable steps are taken to prevent unauthorised persons accessing the computer.

   d. You are not in breach of the GDPR if your computers or files are stolen, but you should inform the ICO immediately that there has been a possible breach. It would be good practice also to inform the General Council, but it is not a requirement.

   e. If using a cloud-based data-processor (PPS, TM4, Cliniko or similar), you need only check that the provider is GDPR compliant. Check with them too that there is no personal data saved on your own, local computer(s) – this is simply so that you know whether there has been a data breach in the event that the computer is stolen or lost. And bear in mind that you may be saving personal data yourself in the form of Excel spreadsheets, letters to GPs or similar.

   f. There is no requirement under GDPR for you to back up data. However, if your computer explodes and all your data is lost, that would be a breach, because the data is no longer available (it's also a bit of a disaster for you!). If you do have a backup, it isn't a breach.

Appointment Reminders

8. There is no need to obtain consent for appointment reminders, as this constitutes "**Legitimate Interest**" under the GDPR, but there is no harm in doing so. The same applies, of course, if you need to change or cancel an appointment.

Information About A Patient's Current Condition

9. "**Legitimate Interest**" is also sufficient reason to send a patient information about their current condition – things such as exercises, or specific information which may help them recover.

10. It's OK to contact a patient to find out how they are (and if they are doing well, there's no reason that you shouldn't then ask for a testimonial).

Consent

11. Unlike those things mentioned above, "**Consent**" is required for all marketing information: promotions, newsletters, "clinic updates", etc.

12. There are very strict rules about what constitutes consent:

    a. The request for consent is prominent and separate from terms and conditions. So, no weasel-wording to obscure your intention to send marketing bumph.

    b. People must positively opt in (no pre-ticked boxes or any other type of default consent). You can never infer consent.

    c. The language must be clear, plain and easy to understand (so why not make it entertaining?!).

    d. You must give individual options to consent separately to different purposes and types of processing (eg newsletters, info on specific medical topics).

13. Individuals must be able to refuse to consent without detriment. In other words, you can't give them shabby treatment just because they didn't want your newsletter!

14. Consent must not be a precondition of service. Remember, this is consent to receive your **marketing** info; processing their data (your case history) *is* a precondition for providing treatment, but you do not need consent for that element because it's part of the contract, and is classified as Legitimate Interest.

15. You must keep a record of when and how you got consent from the individual, noting exactly what they were told at the time.

Managing consent

16. Review consents regularly to check that the relationship, the processing and the purposes have not changed. This is relevant if you start up a new method of marketing (text messaging, for example).

17. The GDPR require that you have processes in place to refresh consent at appropriate intervals, (remember, this is about marketing only – not permission to treat, and not for processing and retaining case histories), but an "appropriate interval" is not defined.

18. Consider using privacy dashboards or other preference-management tools as a matter of good practice. This only really applies if you are getting consent through a website. For most practitioners this will be an unnecessary complication.

19. Make it easy for individuals to withdraw their consent at any time, and publicise how to do so. This applies to any marketing material and is really important. Patients cannot withdraw consent to you processing their medical records until the statutory period of 8 years has expired.

20. Act on withdrawals of consent as soon as you can and do not penalise individuals who wish to withdraw consent.

Informing Patients

21. Make sure that patients are aware (or can easily discover) how their data is processed and why. A privacy notice on your website is sufficient for this purpose, but you might also consider making the notice available to all patients when they first attend (if they fill in a patient information form, for example, add a single sheet underneath for them to read – they don't have to sign it).

22. You could add a link to the bottom of your emails, or a reference to the web page in other written communication.

23. You do NOT have to have a sign on the wall giving chapter and verse of the GDPR. In fact, you do not have to have a sign on the wall at all!

24. If you are communicating with patients and consent is a requirement (marketing, for example), then patients must be told that they can withdraw their consent at any time.

Stuff You Need to Do or Know About

25th May 2018 **Make sure you're registered** – the GDPR is incorporated into the Data Protection Act 2018. Now it's law!

Make sure you have a **Privacy Notice** on your website and, ideally, as a sheet that patients can read when they first present.

Make sure that you have **consent to send marketing information** (ie anything not related to a patient's enquiry or current problem).

Unless they actively opted in, you'll need to "re-consent" your existing patient list.

Data Requests

You have **30 Days** to provide data or information about the data you hold if asked by an individual (aka a "Subject Access Request"), Pre-GDPR it was 40 days. Make sure you confirm the identity of the individual requesting the data, of course – you simply have to take reasonable precautions (you might **recognize** them, they could provide their **signature**, you could ask for an identity document, such as a **driving licence**). If they make the request from their email address, you could send the data in a password-protected file, then contact them by telephone to provide the password.

Data Breaches

You have **72 hours** from discovery to report a data breach which is likely to cause a "risk to an individual's rights and freedoms". You do NOT have to report every trivial lapse, however.

If it's a high risk (eg significant detrimental effect such as damage to reputation, financial loss, or other significant economic or social disadvantage) then you have to tell the individual as well.

Charges

You **cannot charge** to provide data if an individual requests it (ie a "Subject Access Request). You **can** charge a reasonable admin fee if it's a third party that requests the data (insurance company, solicitors etc).

Use common sense.

This is all about being polite. It's about preventing patients from getting unwanted messages, which they might think of as spam (no matter how hard you worked on your marketing masterpiece!) and making sure that personal information isn't shared with people who don't need to know it.

Call us if you need help: 01933 328150