GDPR: CONSENT IS NOT EVERYTHING

There are those who would have you believe that you have to have explicit consent from every individual whose personal data you wish to process, including all your patients. In particular, some will argue that you need signed consent in order to take and store ("process" in GDPR lingo) a case history.

Bollocks.

I'll try to make this really simple. There are 2 elements involved, and you have to satisfy both:

1. You must have a "lawful basis for processing" the data

2. Because health records are considered under the GDPR to be "Special Category Data", you have to have an additional justification to process them.

Your Lawful Basis For Processing Data

Consent is only one of the 6 possible reasons for processing personal data. Any one of the 6 is sufficient on its own.

Here are the 6 lawful bases, with examples of where they are relevant to you as a medical practitioner:

1. **Consent**. Particularly relevant if you are sending marketing information, such as newsletters, offers, vouchers etc. This is when a person actively ticks a box to indicate that they consent to you processing their data in the way you describe.

2. **Contract**.

   a. You have a contract with your patient that you will provide them healthcare – this does not have to be written down, nor does a fee have to change hands. The fact that a patient has asked you for your help, and you have agreed to do so constitutes a contract. You are allowed to process their data to the extent necessary to fulfill your part of the bargain. That means you can take a medical history, record your actions and keep that record in accordance with your legal obligation.

   b. Staff and Associates will also have a contract with you – in this case a written, signed contract (well, they should!). Therefore, you can process their personal data in order to fulfill the contract – store it, record bank details and payments. Otherwise you cannot fulfill your contract – they won't get paid!

Written consent is not necessary in either of these cases.

3. **Legitimate Interest**. This is a very broad category, and can refer either to your own legitimate interest or that of the patient. You do have to explain in your Privacy Notice why you think Legitimate Interest is an adequate justification for processing data, however.

   a. If you are treating a patient it is clearly of legitimate interest to you that you record your findings and treatment. No additional form of consent is required.

   b. Legitimate interest also applies if you are sending information directly related to a patient's enquiry or condition – rehab or exercise information, for example.

Some might argue otherwise, but "Legitimate Interest" is an extremely tenuous reason to send patients information which does not relate to their own enquiry (whether through the website or as a consultation). It could be argued that that is straightforward marketing and DOES require consent. So just be cautious on this one, and make sure there's a very prominent opt-out link.

4. **Legal Obligation**. This covers the storage and processing of patient notes. You have a legal obligation to retain patient notes for the statutory minimum period **(although this is *not* a reason to collect the information in the first place!!)**.

5. **Vital Interest**. Unlikely to be relevant. Maybe a patient suddenly suffers a heart attack and you have to call an ambulance and provide their data – but seriously, what casualty is going to complain?

6. **Public Task**. Not relevant unless you are a copper, trying to exercise your public duty.

But is signed consent a good idea?

Well, you might think that there's no harm in it. Belt and braces, as it were. And if you're like most practitioners, you probably get patients to complete a short form when they first attend. So why not have a check box (not pre-checked, remember!) at the bottom, which says they consent to you processing their medical records?

But, actually, it might be a BAD idea (and I'm grateful to Deborah Smith of Mint, for bringing this up). Here's what she pointed out:

1. Asking for consent implies that consent can be withdrawn. The moment you have a medical record, you have a legal obligation to retain it for the statutory period. So the consent is actually meaningless.

2. If a patient does not tick the consent box, and you fail to notice, you might then proceed with treatment, create a medical record and be required by law to "process" it. Against the wishes of the patient. Now this is very, very

unlikely, but why create a possible problem for yourself when there is absolutely no need?

Special Category Data

To process "Special Category Data" (which includes health information), you have to satisfy an additional condition.

There are 10 conditions which justify the processing of Special Category Data, and you have to satisfy at least one of these as well. Consent – as above – is one option. But here's the one that's relevant to you:

> "processing is necessary for the purposes of...medical diagnosis, the provision of health or social care"
>
> *GDPR, Article 9, para 2(h)*

So, you have 2 reasons from the standard list to process your case histories (ie store them and use them), and you have a reason to collect Special Category information. That is all you need – **you do NOT need signed consent**.

Unsubscribing

If a patient asks you to stop sending information about their back pain or their next appointment, you have to stop, of course. And you have to do it pretty much straight away.

The "Right to be Forgotten"

No matter what a patient says, you may not delete their records before the legal minimum of 8 years (or age 25 if longer) has expired – it's a legal obligation and overrides their right to be forgotten.

After that legal period has elapsed, you must of course delete their data unless there is a reason to do otherwise (court case/insurance claim pending for example). But you must also keep sufficient data so that you know that they have asked to be forgotten! This is to prevent you inadvertently contacting them again, and so that you have a record that their medical notes were deleted at their own request.

You do NOT have to delete their records immediately the 8 year period is up if they don't ask you to. You can keep their notes indefinitely (but you should explain that this is your intention in your Privacy Notice).

Passwords and Encryption

The GDPR does not specify any need for encryption or passwords, but it is incumbent on you to take reasonable measures to secure personal data. This will in part require common sense, but also may be affected by your risk assessment: how often have properties in your area been burgled? Is you building alarmed and locked at night?

If you keep personal data on your computer (remember this may not be the case if you are using a service like PPS, TM4 or Cliniko) then make sure the computer is password protected. Just apply the normal rules: make it complicated, change it regularly and don't have it sellotaped to the screen (or written down in an obvious place).

As for encryption this is unnecessary. It is certainly a good idea to password protect documents that you may be sending to other practitioners, solicitors/insurance companies etc, and to send the password separately, preferably by a different means. But let me re-emphasise that opening sentence: **the GDPR does not specify that you must encrypt your emails.**