Academy of PHYSICAL MEDICINE

Broadcast Summary

Caution: These notes should be used in conjunction with the recorded interview. While every effort is made to ensure accuracy, APM cannot guarantee freedom from any errors. If you do spot any errors in this text, please let us know so that we can correct them.

Notes:
1. The discussion transcript has been supplemented with new information, from either the Information Commissioner's Office or legal sources.
2. Where that new information, or the original discussion, addresses important or frequently asked questions, the text is highlighted in yellow.

The General Data Protection Regulations

With

Simon Butler, Barrister (specialising in healthcare and related data protection)
and
Paul Grant, Solicitor and Registered Osteopath

Much information about GDPR currently:

- it has implications for practice
- much of what is available creates unnecessary fear and confusion
- compliance with the GDPR actually requires very little extra work in most cases.

The aim of this discussion is to try to make your working life as easy as possible and take away the fear and other problems that come with great bureaucratic tangles like the GDPR.

Three things worth referring to (posted on the website):

- a checklist for your staff on ensuring that you are complying with GDPR.
- Info you could give to patients
- a summary of what should go into your privacy notice.

Three areas of relevance:

- processing patient or staff data
- communication with patients, and

- marketing, which could be subdivided into:

    - dealing with your existing patients who may have consented or not and
    - people who you may be marketing to through other means. Probably the area of most contention or most change under the GDPR.
    - But before we do that, would you like to give us a quick overview on what the hell

OVERVIEW

GDPR is a European directive, which will be incorporated into the Data Protection Act 2018, replacing the previous DPA. The new DPA comes into force on 25th May 2018, and is intended to simplify data protection across Europe, ensuring all citizens are aware of rights and obligations relating to data. People need to know:

- how they can access their data
- how others might process it
- how long it will be retained
- when they're entitled to erase it.

Much of GDPR will not apply to most practitioners - it is more relevant to large corporates, such as Facebook.

PROCESSING PERSONAL DATA

Processing personal data means using any information which can identify a living person, whether you do it in order to provide your service or for marketing.

Consent is an important part of the GDPR, but is only one of the 6 "lawful reasons" to process data.

With existing patients, whose data is already being used, Osteopaths and chiropractors may be a need to go through a new consent[1] process (but see the notes below on when consent is required):

- Consent to retain patient data:

    - since the broadcast, APM has had discussions with the ICO, who have confirmed that you DO NOT need consent to retain patient notes (in GDPR terms, you can "lawfully process" this data because of your "contract" with the patient and due to your "legitimate interest" in doing so. Retention of the notes is a "Legal Obligation" under the GDPR. Health data is "special category" data, but you are permitted to process it for the purposes of diagnosis and provision of health care). Simon Butler accepts this but

[1] *Note: consent in GDPR terms is NOT the same as the informed consent necessary for treatment. As noted in a previous discussion, written consent to treatment, signed in advance, is unlikely to be adequate in court, although it at least shows good intent. If written consent for treatment is used, it should be separate from consent to process personal data.*

notes that it *could* be regarded as good practice to get consent[2].

- You can send appointment reminders without explicit consent (confirmed after the broadcast with the ICO).

- Consent can be oral, with the practitioner noting it in the records, but a signed form is more robust.

- Retain consent notes for as long as you retain medical records.

- Theoretically, if you choose to ask for consent to process data for your case histories, a patient could refuse:

    - It would be unethical to treat a patient who insisted that you could not record your findings etc, so you could refuse to treat.

    - You DO NOT have to have consent to create and store case histories (see above)

    - The situation is highly unlikely!

- Standardised Forms: the iO has produced one (bit.ly/io-gdpr), and we are informed that The Royal College of Chiropractic also has a GDPR toolkit. But note that consent to process medical records is NOT required.

- Electronic consent

    - Online forms can incorporate a "signature" box

    - Acceptable for the practitioner to record that patient gave consent (but less easy to prove in court).

    - Possible to upload scanned consent forms and store those with patient notes.

- Processing Staff Data: you have a contract with staff, so it's fine to process their data without any other form of consent. You need to do so in order to fulfil your obligations (eg pay them!). Your privacy notice should indicate what you will be doing with their data.

[2] *Note: there also are arguments **against** asking for consent to process patient data. Asking for consent implies that it can be withdrawn, but once you have medical notes, you have to retain them. Also, it would be easy to overlook that a patient had NOT given consent, with the potential for an awkward situation once the notes had been created. And, it's more paperwork!*

Privacy Policy:

- must be easily accessible to patients (on website is fine – you DO NOT have to have it displayed on the wall!)

- patients must be made aware of how to find it at the earliest opportunity (could be reproduced on a sheet when they first present)

- must be clear and simple to understand, and separate from your Terms and Conditions

- must show:

    - how the data will be used

    - whether you may wish to use their personal data to contact them in order to promote other services

    - how long the data will be retained

    - if you intend to share it with a third party, such as a marketing consultant, exercise prescription service, outsourced patient database (eg PPS/TM4/Cliniko/BUPA)

    - Who is responsible for the data (the "Data Controller"), who to complain to and how

Retention of Personal Data (electronically or on paper):

- legal requirement is 8 years or until aged 25 if that is longer. No consent is needed for this as it is a "Legal Obligation" under GDPR. You may legitimately erase/destroy patient data after this period, but there is no obligation to do so.

- you can retain patient data beyond that period without consent. You should state in your Privacy Notice that this is your intention. The GDPR states that retention should be for the minimum necessary period, but this is open to interpretation – if the patient returns after 10 years, it is advantageous to them that you have access to their earlier records.

- After the legal minimum, a patient has the right to ask for their data to be erased. You are entitled to retain sufficient data to record that this has happened.

- Note that the clock does not restart if a patient askes to see their notes, or to correct errors. The 8 year retention period starts from the time of the last medical consultation.

- Your legal liability is general only 3 years after an incident, but may be much longer, or unlimited, in certain circumstances.

Realistic risks:

- The probability is extremely low that patients will complain to the ICO about data being retained for treatment purposes, as opposed to marketing purposes.

- Fines have increased and would be significantly higher than under the Data Protection Act if a breach had occurred.

- If referred to the General Council for other reasons, it is very likely that they will explore your compliance with GDPR (DPA 2018). If you are not compliant, they are under a legal obligation to report this to the ICO.

- If you are compliant with the current Data Protection Act, then you are compliant with 90% of the GDPR, and therefore DPA 2018.

Informing Existing Patients:

- You are not obliged to contact all patients in your database/filing cabinets to seek/update consent. However, after 25th May 2018 (when the GDPR enters UK law) you must not send marketing material to those contacts without their consent.

- Writing to patients (or emailing) explaining how the new legislation affects their relationship with you could be construed as good practice. It is also a reason to contact your list, which effectively could help your marketing.

Security of Data:

- Management of filing cabinets: as long as data is in a cabinet and there's a key that locks that cabinet, that is enough, provided access to the key is controlled (don't leave it where the cleaner can easily find it, for example). If the premises are locked out of working hours, there is no requirement to remove the cabinet keys from the building. Apply a sensible approach to risk assessment.

- An independent practitioner operating in a larger clinic may be responsible for security of their own patient notes – in which case they would need to lock their own cabinets/protect their own computer etc. If the clinic is processing patient information (booking appointments etc), the independent practitioner would have to make this sharing clear in their privacy notice. The independent practitioner's notes could be stored in the same cabinets as others, provided this is made clear in the privacy notice.

- Computers: as long as the premises are secured that would be sufficient security. You can't be wrong because you have been robbed, but it is a requirement to notify the ICO and would be sensible to notify the General Council if computers containing data[3] were stolen.

[3] *Note that data processed by an external source (PPS/TM4/Cliniko etc) is probably NOT stored on local computers. Check with the supplier.*

- Passwords: normal security precautions apply.

Obligations under the GDPR override anything set by the General Councils, in the unlikely event that they contradict.

Amendment of Data:

- Patients have the right to request that you correct errors in their data. This is straightforward when it relates to matters of fact, such as name, address, telephone number, but less so if it relates to what took place during a consultation.

- You are not under an obligation to change records unless you are satisfied that they are incorrect. Historically there are cases where patients have sought to have notes altered to suit a personal injury claim, for example. There has to be a good reason to alter the data.

- You should always note that such a request has been made.

Titles, roles and Responsibilities

- There is no requirement to have a Data Protection Officer. Your business is too small!

- "Data Controller" and other titles: don't concern yourself with these, they are unimportant for small businesses such as osteopaths/chiropractors etc. If it's you that decides what info is collected and how, then you are the data controller – therefore if you're a sole practitioner, it's certainly you. If you're an associate probably not (at least, not in that clinic – if you have your own clinic as well, then you will be the DC for that practice).

Erasing Data

- Patients have the right to request that their data is erased (provided the statutory minimum period has expired)

- You should keep a record that they have made the request and that you have complied.

Transporting notes/data

- Container should be secure and in your position at all times (leaving a briefcase on the tube could prove costly!)

- A secure case, in the boot of the car, out of sight, with a secure lock on it is acceptable

Registration with the Information Commissioner's Office:

- Currently not necessary if records are all paper (which means nothing is processed electronically, even GP referrals, MRI reports etc)

- Under GDPR paper records will be included: if you are the data controller, **you must register before 25th May 2018.** Here's where to go: https://ico.org.uk/for-organisations/register/

- Registration under the current DPA will carry over to DPA 2018.

Transfer of goodwill:

- It's OK for a new owner of a practice to retain patient notes.

- If the sale is of a business, then that business has the consent and this transfers to the new business owner. The "owner" of the data should be made clear on the privacy notice.

- As a sole practitioner, consent to marketing will have to be renewed unless transfer of consent on sale of the business was covered in the original patient agreement.

- A simple option is to include a statement in the Privacy Notice that simply said, "In the event that the practice is sold, data will be transferred to the new owner so that they continue to treat you".

Data Breaches

- Sole practitioners likely to be treated on the same basis as large commercial enterprises

- The gravity of the breach will dictate the penalty.

- Examples of breaches:

    - laptop or a mobile phone left it in a car and stolen. Either don't leave it in the car or lock it in the boot, inside something else.

    - Paper notes disposed of in a waste bin and found by cleaner or another unauthorised person.

    - Talking about a specific patient to other people.

    - Paper notes for other patients left in treatment room unattended while current patient dresses/undresses.

    - Paper notes left in pigeon holes in reception, which are unattended when, say, the cleaner is at work.

    - Previous patient's notes are visible on the screen and overlooked by current patient.

- Need to be realistic: a patient who glances at a computer screen and happens to see another person's name is probably not worth reporting as a breach. Loss of a laptop containing all patient records would definitely need to be reported.

The right of access to data ("Subject Access Requests")

- GDPR (DPA 2018) gives all individuals the right to know what personal data is held on them (right of access). There are no exceptions - Government and regulatory bodies are also subject.

- Time limit of 30 days to comply (reduced from 40 days under DPA 1987)

- If a third party requests patient records (eg lawyer/medical consultant), the patient has the sign a consent declaration (no change from DPA).

- Charging:

    - Cannot charge for providing notes, however you can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.

    - You may 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".

    - You can charge third parties (insurance companies, for example) a reasonable fee. You cannot charge the patient however, even if you know they are asking for the data in order to provide it to the insurance company.

Death

- Patient death: still under an obligation to retain the notes, but family/coroner may seek access.

- Practitioner death:

    - In a corporate environment, successors continue dealing with that information.

    - If you're solo practitioner, then spouse or partner has to deal with matters. But realistically, you're dead anyway, so unlikely to suffer a significant penalty!

Information that patients submit via text:

- Still counts as processing information personal data, so has to be secure.

- Phone (or iPad etc) should have a password on it and the information kept securely on your phone or in the cloud etc. Good practice to transfer info to patient notes, then delete the text.

Use of WhatsApp to communicate with other practitioners

- WhatsApp is now used in medical environments

- If sharing info with professionals outside your own practice, specific patient consent would be required

- Within your own practice, as long as it is covered in your privacy policy, it would be acceptable.

Third party compliance (eg PPS, Cliniko, TM4 etc)

- The law requires them to be because they're processing data about people in the EU

- You need to assure yourself that they are compliant, however – this should be obvious from their own Privacy Policy/T&Cs

- You can always ask them!

Contractors (eg IT consultants) should sign a non-disclosure agreement (also known as Supplier Data Protection Agreement)

Portability of Data

- Patients have the right to insist their personal data is transferred to, say, a new practitioner

- Practitioner should ensure that signed authority is received to do so.

- 30 days is the maximum time allowed to comply. Perfectly reasonable for the requesting practitioner to ask for notes in a shorter timescale but you aren't obliged to do comply.

Complaints

- If a practitioner is a subject of a patient complaint, the regulator and any defence counsel will need access to clinic notes

- there's a statutory provision that gives them the right to access that information for that purpose. In law, if you're subject to a complaint and you need to take appropriate advice, you're always entitled to refer to that information as part of your defence.

- The regulator will seek permission from the complainant to have access to their medical notes.

COMMUNICATION

It's OK to send appointment reminders without consent (it's "Legitimate Interest")

It's OK to send information to a patient regarding their medical problem, or a specific enquiry they have made (again "Legitimate Interest")

It is questionable that you can send information NOT relating to the above (eg a newsletter with no info on those issues), but it is a grey area. Be cautious and think about how you might justify this as being in the patient's "Legitimate Interest".

To be on the safe side, you should get explicit consent from your patients that you can send marketing material (but refer to it in a more appealing way than that!)

Christmas cards to your patients are technically a breach of confidentiality! But who is going to complain (top tip: avoid sending to patients with the name E. Scrooge)?

Using email:

- You are not obliged to use encryption software. Take a sensible approach to risk.
- ICO confirm that emails are "reasonably secure" in their own right.
- If you password-protect attached documents, that's better still. Send the password by a different means (phone).
- In any case, it is fine to send emails with clinical information on them if you have the consent of the patient

MARKETING

Marketing to patients:

- you must get explicit, clear consent. Pre-checked boxes are not allowed.
- It is not sufficient to have a single signature at the bottom of a page where general consent to treatment/correspondence about appointments/marketing is assumed.

Marketing to prospects (ie not yet patients)

- You must have consent to send marketing information (or to use their data in any other way). This means you cannot, for example, buy data lists and email to that list.
- Facebook Ads, Google Ads: Data collected from these ads has been freely provided by the prospect, so you can use it for the purpose of whatever was advertised (again, be careful about assuming that you can send unrelated marketing)
- Consent boxes must not be pre-ticked.
- Facebook Messenger (via Manychat):
    - A patient responds to a FB post, which links to ManyChat using FB Messenger.
    - Manychat ensures that the person opts in, using text you have provided, and records that opt in.

- You can then send them information **related to that enquiry**. But, as above, be very cautious about sending advertising/info relating to other matters. Just because they asked for info about sciatica doesn't mean you can send them your newsletter!

- Make sure that there is a very clear and easy to understand way of opting out: somewhere in the conversation you should let them know that they can type "stop" or "unsubscribe" to call a halt.

OWNERSHIP OF DATA

This is not a GDPR issue, but was raised during the discussion and will be important for many practitioners (especially principals of large practices). It concerns the "ownership" of patient notes. Can you insist on taking with you the notes and data of patients you have treated when you leave a practice?

- If you are one of several practitioners at a practice, where the practice itself acquires, processes and allocates patients, then that practice *probably* "owns" the data. This is potentially a disputable area however. It is a legal issue of whether the contract is between the patient and practitioner, or patient and practice. This should be made clear in practitioner/associate contracts.

- If you rent a room, and patients are yours alone, then you are the "owner" of that data.

- If you are *employed* by the practice, then the notes are definitely "owned" by the practice.