Academy of PHYSICAL MEDICINE

Transcript

The General Data Protection Regulations

With Simon Butler and Paul Grant

Steven Bruce:

The reason we're doing this broadcast is because there is a lot of information out there about GDP and lots of osteopaths and chiropractors and others are worried about the implications for their practice and the workload that it might entail. If you know anything about me, you'll know that I hate bureaucracy, I hate people spreading fear and misinformation, and what I'm determined to do this evening is to give you the simple guidelines in what you have to do in order to comply with the GDPR and I think you'll very be reassured to find that it is very, very little extra work in most cases.

On the website this evening, below the video pane, there are three documents. We have a document, which gives you a checklist for your staff and what should be done for complying with GDPR. We have one, which shows what information you should give to patients, and the other one is a summary of what should go into the privacy notices. It's information, which has been culled by me from the ICO, the Information Commissioner's Office website and they are draft documents. What's going to happen with those documents, which by all means open them now and use them as a guide to formulate your own questions as we go along. But what's going to happen with those documents is as we update them and finalize them and get something, which we think is just what you need, we will be pushing the updates to everybody who watches this broadcast and everybody who watches the recording.

As always, our aim is to try to make your working life as easy as possible and take away the fear and all the other problems that come with great bureaucratic tangles like the GDPR. Anyway, I hope that's reassured you. By all means, as I say, get those documents down now because it may help you follow through what we're talking about this evening because as you know, we don't do PowerPoint in the Academy and all the other broadcasts that I've seen about GDPR are PowerPoint heavy, deadly boring, and some of them downright misleading. We're going to have a good old chat this evening about the GDPR and all the things that we say will of course be typed up into a nice, concise summary document for you so you've got a good record for CPD but also an excellent guideline for compliance. Enough with

that.

Let me introduce my guests. First of all, I have Paul Grant back with us. Now, Paul is a solicitor and an osteopath, which is a curious combination. He is also the chairman of the trustees for the College of Osteopaths and he and I have been colleagues and friends for many years now. You might remember that Paul was with us when we talked about consent in a different context a few months ago when we were talking about informed consent with our patients. Welcome back to Paul.

But my principal guest, my prime guest this evening is Barrister Simon Butler. Simon, welcome to the Academy for your first time. Nice to have you with us.

Simon Butler: Nice to see you.

Steven Bruce: Simon has been a barrister since 1996. He has a number of areas of expertise including local government and healthcare and in particular primary care healthcare. He is very well versed in the ins and outs of the GDPR. If you look at his website, which is a smart website, I must say, he prides himself on being able to deliver information to his clients in a clear and easy to understand manner, which I think is what we all want because we don't like legal jargon, we don't bureaucracy, we just want simple facts and figures to tell us what to do. I hope I got that all right.

Simon Butler: Thank you.

Steven Bruce: When I sent out that little briefing note earlier on today, I kind of divided what we were going to talk about into a number of categories. I thought we ought to talk about the GDPR as it relates to:

- storing patient data or storing data generally, whether it's patient or staff data,
- communication with patients, and then
- marketing, which seemed to me to be the three distinct areas of application of the GDPR. Of course marketing 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.

I think it's that marketing area, which is 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 the GDPR is and why we've got it?

Simon Butler: Yeah, the changes to the GDPR was to simplify the process. It's a European directive so it's to simplify it across Europe so all citizens were aware as to their rights and obligations as to data. There's so much data out there now and how process it and how people are using it that the whole objective is to try and keep it in a modified form so that people know how they can access it, how people are

entitled to process it, retain it, and when they're entitled to erase it. The document and the regulations in itself are detailed but an awful lot of it would not apply to most practitioners. It applies to large corporates, Facebook, companies that are processing information what we call data, what we buy, what we sell through different websites and using that for marketing purposes.

For your members, the most important thing is, in my view, is for the current patients of course they have the current information. If they are still seeing those patients, then they will need to go through a new consent process and that consent process is different to what you and Paul have discussed about consenting to treatment. But as they go through that process, on a standard consent form, the form can contain the information that you need to comply with these regulations and the most important thing is, is to notify your patient what information you're going to store, the reasons for storing that information.

The point you made a moment ago, if you're going to market to your client base, I'll call it that way, then you must be transparent and say to the patient, when I retain your information, it's not just the treatment I provide or the symptoms but your name, address, email address, mobile number. I may wish to use that by contacting you to promote other services or if intend to use that information to hand it on to a third party, such as a marketing consultant I'm going to employ to come in to market my services, then your form, which you get your client to sign, must state that because they are consenting to what you're going to use that information for. You may use it for a very limited purpose and some others in a larger practice, may want to use it for another purpose.

Steven Bruce: In my own practice, when a patient comes in, they fill in a standard paper data form, which has their name, address, date of birth, contact details and on that form we have two lines, one of which is I'm happy for you to contact me about appointments and other things related to my treatment and another one, which says I'm happy for you to send me other information such as newsletters. Both of those have an empty checkbox next to them so they can decide whether or not they want us to do those things. Is that compliant?

Simon Butler: That would be compliant. You have to explain the information to clients. You don't have a fallback position on a standard form. That is by signing this document, you're confirming, you're agreeing to all of this because that would not be compliant because most patients who read a form will just sign it and they haven't read it in detail. The exercise has to be that you're going to have to have something on the form where the declaration as to the information that you're storing, the information you're obtaining is a signature separate to the signature for other information on the form that you may be seeking their consent. I wouldn't suggest you just have one signature on the form so you're consenting to treatment and you're consenting to data information. I think the two are quite separate and you need two separate signatures.

Steven Bruce: There was no consent for treatment on this because that has to be done at the

time of treatment. This was consent to market to them and to tell them about appointments.

Simon Butler: If it's on the same form, I think you need separate signatures. There's nothing wrong with having it on the same form with a new patient arriving, whether you're dentist, osteo, or doctor and saying, as part of the consent process, now I've just met you, you're consenting to allow me to treat you, you're consenting me to allow me to go through this process but furthermore, I now want to go through the data protection process with you because the information I'll obtain from you, whatever that may be, the patients may talk during the procedure, issues may come to the service during the process, which become confidential and may implicate or become important and therefore, you're consenting for me to record that data and store it for this particular purpose.

Steven Bruce: Would we, on that form, have to say that this data will be retained for whatever period we're going to retain it for? Now, I know you're about to say there's a mandatory period you've got to retain medical notes for but we'll come to back to that in a second. Would you say on that, I intend to keep this information indefinitely and the legal minimum is eight years?

Simon Butler: Absolutely. As with anything, the statutory regime states you would need to keep it for a set period and you know that's eight years. There's nothing wrong with you retaining it for a longer period. As long as it's stored properly, there's nothing prohibiting that. It just gives you the right to delete that information after a set period.

Steven Bruce: I want to clarify this because the really important that came up in that discussion we had just before went on air. The fact that you have information on your computer or in your filing cabinet does not in itself constitute processing data, which is what the GDPR relates to. It's only processing if you're using that data. The fact that I've got 5,000 records in my filing cabinets, I don't have to write to all them and get new permission.

Simon Butler: No, you don't. If you currently have patients who you have not seen for a significant period of time or even for a period of time beyond 12 months, you don't then need to send them a form saying I now need your consent for this information. What you do need to do is for all new patients or you could write to the old patients stating, this is what I now need to notify you of and if you intend to return to my practice, then I would need you to sign up to a new consent process for me to retain this information, deal with it in a particular way. But there is no obligation to old clients or old patients, whatever you want to call them, writing to them and saying you must now sign this form.

Steven Bruce: Let us say I had a patient who came in to see me six months ago and may well come back in next month for routine treatment, can I just wait until he comes in to do another-

Simon Butler: You can.

Steven Bruce: I don't have to send him-

Simon Butler: No, absolutely not. You just wait for the patient to return.

Steven Bruce: What was that brainy idea you had a little while ago about writing to patients?

Simon Butler: Well look, some people may wish to if they've got a client database. They may wish to write to them as part of a letter just updating on the new process out of good practice, you don't have to but if you do, you write to them and say, if you do return, I just want to put you on notice. There is a new process that we have to go through because sometimes the public, we may be aware of this process, but when a patient has been seeing you for a period of time, and I know because I use osteopaths frequently, you go into an environment and if you're not a lawyer, if you're not familiar with this process, they'll be wondering why you're going through this with me.

In fact, what is it you intend to do with this information because it would be a bit strange to the public to suddenly have somebody say to this, could you sign this form confirming I can use this information for this purpose and for this purpose, and I can only do it for this. I think most people just go for a treatment and consenting for that treatment. For your members, you'll have to get into, hopefully, in a very short format just explaining why you have to do it.

Paul Grant: As I said, just to emphasize, we're here not to make your members worried at all, but it comes under the rubric of a privacy notice, which actually explains it. It is important, I'm just underlying what Simon says, of having a proper document, which I'm sure somebody can formulate, setting out all these requirements as how you're going to process it. It says here your lawful basis for processing it, your data retention periods, and they have a right to complain to the ICO if they think there's a problem with the way you're handling their data, which is probably unusual that somebody would make such a complaint.

Steven Bruce: That's a good point you've made there, that's quite a useful thing, isn't it? The chances of people complaining about what we do with data in terms of patient data being retained for treatment purposes, not marketing purposes. You've got more experience with people who have complained about these things but it's very rare isn't it? If all we're doing is hanging onto notes, people are going to complain if you do something they don't like with their data. If you're just hanging onto notes, they wouldn't even be aware that you were doing it in most cases.

Paul Grant: I must admit, I haven't come across such a case where people have complained about that, no.

Steven Bruce: One of the worries people have is that if we are outside the GDPR for some reason, we're immediately going to get fined 4 million euros is it or 20%, which of course

again, we aren't going to be fined those sums but the sums that we could be fined are much higher than they were under the Data Protection Act. Is that right?

Simon Butler: They are, they have increased and the fines would be significant if it was found to be a breach. If a member of the public, a patient, a member of the public, whoever decides to ask for information from one of your members and then wants to know why you haven't done this and why you haven't done that and sees to make an issue of it, it could end up being a very costly exercise. I'm not saying to members, alarming them saying they're going to fined huge amounts but sometimes if you get a difficult patient who decides to refer you on to your professional body. Not to say there's any merit in the complaint, but if you happened to be there and then the investigating officer asks your member, by the way, could you provide all these documents to confirm you've complied with such-and-such and you can't produce that, under the new regime, your professional body is under an obligation to refer to the commissioner. It's as simple as that.

Steven Bruce: Right, and it's the commissioner who would take action.

Simon Butler: The commissioner who take action, investigate, and decide what the appropriate punishment should be and that would depend upon the seriousness of it.

Paul Grant: It can work the other way, can't it with regard to advertising in the same way. If someone makes a complaint to the ASA, the Advertising Standards Authority, they have a problem. They have no teeth as one knows and they go to the Office of Fair Trading but it could work backwards. They can refer to GOSC to complain because obviously, as you know, under a standard D8 of the code of conduct, you respect your patients rights to privacy and confidentiality, etc. and therefore, you've got to be concerned if it's the other way around. The ISO could therefore report. I not here to worry your members but they should be careful.

Steven Bruce: I think perhaps we should have started with this. If chiropractors and osteopaths and physiotherapists are compliant with the Data Protection Act, which they all should be, then they're compliant with 90% GDPR anyway in terms of handling patient data.

Paul Grant: Absolutely.

Steven Bruce: There are very few changes required and we'll come on to what changes perhaps are needed shortly. Before we even came on air, I had a whole heap of questions so can I start with one of those now before we move on? Jeremy has asked about the security aspect of patient notes recorded on card or paper kept in locked areas at night but aren't we obliged to lock these away more securely in locked cabinets? How do I manage dozens of cabinets holding thousands of paper notes?

Simon Butler: The standard rule is, as a barrister I am required to secure my client's information. As long as you have it in a cabinet and there's a key that locks that cabinet, then you're perfectly fine.

Steven Bruce: Even if the key is left in the receptionist drawer next to the cabinet?

Simon Butler: It depends if somebody can access it. Some of your members may work from home and therefore, they would have to remove the key if a member of the family or a visitor could open it and look at what is in there. It depends on the person's personal circumstances. If you're in shared premises and of course you've got a cabinet with private information and the receptionist or a cleaner or a contractor could walk in and open it, then of course you're in breach so you'd have to keep it locked and hopefully keep the key on you.

Steven Bruce: Right. In a previous discussion on this, we were told that it's not sufficient to have locked cabinets. You have to remove the keys from the premises every evening when you leave. I think we're talking here about a practice, which is a standalone practice. That struck me as being a bit daft. If the practice itself is locked and alarmed, then what's the point of removing keys to cabinets because if a burglar gets in, they're not going to be put of by a filing cabinet lock.

Simon Butler: No, it's people's personal views as to how they want to store information. But as long as the building is securely locked, of course you don't need to take the key out of the cabinet and have that locked at the same time because it's already securely locked. One has to risk assess what's the likelihood of somebody accessing this information in a particular way and everybody will be different because they work in different premises, the risks may be greater. If there's a history of somebody trying to break into the premise, then of course you may need to take sufficient measures because you've got a history in the area of break-ins of somebody trying to target your property. I think it's a personal risk assessment to determine security.

Steven Bruce: Yes, and again, we don't want to get into the weeds of this. I think for most people, if the practice is locked and possibly alarmed, then probably that's a reasonable security measure, isn't it?

Simon Butler: Of course, it is. They're more than sufficient.

Steven Bruce: Because I've worked closely with the police in the past, and they've also told me that once a burglar is inside a building, locked doors are often not relevant because they can break anything down and no one will know about it.

Simon Butler: The other point is that at the end of the day if you take the count of a cabinet, depending on how big the cabinet is, what stops somebody breaking in and removing the cabinet.

Steven Bruce: Anyway, we've done that one to death, haven't we. Earlier on, you were mentioning what about computers. If people are using electronic notes and all those notes are recorded on the hard drive of their computer, then that is a very portable and burglarable item, if that's the correct word.

Simon Butler: I think that's right but I think that's the same for doctors, dentists, any primary practitioner who is now storing information on computers. Anybody that breaks into the building can remove the computer and the hard drive. In my experience, it has happened where people break in, drug addicts, whatever to a practice and they decide to steal something and then sell it afterwards. As long as the premise is secured and you've taken those steps and as long as you back up the information somewhere, iCloud, hard drive that's secure, then that would be sufficient. You can't be wronged because somebody is going to come in and break in and decide-

Paul Grant: And obviously passwords as well.

Steven Bruce: Yes, I was just going to say, presumably you would be expected to put a reasonably secure password on a computer so that people couldn't just type in “password” and get into all your patient data.

Simon Butler: Absolutely, but most computer software we all have passwords and it's very difficult for somebody to access it unless they're a whiz kid, and if they are, they're going to access it whatever password you put on it.

Steven Bruce: That's always puzzled me as well. If somebody stole my computer, I would definitely say that it had a really secure password on it, who is to prove that it didn't?

Simon Butler: You could never prove otherwise.

Steven Bruce: Excellent. You heard it here from a barrister!

Simon Butler: You're absolutely right with laptops and software now, we all have passwords. It's standard, I think most software requires you type in a password anyway. In my practice, we have computers and laptops in our room. If somebody is going to break in and steal that, what can I do about it? I'm not going to take my whole desk and computers home with me.

Steven Bruce: You did say earlier on that if your computer was pinched, you should report it immediately to the ICO.

Simon Butler: You are obliged to, you have to. If you're aware that information has been stolen or taken or compromised, you're under a duty to notify the commissioner and you're under a duty to notify your client base.

Steven Bruce: Right. When you say the commissioner, we're talking about the Information Commissioner's Office.

Simon Butler: Yes, sorry.

Steven Bruce: Not necessarily the GOSC but would we have to tell the GOSC as well?

Paul Grant: Interesting question. Actually, I haven't thought that one out.

Simon Butler: Or the General Chiropractic Council, obviously.

Paul Grant: In theory, if a potential breach, I see no reason why you shouldn't as just done to precaution. You would write to them and say, I have told the ICO but as a matter of caution, I'm telling you as well so it's on the record so they can't complain later on if the patient then makes a complaint. I think the answer must be yes, provided you'd use guarded language.

Steven Bruce: I've got a really long question here. I really welcome questions but it's nice if they're short and concise. This one says, what happens when the General Council rules and the GDPR don't tally? Of course, I realize that the former are professional rules and the latter are statutory requirements.
Aren't the GOSC regulations statutory as well because it's a statutory body?

Paul Grant: The answer is the rules come under the process of the Osteopaths Act 1993 or the Chiroprctors Act 1994 so far as people are osteopaths or chiropractors and they produce regulations and codes, which are all under section 19 of each of the acts, which say that they can, it's like secondary or delegated legislation so therefore it does come under the rubric of the particular act.

Steven Bruce: The answer to that question was yes.

Paul Grant: The answer is yes. I'm a lawyer, I have to earn my money somehow

Simon Butler: Also, legally as long as registrants comply with the statue of obligation under the GDPR, your professional body cannot override that. As long as you're compliant, you're compliant.

Steven Bruce: I think this question is mistaken. I think it's Matthew, he says the GDPR says that the period for which personal data is stored should be the minimum and that time limit should be established by the data controller, definitions again, by the osteopathic standards and therefore the chiropractic standards as well saying we have to retain patient records for eight years. I think there's a bit of confusion there, isn't there? Because there is a legal requirement to maintain the patient records for eight years after you last saw the patient or up to the age 25 if that's longer. That doesn't override any requirement to keep them for the minimum time necessary. But you were saying earlier, it actually doesn't matter if we keep patient records indefinitely in case the patient comes back.

Simon Butler: There's nothing wrong with that. There's nothing prohibiting you retaining that information beyond eight years.

Steven Bruce: We can say that is the minimum necessary because if they ever do come back, we want to know that patient history.

Simon Butler: The requirement allows you to erase it after eight years but there's nothing to stop you-

Paul Grant: Can I raise two points? One is, if you like at the website for the General Osteopathic Council, they do link themselves up with the ICO so there is a synergy between GOSC and the regulation and the Data Protection Act, etc. and GDPR. That's the answer to that one. I just wondered, the right to erase we say doesn't apply to medical notes. But what would be a question to Simon, I'd be unfair, I should really be able to answer it or maybe there's no answer to it. After eight years, there's no longer that obligation to hold it and the patient then writes in and says, I know 20 years ago I saw you and I want you to erase those notes. How would we answer that? I'm asking myself, I'm not sure how we'd answer it.

Simon Butler: I think if the obligation, it clearly is that you must retain for 8 years, and therefore, the patient after eight years invites you to erase it, I think you need to. I think that would be proper practice because that would their right because the statutory period has expired.

Steven Bruce: But I would certainly keep a record that they asked me to do that.

Simon Butler: Oh, yes. Definitely. You'd have to retain that to make sure. But the other point I just want to mention, which is important to your members, is that if a patient contacts you and wishes to correct your records, if they say, by the way, I'd like to have access to my records because I'm pursuing a personal injury claim or my doctor says I've got a condition and the consultant wants to look at what I've been complaining about and they read it, then they do have a right to write to you to say, I'm not sure that's correct. I didn't say that to you, could you please correct it? It's not to say you are under an obligation to correct it, it's a matter for you as the practitioner to determine whether or not the patient did say that to you.

Steven Bruce: Yes, business also to record the request to make sure .

Simon Butler: Yes, absolutely because sometimes in my field as a lawyer, you don't come across this as osteos. We live in a murky world where people want to manipulate, change information for their own gain or benefit and therefore, you've got to be very cautious about somebody writing to you and saying, I want full access to my records. I want to check what I supposedly said. As I said, if they're trying to use it for another purpose, for a claim, for benefits, and it doesn't tally with what they put elsewhere, it doesn't mean you should amend it. You've got to be quite cautious about that because you could end up being implicated in some form of conspiracy to benefit somebody. There's got to be good reasons to correct it and that's no different to hospital doctor's records. There's got to be a good reason to do so.

Steven Bruce: One of the patient rights, one of any person's rights is that they can correct data that's held by somebody but only if it is incorrect and you agree with it.

Simon Butler: Yeah, if they can prove it's justified and they can show to you that my date of birth is wrong or my address is wrong. But when it comes down to what they discuss with a practitioner during the treatment, I think it's very rare that a treating practitioner will get information incorrect. Doctors do in hospitals in A&E when they're overworked but not in a therapeutic treatment room where you're one-to-one and having a conversation.

Paul Grant: That must be like a date of birth, things like that.

Steven Bruce: Simple stuff, factual stuff.

Paul Grant: But your diagnosis or your treatment plan, that can't. That's your own personal ...

Simon Butler: I think that's just very important to really emphasize that because you don't want somebody doing that and then you correcting everything and then a year later you have a claim made against you saying, you did this to me. Then of course, you've erased all the records, which would allow you to prove otherwise.

Paul Grant: Absolutely.

Simon Butler: Is to be very careful.

Steven Bruce: We have one that says, hi Simon. Now, it's very kind of them to say hi, Simon but they don't tell me who they are, which is disappointing. They say, if the patient does not consent to store data, where do we stand with obtaining patient data for case history?

Simon Butler: That is interesting because if the patient that will come in to see you, literally refuses to sign a consent form saying I'm not going to permit you to store any information or data concerning me, it doesn't mean you can't treat the patient because of course, they're still consenting to the treatment. But it just means you're going to be in difficulty with the information that you have to weigh up as again, as a practitioner, do I want to run the risk of treating somebody by them refusing to permit me to then process the information they provided to me to undertake that treatment. It's a bit of a bizarre situation.

Paul Grant: I wouldn't go ahead with that patient because I would say, this is an obligation, it's confidential, etc. I certainly wouldn't. It's recipe for disaster if they make a complaint later on and you haven't got a record før it. It offends the GOSC D8 as well.

Steven Bruce: But also, I would as a practitioner, I would simply say, look, I have a legal obligation to record what happens to you and keep it for eight years and I can't treat you unless you let me do that.

Simon Butler: I think you can be robust in that way. It's not to say you can't treatment because

the information you then obtain through the treatment, you're not processing it because you have to hand it back to the patient. I just don't think it is good practice. I think you're putting yourself at risk because this is a simple process. As we all do, we go and see a GP, we know that information is processed. I end up in A&E because I've been hit and I've got injuries. That information is going to processed.

Steven Bruce: That was some discussion in a previous webinar that I've seen about the GDPR. By attending for treatment, implicitly you are giving consent to give keep your data.

Simon Butler: You're not. That changed under this. That is a fallacy. You cannot for one moment imply anything now when it comes to consent. It has to be absolutely clear to the patient that you must consent to me, retain this information. Of course, there are situations when I'm put in a different scenario with doctors and you're unconscious, you go into hospital. You can't consent, you just get on the treatment. That's provided for with exemptions anyway. But when somebody is actually coming in to treat and you're obtaining information on this and a discussion about things, you need their consent to process that information and the reasons why you're going to retain it. In my view, most people would consent to that because it's better for them and the ongoing treatment and their own health because how is an osteopath going to remember every single patient they treat if they don't look back at their record?

Steven Bruce: Let's move on. I've got another question here, which says, we're getting into the business of definitions here, which I don't want to dwell on but this person asks, "Can I be my own data controller and if so, do I get a hat? In a small practice with just my partner and no other staff, it would appear I have no other choice." Data controller is effectively just a title isn't it?

Simon Butler: Oh no, I wouldn't get bogged down by titles. At the end of the day, if you're a sole practitioner and most people in the healthcare sector providing these wonderful services will be a sole practitioner, then you can give yourself whatever names you like. You are a sole practitioner and you will just comply with it and process the information and obtain the consent. I wouldn't get too bogged down. If you want to drop a policy and say, I am the data controller, I am the data processor, I am the complaints data officer, so be it. You can be anything you like.

Paul Grant: Exactly. In so far as looking at what the osteopathic account says, data controller is people in organizations who process personal information are data controllers and must register with the Information Commissioner's Office.

Steven Bruce: We all have to register anyway. [crosstalk 00:31:36].

Simon Butler: You are registered, we're all registered.

Paul Grant: We're registered with the ICO, that's right.

Simon Butler: One thing I just want to mention is, there has to be a positive act of the patient opting into this. There's no default position. You can't put on the form some default position that by attending the practice and have treatment and by handing this form to you, you've accepted it. That is not permitted. There has to be a confirmation and a signature that I am consenting to this.

Steven Bruce: I think one area I would like to clear up, if you want to see all the definitions and the titles and so on, data processor, data controller, data whatever else it might be. They're all somewhere on the ICOs website but as Simon said, it's probably not relevant to us in small business. But there is the issue, which has been raised in previous discussions about this of the data protection officer. People have been advised to find a data protection officer and so forth. Actually, we're not required to have one, are we? We're only small businesses.

Simon Butler: No, no requirement at tall.

Steven Bruce: Good, that answers that question. If you were thinking of appointing a data protection officer, you're entitled to do it, but you don't have to do because we're too small for that. Question here, what happens is a practice is transferred to another practitioner or the goodwill of a business is sold? Does that have to be anticipated with the original data consent form? What happens to the collection of the original personal data, which predates the GDPR? What do we have to do if we sell our businesses off?

Simon Butler: Right, well so far as the consent of data is concerned, it depends upon how you structure your business. If you're a sole practitioner, then the consent will be with you as a sole practitioner. Some may operate through a company, through a partnership. If you're going to sell your practice, then of course if you're gonna transfer data. If you're a sole practitioner, Simon Butler, and I'm gonna sell, what is it you're selling? The goodwill is the patient list, it must be. Therefore, if you're gonna sell that onto somebody else so they can contact them, then unfortunately, if you haven't provided for that in your original consent form, you're then gonna have to write any single patient stating, I'm intending to sell my business and I intend to provide and transfer your private information to this person. Can I have your consent to do so?

Steven Bruce: But a simpler method would be in your information to the patient to include in that. I think there is a section for transferring to outside agencies, isn't there? If you had a statement that simply said, in the event that I ever sell my practice, I will transfer your data so that they continue to treat you.

Simon Butler: Yes, absolutely. Or you'll want to put in the, you could obtain the consent from the patient again anyway, but you could put it, should the patient be treated by a third party practitioner, and there's a request made for your information to understand what it is they're treating the for. I have the consent to disclose that information to a doctor, a consultant, or to another osteopath.

Steven Bruce: I'm gonna move on. You were worried we wouldn't last 90 minutes and I have got a yard-and-a-half of questions and we haven't even talked about the topics that I had in mind. There's a good question here. We've been talking about paper forms and people putting signatures on them but in so many practices now things are electronic and you might be putting your data iPad. How would we go about getting legal consent on the GDPR if it's electronic.

Simon Butler: It's no different because now what you have to do is an accepted practice if you're online with a standard form, you will put in on the signature, you'll type in the patient's full name and then they'll be a box next to it confirming that they've agreed to it. That's it, those are the standard electronic forms.

Steven Bruce: It's okay then for me to record that this patient specifically agreed to this statement. It doesn't have to be the patient signing it.

Simon Butler: You are signing it because the patient will put their name into a box. You don't have to have an electronic significant. They'll put the name in. You see it on government documents now when you're emailing things. Just type your name in and obviously you tick the box and I confirm I'm giving consent to this. That is permissible. Obviously, the fallback position will always be if the patient says that I didn't tick that box and I didn't consent to it, then obviously it's a disputed fact between the parties. But that's a fact of life. As long as the practitioner knows they have consented to it and they've inserted their name to it, I think you're perfect fine. That's not a problem.

Steven Bruce: I think with modern clinical software, once you upload that form to the software, it can't be amended afterward so there is some reasonable robustness in the evidence that it was ticked at the time and if that is your normal policy then ...

Simon Butler: It's always a question. There is no difference to a dispute between a practitioner and a patient and the patient saying, well, you did this to me. Well, I did not. It's a dispute of fact and one would have to resolve it. If it's your practice and you have a policy if that is what you do and you've explained it to the patient and the patient has inserted the name and ticked the box confirming that's happened, you'll be perfectly fine.

Steven Bruce: Okay. More questions. Is there any concept of good intentions in the application of the GDPR. For example, would a sole practitioner doing their best to comply be treated on the same basis as a large commercial enterprise with a dedicated legal team in the event of a breach?

Simon Butler: Sadly, putting aside how the breach arose, I don't think It would make much difference to somebody at the Commissioners office investigating it. A breach is a breach. Of course, one has to look at the gravity of the breach and they look at that when imposing a penalty. But there's no different standard to determining whether a breach has arisen and the reasons for that breach.

Steven Bruce: The difference is likely to be in a big company like Facebook, for example, it might be five million records that have been disclosed. Whereas, in a small practice, it might be a couple of records or a half dozen records.

Simon Butler: Exactly, and the penalty, they tend to assess them according to the significance of the breach and of course the person who has committed that breach.

Steven Bruce: Right, okay. Are there any exceptions to the right to access your own data. This is Matthew again. He says, "I'm thinking of the one the general osteopathic council uses but claiming that certain retained data is part of a regulatory process and so is exempt." I'm not aware of what that might be.

Paul Grant: I don't understand that. They can't mean a finding, a disciplinary finding. There are certain time limits where they keep that information but that doesn't relate to the patient per se. Could you argue a disciplinary finding is information, which comes under the GDPR?

Simon Butler: It is.

Paul Grant: It is, and therefore it could be.

Steven Bruce: In any case, there's no difference to what was under the Data Protection Act, which is currently in force, is there? It's the same rule, isn't it?

Paul Grant: It must be right, it must be right. I don't know. There must be more to that question. Maybe you can clarify that.

Steven Bruce: Whoever asked that, if you want to clarify that a little further, that might be helpful. Let me have another question. Is the government and the DHSC in particular subject to GDPR. For example, with respect to misuse of patient data relating to care and subsequent attempts to make use of patient records.

Simon Butler: They are.

Steven Bruce: Everyone is subject.

Simon Butler: They are subject. In personal injury clinical negligent practice, when we're suing actions on behalf of patients, when we request patient records, the patient has the sign a declaration consenting to the legal practitioner obtaining those records. You wouldn't disclose anything unless there's a signed declaration from the former patient saying, I give you permission to disclose the information to a third party. That's all part of this process.

Steven Bruce: Just taking you back a little bit, we talked quite a bit about breaches, which was right at the end of the list of things I wanted to talk about it. What exactly do we mean by a breach under the GDPR, a breach of data security.

Simon Butler: A breach would be, I'll give you three examples. An osteopath decides they're going to leave their practice. They put all their patients' information on a laptop or a mobile phone and they've left it in their car and somebody smashes the window and takes it. That's a breach because you're supposed to secure and make sure that information is secure. Any way you can secure it is by not leaving it in the car and of course, locking it in the boot inside something else to make sure it is secure. That would be considered a breach.

The second breach could be for those who still use paper. If you happen to dispose of it in a waste bin or your cleaner does and then somebody picks it up in a high street, that is a breach. The other one, which we all need to be conscious of is an osteopath is at a dinner party and they're talking about a specific patient to other people in the room. That is a breach.

Steven Bruce: That's oral breach, physical breach of pinching a computer, and then the paper notes. What about in a practice, each of the practitioners has a pigeon hole with paper notes for their next patients stacked in the pigeon holes and those same practitioners they'll take that whole wodge of patient notes, case histories, and put them into their tray in their treatment room. While you're taking your clothes off, I have to leave the room but you're left alone in that room with a whole stack of patient notes sitting on a tray.

Simon Butler: That shouldn't happen anymore anyway. It's not permissible but sometimes it does, you're in a rush, you're busy. But you shouldn't allow other people left on their own to access private information.

Steven Bruce: What about the business going stays back in the reception area where there a whole lot of pigeon holes with the case notes out for the practitioners before they arrive. The cleaner is in there hoovering at 7:00 in the morning because this was all done the night before and then the receptionist turns up and all these notes are there waiting for the practitioners. Again, a potential data breach.

Simon Butler: It is a potential data breach because of course, the information is accessible by somebody who has no right to access it so sadly, yes. In chambers where we have papers coming in from solicitors and clients and we have pigeon holes but the room is digi-locked so during the day, the staff, the clerks are working in the room but when everybody has left, it is kept securely locked.

Steven Bruce: It actually looks as though electronic notes are the way to go with this because it'll make securing all those notes a lot easier, won't it? Provided of course, you make sure the screens of your computers are not accessible to the patient left in the treatment room as they get dressed or undressed.

Simon Butler: Yes, there's always going to be moments where there's a lapse. Do you leave a laptop on because something takes away your concentration.

Steven Bruce: Do you have to report that?

Simon Butler: No. I don't accept that somebody is in the patient room just waiting for the next treatment and I don't know, they may have glared at your screen then no.

Steven Bruce: We were saying earlier on that when you go to visit the GP, invariably the previous patient's notes are up on the screen while you're sitting at the desk discussing your case. A nosy patient will probably get some information. What should happen to paper or electronic notes in the case of the death of the practitioner. What arrangements should we make and who should handle them.

Simon Butler: Do you want to answer this?

Paul Grant: You seem already aligned, I'll back you up.

Simon Butler: If somebody has passed away, then firstly, you're still under an obligation to retain the notes but you tend to find that the family may seek access. I don't know, if there's a coroner inquest, the coroner will ask for the notes. But you still have to retain the notes for the set period that you're obliged to anyway even if somebody has passed away. You never know when a member of the family or somebody needs to access them. I've never known, obviously the GP or the osteopath may be notified of the person's death. If you can't contact the estate or relative to ascertain what should happen, my fallback position would always be you hold onto the relevant period and then dispose of them.

Steven Bruce: Doesn't this fall into the category that you described at the beginning. Actually, you're no longer processing that information and there's no law against retaining certainly for the minimum statutory period.

Simon Butler: I appreciate they're not processing the information but I don't know the cause of the death of the patient.

Steven Bruce: No, it's the practitioner we're talking about who died.

Simon Butler: Oh, sorry. The practitioner, I apologize. Sorry, I do apologize. I thought you were referring to the patient. If the practitioner dies, then that's the end.

Paul Grant: Who is asking the question? Are you suggesting in a will, you should put a special will for please retain my notes.

Steven Bruce: If you're a sole practitioner tomorrow and you've got a whole filing cabinet full of notes, what happens to them? Presumably, the still have to be retained for legal reasons if there's something that happens within that eight-year period after treatment?

Simon Butler: Of course, it's an interesting point but generally, if you're in a corporate environment, then the information is there for your successors to continue dealing with that information. If you're an osteopath and you work from home, and sadly

something happens to you, and therefore, your wife or partner has to deal with matters, I'd like to think that they would dispose of the information in an appropriate way but I don't mean to sound flippant when I say this, if you decide not to do so, you're dead anyway. You're not exactly going to end up with a significant penalty to pay.

Steven Bruce: Very, very good point.

Paul Grant: It's a similar situation I think where a sole practitioner solicitor dies. There are rules dealing with SRA. Hopefully, the executor will deal with regulatory authority. Hopefully, if anybody whose family has just died and they [inaudible 00:45:37] osteopath or the chiropractor, they should contact the GOSC or GCC for how to do it.

Steven Bruce: I think I prefer Simon's answer, just die, it's the easiest option. You don't have to worry about all this stuff. Emma, you've asked a question about how are we expected to get in touch with old patients who aren't currently coming in for treatment and get consent and I think we answered that right at the beginning.

Simon Butler: No.

Steven Bruce: You don't have to do that. I can move on. I had a question from Mark about consent for treatment. "Is consent for treatment necessary?" We're not going to talk about consent for treatment because it's a completely different thing to the General Data Protection Regulations and we did cover it in the broadcast that we did with Paul. I would suggest if you want to look at the treatment consent, go back to that broadcast and look at that because otherwise, we could spend another hour-and-a-half talking about treatment consents.

Let me come back to the next one. "Could you please indicate what I should with information that patients submit via text regarding their symptoms and progress, etc.?" We talked about this, didn't we? There are many practitioners who deal with their patients via their mobile phone. It may be their main means of communication and it's also their personal phone. You might send me a text saying, my sciatica has got worse and this has happened and this has happened. What do we do with that sort of information? How do we secure that?

Simon Butler: The fact that it's on an iPad or a mobile phone device it's still processing information and therefore it has to be secure, the data. That means your phone, I would hope, would have a password on it and the information is kept securely on your phone or through iCloud or something. But it's not different to any other form of device or data. It is data, you're processing it, you've obtained the consent to process that information. Hopefully, by that stage-

Steven Bruce: It should be in the consent form. Should we simply say, your data will be processed using my mobile phone?

Simon Butler: No, because I think in a transparent way, any form of processing information is just about your giving me the right to process it that information, store it for a particular purpose. If the patient decides to send you a text message, an email, a letter, or a phone call and it's left on your answering device, it's all processing information and it's about securing it and storing it in a secure manner.

Steven Bruce: And of course by virtue of the fact that they've communicated with you by mobile phone, they know that you're handling the data on a mobile phone, don't they? Could you just write it into their patient notes, either on your cloud systems or your paper notes and then delete the text? Is that a good process?

Simon Butler: The problem is with deleting is, where are you gonna store that information if you want it have it?

Steven Bruce: No, I said you'd write it into the notes. You'd take the information from your mobile phone and write it into your notes and say, sent in by text.

Simon Butler: Absolutely. You could type it up later when you get back to your desk and confirm the patient sent a text and this is the information that was conveyed.

Steven Bruce: Fiona sent an interesting point here. "If someone contacts us to see their notes, change their notes, discuss their notes, that surely re-opens the eight-year rule as it is effectively another consultation no matter how they've done it." Let's say I saw you seven years ago. You contact me and say, I want to see my notes and then you say, I want to correct my notes. Effectively, that's a consultation so the eight-year rule starts again. Is that right?

Paul Grant: I wouldn't agree with that because they are the same notes. The notes are being corrected but they are still the same notes, which have been retained for eight years. Would you agree?

Simon Butler: My view is, is to ascertain the purpose of the visit and to determine why so the question being asked is, if Simon Butler comes in to see his osteopath to say by the way, how are you? How is everything? I just want to check my notes. That is not a consultation, you're not processing information, it's just a request to check your information and therefore, the eight-year rule does not tart afresh then. The eight-year rule will start afresh if I come in for a further treatment because of ailments and then therefore, it starts.

Steven Bruce: I hope that satisfies Fiona's curiosity on that one. How about communicating with other practitioners and doctors? A text would not be secure but what about using WhatsApp? Professionals don't communicate with WhatsApp, do they?

Simon Butler: It's interesting, they do now. It's an interesting question because WhatsApp is a group format, is used in medical environments now, and of course, they all attach to it and they all share information. As long as your patient on your consent form, consents to you using information in that format on a WhatsApp forum, it's

permissible.

Steven Bruce: Right, but you specifically got to say that.

Simon Butler: You've got to get their consent for it.

Steven Bruce: Right, okay.

Simon Butler: As long as they consent to that, then that's absolutely fine.

Steven Bruce: WhatsApp is quite secure, isn't it? I'm led to believe. End-to-end encryption, whatever that means.

Simon Butler: I think it's becoming securer and to be quite honest, in the 21st century, I don't think anything is secure anyway because if somebody wants to access it and they're sophisticated enough, they're going to. But the measures we can take, the standard measures as practitioners that are available to us to encrypt and you have a password.

Steven Bruce: I think this is a very good and very personal question here because this person, again anonymous says, "I and many peers use diary systems such as Clinico or PPS or TM4 or whatever. The information, I believe is stored in the cloud on servers across the globe and the company is not in the EU so how can we know that they're compliant with the GDPR?" They have to be because they're processing data about people in the EU but how do we know that they are?

Simon Butler: It's not a question of how do you know they are as long as the terms and conditions state as a user that they do comply with them, then you're fine.

Steven Bruce: Whose terms and conditions? Theirs on their website?

Simon Butler: The iCloud, whoever you're using as a provider. As long as the terms and conditions confirm, that they are compliant with these regulations, which of course people such as Facebook, WhatsApp, all the big groups now that wish to operate in Europe will have to comply with these regulations.

Steven Bruce: What are practitioners need to do effectively is just have a look at their website or send an email to the person providing it and say, are you compliant with the GDPR and take that answer as being sufficient to protect us.

Simon Butler: Yes.

Steven Bruce: Dear oh dear, there's a lot of questions here, and we're not half way through them yet. "If a clinic is used by multiple, self-employed therapists, and let's face it, most practitioners are self-employed in the way we do business these days, do they each need to secure their own notes with their own key?" I'm picturing here an array of filing cabinets with 3,000 patients notes in them all of which belong to various

practitioners or whoever happens to be treating them at the moment.

Simon Butler: I can answer that very briefly. If you are in a shared practice, if at the time you obtain consent for data, it's made absolutely clear that this is a multi-disciplinary practice and the cabinets are shared and therefore, other third parties, my colleagues, will have access to that cabinet and possibly open a file and have access to that information, that's perfectly fine. But if the patient is not consented to it being stored in that way, then it's not permitted.

Steven Bruce: Okay, that's fairly clear. This is the second comment we've had about practitioners being well aware of patients asking to have their notes changed when it suits them with respect to personal injury claims and so on. It does happen, but you're not required to change the notes just because you've been asked to do it.

Simon Butler: You're not required. Obviously, you do have a reasonable discussion as to why they think you made a mistake. If you accept it was an error, sometimes we're human, we may have made an error. Then both of you will agree to erase that part of the notes. But as a practitioner, if you're absolutely adamant that is actually recorded correctly, then you do not erase it.

Steven Bruce: Matthew again, Matthew says, "But most practice management systems do not store data locally." Yeah, we accept that. "It should be accessed encrypted from the provider's service. If not, the practitioner should probably upgrade."

Simon Butler: It's a very technical question, Matthew. As a barrister, I was looking at storing my clients' data recently with a provider. I had to go through the process of checking it was secured and it was compliant. They confirmed it was secure and compliant and other chambers were using it. Under my rules and under this criteria, I had made the relevant checks.

Steven Bruce: That's what we have to be cautious that we do, is that we've asked them and we've checked. If they tell us it's secure, we can accept that because we've done our due diligence.

Simon Butler: Sometimes there are issue where people use Dropbox and some people would say, I'm not putting information on Dropbox because it's not very secure but Dropbox would tell you it is secure and as long as they're compliant and that's what they represent as being compliant, then I think you're perfectly fine. I think the situation could arise, as has arisen recently, if you take Facebook for example and people who joined Facebook believed their information was going to be secure. There's a potential recently that that may not have been the position. If you are an osteopath and you're using a particular database or a provider of iCloud and it becomes an issue where there may have been breaches by that provider, then of course you need to stop that service and move everything over to a different provider because you have the knowledge and you've become aware that your clients' information could be compromised.

Steven Bruce: Does that pose us another problem? If I say I'm gonna stop using you to handle my patient data, I'm gonna move to this other cloud-based server, is there then a problem of getting consent to transfer that data to another outside authority?

Simon Butler: You don't need to because the consent you've obtained is to process information and store it. You don't need to specify how you're storing it.

Steven Bruce: "Is there a standard for osteopaths to download for patients to sign? Is there a recognized standardized paper note system that includes the GDPR information for the patient to sign? If not, could there be?" That's probably not a question for you, is it? The answer is that the Institute of Osteopathy through their outside contractor is going to provide some of that information. What we will do with the Academy so certainly for the chiropractors and others benefit, we will be doing exactly the same thing. We will provide some standardized documents that you can use and incorporate either into your electronic or your paper note system so we'll make it as easy for you as we possibly can, that being our purpose in life. But at the moment, there isn't, as far as I'm aware any standardized form.

Okay, I don't understand this question. It's from Jason. "Although records have to be kept for eight years, do patients only have a legal right of three-and-a-half years as in the NHS to take up a complaint against a practitioner?" Probably not GDOR related this, but interesting.

Paul Grant: They're thinking about limitation of liability, which is when you can sue for clinical negligence. The usual period is three years but there are much longer periods. If you're disabled, there's no limit. If you're a child, then the three years runs from 21, etc.

Steven Bruce: My next question was is there a time limit for making a claim against practitioners so the same thing applies there but it's GDPR related.

Paul Grant: No.

Steven Bruce: "Can we request verbal consent over the phone to use emails to confirm ..." This is the next part of what I suggested we talk about beforehand, isn't it? One of the things that we would like to do in most of our practices is communicate with you, our patient, to say your next appointment is tomorrow at 5:15 or whatever it might be. Can we get verbal consent to do that? Do we have to have specific consent to do that?

Simon Butler: The consent you've obtained from any patient is capable of being updated and varied at any stage so as long as you get the core consent as to storage and the purposes being used, if whatever purpose that changes during your treatments because that's the way the parties agree that's how you're going to communicate it, as long as you record that change and the patient has consented to it, it's perfectly fine.

Steven Bruce: I can physically write that down and maybe sign it myself.

Simon Butler: Absolutely.

Steven Bruce: Hopefully, that satisfies that question. Bob Allen, hello Bob. Bob says, he wonders, "What would happen if a patient asked me to delete their data before the eight-year time limit is up?"

Simon Butler: You can't do that. You're not permitted to erase the data.

Steven Bruce: No, because there's a legal requirement. But also, could you just go into more? Patients rights under the GDPR are that they have the right to be forgotten. Could you elaborate on what that means and what it means in terms of can they have their data erased?

Simon Butler: They can have it erased but not during the eight-year period. After the eight years, they can contact you if you still have the data, and ask you to erase it.

Steven Bruce: Good, that satisfied that. What about the right to be forgotten? What does that mean?

Simon Butler: It just means you have the right to have your information erased but you have to put in the context. A lot of this information in the GDR, the general data protection regulations, relates to organizations that obtains information about us and they keep phoning us wanting to service and they've got your information because you've gone online at some stage in your life and now it's being shared with so many people, you keep getting calls all the time trying to sell you something you don't want. Therefore, you have a right to ask them to remove that and do not use my information again. That is my instruction. You've not had my consent. That's what relates to. It wouldn't really be applicable unless of course, you get a practitioner who likes contacting their patients all the time promoting services but I can't see that being a common occurrence.

Steven Bruce: Here's a nice easy question for both of you gentleman, "As a sole practitioner, would I need to register with the ICO, the Information Commissioners Office?"

Simon Butler: You do.

Steven Bruce: If you haven't done it, do it tomorrow.

Paul Grant: You should have, yes.

Steven Bruce: Because you are required to do it and it costs, what? 35 quid?

Paul Grant: 35 pounds, yes.

Steven Bruce: It's not expensive.

Paul Grant: There was a ford going around with somebody, I copied the ICO, they said they wanted 100 pounds.

Steven Bruce: It's dead easy to do if you go onto the ICO website.

Paul Grant: Of course, it is.

Steven Bruce: What have we got here? "Other information I have been given on GDPR has said that the right to erase does not mean the notes have to be destroyed but just that there should be no further contact or processing of the data." For example, this was discussed yesterday. So, there is a difference, isn't there, between not being contacted and having the data erased, which is why I asked that question about right to be forgotten. The question is-

Paul Grant: What is the question?

Steven Bruce: The question is from Matthew, I think again. He's a very busy chap.

Paul Grant: Good old Matthew, carry on Matthew, you're doing well.

Steven Bruce: "Other information I have been given on GDPR has said that the right to erase does not mean the notes have to be destroyed but just that there should be no further contact. Is that the case?" You said, no a second ago.

Paul Grant: No, no.

Steven Bruce: If they specifically say, erase the notes and the eight year period has elapsed or they're over 25-

Simon Butler: If the eight years has elapsed, you can erase it if they wish to have it erased.

Steven Bruce: Is there a reason why you shouldn't do it?

Simon Butler: No, again with most practitioners, how many patients are going to write? I'm just thinking of the years of treatments I've had and you see your chiropractor or osteopath and you haven't seen them for a couple of years and you return again. I can't see most people writing after eight years saying, I want it all erased. Why would you?

Steven Bruce: But if they say it?

Simon Butler: If they say it, then by all means erase.

Steven Bruce: I do think and maybe you can back me up on this, that a lot of people are worrying about things, which are very, very unlikely if every likely to happen. Like everything, you can think of all kinds of permutations and scenarios but mostly, this is really,

really simple. Most of it is no different to what we're doing already.

Simon Butler: The most important thing I would emphasize is, is when you obtain the consent, you've got to be transparent about the purposes of which you're using the information for and if you've obtained the consent for that purpose, you'll be absolutely fine, nothing will come of it. It's those situations where you've not gone through that process of confirming to a user of your service that you're gonna use it for a particular purpose and then they find out some third party has obtained the information and they get a bee in their bonnet and it implodes and regulatory proceedings and complaints to the commissioner. That will become a problem.

Over the years in practice, I'll explain to your members where it does become a problem and they need to be aware of is, as I've said, if you get clients who come in and see you for ailments and it's connected with an accident at work or they're trying to bring a claim against somebody and therefore the other party wants access to records then sometimes it can become a bit of a sensitive topic and they'll deny saying things and not wanting things disclosed and it all becomes very personal.

Steven Bruce: Somebody has commented here that, I'll read their question. "I understand that SAR requests will have to be granted free of charge. BP practices are being advised by the BMA that this includes requests from third parties such as solicitors if consent is given from the patient. In other words, we have to copy patient records free of charge to whoever asks for them provided the patient has consented."

Paul Grant: Just to define, SAR means subject access request.

Steven Bruce: Yes.

Paul Grant: It's basically a request for the information. That's what they're talking about. In most cases, you can't charge. In the old days you could charge and there was a fixed amount, 10 pounds for computer records and up to 50 pounds for manual records. That seems to have gone by the way to that. Now it's just basic things. One month you have to comply now, not the 40 days before. The other question was?

Steven Bruce: Can you charge for it?

Paul Grant: The answer is no.

Steven Bruce: Under no circumstances now can you charge for copies of patient records?

Paul Grant: So far as I can see. There was somebody, somebody made a point to me. I did speak to somebody at the ICO and they said there are certain circumstances but my current information, I don't have that.

Simon Butler: The current guidance is you can't charge. It has to be free of charge and if the request is made through a third party, because of course sometimes the patient

you're treating may end up reaching a stage in their life where they cannot make decisions and somebody then becomes their guardian and requests information. You just need to be cautious and conscious of all of that.

Paul Grant: You should be careful if you refuse the request, you must tell the individual why and that they have a right to complain to a supervisory authority and to a judicial remedy. You must do so without due delays. If there's a problem or concern, obviously speak to the IO or speak to GOSC or speak to somebody. Speak to a lawyer, speak to your insurance as to how best to deal with it, don't just sit on it.

Simon Butler: The change in this is, is that the deadline for replying or providing those copies is now one month, 30 days.

Paul Grant: One month. Not 40 days.

Steven Bruce: We talked about this again earlier, if a patient asks for their data to be erased, surely you have to keep a record of the fact that they did that and isn't that then keeping a record?

Simon Butler: No, no. That's quite different. It's a very good point, it's an intellectual point but at the end of the day you're not processing information on the request, you're just retaining information confirming they've requested it to be erased because there's no longer any data to process.

Steven Bruce: What about transporting notes, you know, paper notes for home visits and things like that.

Simon Butler: It's the same as we're guided at the bar when I go to consultations with clients and I carry my bag with all the papers in. As long as the back is secure and as long as it's with me at all times and I don't leave it where somebody can obtain information, it's perfectly fine. But one of the common problems that we have at the bar with barristers is after a long day, some barristers will go on the underground, they'll have the papers, and they'll leave them on the train for whatever reason. It becomes very expensive for them if they don't have insurance.

Steven Bruce: Again, really what you're saying, for those home visits, if you take your paper notes with you and you go to the visit, they're in your possession all the time, that's fine. If you leave them in the car when you go to the shops and they're nicked from the car-

Simon Butler: You're in trouble.

Steven Bruce: That's an expensive data breach.

Simon Butler: You are in trouble. There's no defense saying somebody broke into my care because the rules state you should have a secure case, in the boot, out of sight, with a secure lock on it and that's how you're supposed to transport the transfer

information.

Steven Bruce: Is that a secure case fixed to the boot or a briefcase with a lock?

Simon Butler: No, you've got to have something with a lock on it and therefore, it's kept secure, locked and out of sight.

Steven Bruce: Now, Sally in Milton Kings says, she set up an osteopathic practice from scratch, took herself and her entire team to the new premises. The finance director of the premises told me that he would treat any removal of notes as theft and would arrest me if took them. I left eight years of patient files behind. Most of the patients found me in my new place. I'm concerned about the notes I left, who they are being used by, and what will happen if they decide to throw them away?

Simon Butler: I could answer that question and maybe she can come back and send an email because I need a bit more information. If you are in premises and you're sharing it and you're paying for a room, the goodwill and the rights in those notes vest in you as the practitioner. They do not belong to the person who you may be renting a room within the building. You mentioned a moment ago earlier, most chiropractors, osteopaths, and physios are all self-employed. If you are self-employed and you're just paying a fee to use a premises, those notes belong to you.

Steven Bruce: Even if they're stored on the premises?

Simon Butler: It doesn't make any difference how they're stored, they're your notes, they're your patients, they are yours.

Steven Bruce: I suspect in this case, it might be that the practice is the entity taking the bookings and issuing the patients to the practitioners. If that were the case, if a phone call came to a receptionist and the receptionist said, "Sally, you're getting this patient." The patient then presumably is a patient of the practice, not that individual.

Paul Grant: It is arguable. I've had a case, it sounds like an identical case to mine. I'd be very firm about it because the patient comes to the practitioner. I know with the practice we have a slight gray area here. Those notes have been imparted to the practitioner. The practitioner could probably demand them.

Simon Butler: They are in law, the practitioner's notes.

Steven Bruce: What if the practice gives you the patient today, you're not in tomorrow so I give you the patient tomorrow. The practice is giving the patient to a practitioner who is available in the best interest of that patient. They are no longer a single practitioner.

Simon Butler: The principle is this. If you are a self-employed practitioner, I understand that you will use different premises and somebody may charge you and therefore they go

through a central ... It's a bit like Neil's Yard in Covent Garden, which I tend to use for treatments. My name is on Neal's Yard but there are individual self-employed practitioners that come in. I am paying a fee for a service, I am entering into a contract with that practitioner for that service. The fact that the agent, the middle man or woman gets a percentage of it for using the rooms is irrelevant. There is a contract between me and that practitioner and the information that I convey to that practitioner vests in that contract between us and therefore, legally, those notes and the information and everything retains with the practitioner. Unless the practitioner is employed by a corporate body, then it vests with a corporate body and then the corporate will be obtain that consent and you're an employee. But if you're self-employed, those notes vest in you and you're entitled in law to them.

Paul Grant: Can I add to that, that if there is a concern with this practitioner and the clients have followed her but the notes are there, I would be speaking to my patients and say, what's happened is this, can you make a personal request, and they can extract them.

Steven Bruce: That's one of the provisions is portability of data, isn't it? If I say I want my data transferred to a new entity organization, then you have to allow that.

Simon Butler: Of course, you do. It's not a question of the patient having to do it. The practitioner could produce the form and have the patient sign it and the practitioner can send it to the other practitioner and say, I want this information within 7-14 days. There's my client's consent to it and if you fail to provide it then obviously-

Steven Bruce: 7-14 days, not 30.

Simon Butler: No, no. I'm just suggesting you transfer all relevant information. The requirement is obviously you can't take longer than 30 days. I'm saying if I'm making a request, there's nothing wrong with saying, I want it in 7-14 days because you're requesting it. If they say no, we're gonna sit and wait for the 30th day, that's a matter for them but I'm just saying, you can say I want it within a timeframe because if the patient is due to have a treatment and they need to be treated, why would this other practitioner deprive the patient of the right to that treatment by waiting 30 days?

Paul Grant: Particularly, because it's a financial person, it's not even an osteopath who is refusing to deliver the notes.

Simon Butler: Anyway it was a breach of their professional regulatory rules but preventing a patient from being treated because they're sitting on the notes, in my view.

Paul Grant: I agree.

Steven Bruce: It sounds like you've got something to work with there. I've got so many questions but there are some specifics that I need to address, I think, which are changes under the new act. The first one of I've got here, is do we need to have a GDR, GDRP, GDPR policy on our website?

Simon Butler: I think it would be helpful to have a policy as to how you deal with this process because of course, as a professional person, we will be having it as barristers, solicitors will be required to have it. It doesn't have to be lengthy but it just confirms you're complying with the rules, which instills confidence in my view in people who may wish to use your services.

Steven Bruce: I think the ICO guidelines that I read earlier were that you should have a policy, a privacy policy.

Simon Butler: You definitely need a policy, yes.

Steven Bruce: And it should be prominently displayed. It shouldn't be tucked away amongst any technical jargon. It shouldn't be part of your terms and conditions so it should be clearly stated as being your privacy policy and so on.

Simon Butler: With any policies, you create a policy and it's accessible to people wish to see. You don't blow it up and frame it and put it on the wall in your practice.

Steven Bruce: There's a good point, because we were told yesterday you've got to have your privacy policy or your information policy on a sign on a wall in your practice.

Simon Butler: No, not at all.

Steven Bruce: I thought, actually no. Signs on the wall, nobody reads signs on the wall anyway.

Simon Butler: Absolutely not, you just don't need to do anything of the sort. You just need to have a policy in place to provide to somebody when they request it. If you put it on your website, all the better.

Paul Grant: That's better, yeah. I agree.

Steven Bruce: I don't want to get bogged down in this but Claire has said that renting a room is different to being an associate isn't it? If osteopathic contracts say that you're an associate, does that make a difference in terms of who the patients belong to?

Simon Butler: Claire, it doesn't it. I'm sorry we get into law now. It doesn't matter what title they use on a contract. It depends in reality what was happening on the ground. It's a bit like somebody entering into an agreement with somebody to rent a room and saying, you're only a license holder, you're not a tenant. So what? You can say what you like but at the end of the day, it depends how I construe the agreement and therefore, if I construe it to say you are a tenant even though you said you were licensee, it is irrelevant.

Steven Bruce: Are Christmas cards to your patients a breach of confidentiality?

Simon Butler: Oh, that's a good point, actually. It would sadly, because of course, unless you get

consent to use their private information for the purposes of contacting them whether that be by Christmas card or promoting your services, then it would because some people, I'm afraid are humbugs, and don't want to be bothered at Christmas with Christmas cards. They may consider it, you know, how have you obtained this information? Why are you sending me a card? Sorry to be frank, but it would be unless you-

Steven Bruce: So the statement they would have to sign up to would have to be something along the lines, I will use your information in order to communicate with you, full stop or communicate with you about ...

Simon Butler: To communicate with you about sending you information concerning your birthday, concerning whether you need to return for treatment. You have to specify it.

Steven Bruce: Right. Okay, that's useful. If you have patient phone numbers on your telephone, is that a problem even if they're not specifically listed as patients? Again, we're talking about your personal mobile phone here.

Simon Butler: When does a patient become a patient?

Steven Bruce: Regardless of the patient, it's still storage of people's personal name.

Simon Butler: It's personal information but I think the question was, if they've not yet become a patient but they've made contact with me and I've taken their information to contact them for a treatment, that's perfectly fine.

Steven Bruce: I read this as they are patients, they're just not listed on the phone as being a patient.

Simon Butler: Oh, right. If they are a patient, then it's still personal information and it has to be secure.

Steven Bruce: If you've got computerized notes and you have someone who assists with your IT, what do you do about confidentiality or anybody else that deals with your data?

Simon Butler: Then at the time, you obtain the consent, you have to confirm that the information may become accessible to a computer technician who has to work on the computers. It's a standard term that you see in a consent form that obviously a third party sometimes may have to access it such as a computer technician.

Steven Bruce: Does that technician have to sign a nondisclosure agreement.

Paul Grant: Yes, an NDA. That's a good question. I think I would do, yes.

Steven Bruce: There's two sides to that. There's consent that the data may be handled by a technician and there is the nondisclosure agreement, which the third party would

have to sign in order to handle your data. We'll put this onto the documents that we make available on our website. Although there's as awful lot we're having to put on these documents at this rate. Somebody here says, thank you so much, this is amazing.

Simon Butler: That's very kind of you to say.

Steven Bruce: It's a little bit early to say that. You shouldn't butter lawyers up, [inaudible 01:16:27]. If a practitioner is a subject of a patient complaint, presumable the regulator and possibly any defense counsel the practitioner may retain will process the clinic notes at that time. Does the patient need to consent to their data being processed by such parties during the first consultation? Anticipating a complaint with your patients at the first consultation.

Paul Grant: Hit me again, the patient is it, there's a complaint.

Steven Bruce: The practitioner is subject to a complaint.

Paul Grant: Right.

Steven Bruce: Presumably the regulator, GOSC or General Chiropractic Council and possibly their defense counsel. I'm sorry, the defense counsel the practitioner may retain will process those clinic notes that are relevant to that complaint. Does that need to be on their consent?

Simon Butler: No, it doesn't because under the regulations, just so you're aware, certain information has to be used in certain proceedings and if it's by your regulative body, there's a statutory provision that gives them the right to access that information for that purpose and that would include the legal teams having access to it for the purposes of advising you.

Paul Grant: Yeah, but two points. There's the regulator and there's the osteopath or the chiropractor. The regulator will also seek permission from the complainant to have access to their medical notes.

Simon Butler: But as a matter of 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 defense. Otherwise, you'd never be able to defend it because the person who brings the complaint could object to it and that's not permitted.

Steven Bruce: I hope that's sufficiently clear. How would you suggest a practitioner deals with the issue of a patient booking their next appointment and looking over your shoulder and seeing the other patient's names on the computer?

Simon Butler: I don't think that's a problem. You're never going to stop nosy people being nosy.

Steven Bruce: Just seeing names on a computer is not a big issue.

Simon Butler: No.

Steven Bruce: Good. I'm quite surprised about that, thankfully. We're getting close to the end of these. Is it okay to send email, oh I like this. This is going to lead us into encryption, which I wanted to nail to some mast or other. Is it okay to send emails with clinical information on them if you have the written consent of the patient? I would like to add into that, does that mean we have to have encryption software so that we can email data to the GP or to the patient or anyone else?

Simon Butler: No, you don't need encryption if you've got permission to convey information by email, then that's perfectly fine as long as your patient consents to it because they consent to it being conveyed in that format.

Steven Bruce: Right. We had a discussion with the Information Commissioner's Office. I can't remember the particular individual that we were talking to but this issue of encryption software has come up time and time again. I think people are very worried about the expense they're going to have to go to. We were advised by the ICO who, let's face it, are the authority in this country for the implementation of these regulations and the data protection, that actually emails are reasonably secure in their own right. If you put a document in there with a password on them, that's better still. But they seemed to imply that it was just okay to send things by email assuming you've got consent.

Simon Butler: It is because just as your members are aware, as a solicitor, as counsel, I get hundreds of emails with independent expert reports, all kinds of personal information concerning my clients.

Steven Bruce: That won't change under the GDP [inaudible 01:19:48].

Simon Butler: No, you can send it by email as long as the email, the system you're using is secured, it's perfectly fine. The courts use it for sending emails internally. It's perfectly fine.

Paul Grant: Absolutely, we issue proceedings through email. Yes, I know. They pay by email.

Steven Bruce: We've got 10 minutes left and I would like to move on to the issue of marketing, which is quite distinct from the business of storing patient notes and I think quite distinct from the business of writing to a patient to say your next appointment is due tomorrow, don't forget, that sort of stuff. I think this is where the biggest changes have occurred in the business of how you can contact people for marketing.

Simon Butler: It is. That's the purpose of it all and the reason behind it because people are fed up being bothered and emails and phone calls trying to market services. I think for your members as long as on the consent form, you have standard sentence stating we can use your, obviously not treatment information, but we can use your name

and address and email address for the purposes of marketing services, then you're perfectly fine. That's pretty standard now on documents you will see when you're signing up to things that they will use it for that purpose.

Steven Bruce: I would argue with my marketing head on that you might be better off not using that standard sentence because if you say, I'm gonna send you stuff for marketing purposes, I will automatically say, no, you can't. If you said to me, I would like to send you from time to time a newsletter that gives you updates on healthcare information, which you might find useful, that's a more persuasive thing to ...

Simon Butler: Yes, it depends upon the language but then you're getting into somebody then construing it to saying well, what were they in fact consenting to? Where I'd rather just be more generic and simple and say, I'm going to be sending you information marketing my services. Most people will say yes or no. We all get those boxes to tick whether you want it or not when you shop online and I think we're all used to it now.

Steven Bruce: We're all used to not ticking the boxes. Remember, they must not be pre-ticked boxes. It's supposed to be a conscious effort on the part of the patient.

Simon Butler: They can't be predetermined. You've just got to be conscious that they've read it, signed it, accepted it.

Steven Bruce: Which then brings us to the issue of people who are not already our patients. If we are getting information through Facebook Messenger, ManyChat, or through Facebook adverts and so on. What do we have to do then to ensure that it's okay to send them information.

Simon Butler: Well, they're not your patient at that stage.

Steven Bruce: But they still have rights of data protection.

Simon Butler: They do but you're obtaining the information from a third party so the third party will have dealt with that party as to whether it could be used for that purpose. Otherwise, how would you come into possession of it.

Steven Bruce: Okay. If I set up a Facebook advert and I put out there Steven Bruce, osteopath, wants to fix your back pain and 300 people, I wish, 300 people respond to that and I then send them a booklet about back pain and a booklet about ... That's all right then, I don't have to have any consent to that.

Simon Butler: Not as long as that when they were on Facebook consented to the information being used for that purpose, then that's perfectly fine.

Steven Bruce: Right, but they won't do that. What they'll do is they'll click the advert and then they'll be taken to your page about whatever it is you're trying to market to them.

Simon Butler: You'd have to be careful about that.

Steven Bruce: I know you don't like Facebook.

Simon Butler: No, I don't use any of it. I know commonly now, the osteopaths that I've used, some of them will be on Instagram and dealing with their services and trying to build up a following and a client base for that purpose but you're not sharing information on Instagram, you're just promoting a service. If you link onto Instagram, you're accepting the terms and conditions by joining that osteopath's whatever it is, page, then they can use that information to promote their services. I've consented to that.

Steven Bruce: Yes, but what you haven't done is consent to that osteopath then [crosstalk 01:23:45]

Simon Butler: Contact me to direct.

Steven Bruce: Then send you by email or by telephone or text or anything else.

Simon Butler: Absolutely. But they wouldn't be able to obtain my personal information because it's not on Instagram.

Steven Bruce: Right, okay. I'm guessing that you're not probably an expert on ManyChat and Messenger either, are you?

Simon Butler: No, I'm not. Are you?

Paul Grant: No.

Steven Bruce: A question has been asked because I have been talking to people quite a lot lately about using Facebook Messenger as a marketing medium and using ManyChat, which is a service related to that and so I'm going to explain why I think it's compliant with the GDPR and hopefully, Simon won't correct me, won't smack me too hard. When a patient responds to a ManyChat advertising message, you have to ask them, can I send you a piece of information? If they type yes into the box, they are then agreeing for you send them that piece of information. At some point, you might want to ask them can I send you more information related to the condition that you're asking? If they say yes, you're allowed to send them information related to that condition. If someone responds to an advert for sciatica and you say, can I send you more information about sciatica? That's fine, send them more. But don't then send them information about migraines because they haven't asked for that information. Is that a reasonable scenario?

Simon Butler: That's perfectly, fine. Yes.

Steven Bruce: In terms of the consent, if you look into ManyChat, you will find that ManyChat records that this patient opted in through this particular mechanism. It will identify

the messages whereby they actually opted in for that service. You do have a record of how they opted in. You should make sure that have got a very clear and easy to understand way of opting out of your messages. Somewhere in the conversation, not in every single message, but somewhere in the conversation you should say, if you get fed up with my messages, just type stop or unsubscribe in the comments box and I will stop sending you messages. Is that reasonable?

Simon Butler: Perfectly fine.

Steven Bruce: And the same with your emails. Of course, emails generally have that unsubscribe option at the bottom of every single email. Good, that's done ManyChat, which I'm very pleased about and we've still got four minutes left so I've got time for this yard-and-a-half of ... Oh, God. What about card machine receipts?

Simon Butler: You're not processing information with card machines.

Steven Bruce: There's no identifiable data on those. There's the last four of the card and no patient name.

Simon Butler: Every time we go into Pret or we getting a coffee and we slap in with our card. You don't need consent.

Steven Bruce: There's Christmas cards here, someone says, I've got some long-term patients I send Christmas cards to and they often send one back. Do I have to get permission in the future? Get permission for them to send you a Christmas card.

Simon Butler: Send them a consent form with the Christmas card.

Steven Bruce: The simple answer is yes. If they're sending you a Christmas card as well, can you assume that that's a [crosstalk 01:26:24].

Simon Butler: No, you can't sadly. I know it sounds terribly sad that we've reached this stage with data but if you're using ... We're talking now about the old patient so you'll be perfectly fine because they've not come in to see you anymore. But all your new patients, if you're sending Christmas cards to them and you've not put it on your form saying you're consenting me to use it for that purpose, it's a wonderful thing to do but if you get the wrong patient who makes an issue about it and you're found to be in breach of the rules, it would be a very difficult and expensive process for you.

Steven Bruce: Simon, you shied away from this when I asked you this question earlier on but I'm going to make this point for you. Turn this on its head and actually writing to all your patients and saying, you won't believe what I've got to do. I have to get your permission to send you a birthday card or a Christmas card. Isn't that daft but please, when you next come in, would you just tick a box and sign it to say that I can send you this. Isn't that a great marketing opportunity? Isn't writing to all those patients who are in your long-term books, the ones that haven't been in to see you,

isn't that a great marketing opportunity? Write to them and say, you haven't been to see me for a while but I have to make sure I've got consent to deal with you. By the way, if you have got any problems, you know where I am. That's perfectly okay, is it?

Simon Butler: It is but my dentist will send reminders or the optician that I need to go and have my teeth cleaned or I need a checkup predating this, perfectly fine. Postdating this, they will now need to get me to sign a new consent form permitting them to do that. I will give them that permission because it's very helpful to receive that information.

Steven Bruce: There was a marketing opportunity in this as well as the requirement to comply with the general data protection regulations. Cranky, let's see what else we've got in here that we've got two minutes to deal with. Do we have to mention in our privacy notice consents about disclosing information to private healthcare insurance providers as a third party. Knowing in mind a patient would come to us first with a request for treatment through that insurance provider?

Simon Butler: That is a good point. If you're providing it through something like Bupa, then yes, you'd have to confirm that you'd be sharing the information with Bupa because Bupa frequently asks for the treatment you performed so you can receive payment.

Steven Bruce: It was [inaudible 01:28:45] ironic. If you're getting people to sign all this on a bit of paper, how long do we have to keep those bits of paper for to prove that they have consented for us to doing all these things?

Simon Butler: Eight years.

Steven Bruce: Effectively, as long as we're seeing the patient plus eight years.

Simon Butler: I think you have to because if there's a dispute as to whether consent was given by the patient, if you've no evidence and it turns on your recollection and that of the patient, there's a risk.

Steven Bruce: Can we scan them and store them electronically?

Simon Butler: Of course, you can.

Steven Bruce: Because keeping another filing cabinet full of consent forms is going to be a pain in the neck.

Simon Butler: Store them electronically is perfectly fine.

Steven Bruce: I think we're coming to the end of our time but let's see if we can fit one more of these in. With patients who are on an email list for marketing but who didn't sign the form as it wasn't part of the process at the time but they are able to unsubscribe on each email, do we have to email them again? Do we have to get

consent.

Simon Butler: I think you do. I've noticed it recently where I'm getting lots of emails from service providers saying if you don't respond to this confirming we can now use this information for a particular purpose, we're going to delete you from our data base. I'm already getting that as a result of these regulations from people that I've used and if I don't respond, I am deleted from their database. They will no longer take the risk of bothering me because the fines are going to be so significant.

Steven Bruce: Once again, we are coming to the end. I would turn that slightly on its head and say, look, you can use this as a marketing opportunity. If you're going to send out those messages, try to make it an attractive option that people will stay on your marketing list. If you just send out a bland statement saying, I'm gonna delete you from records if you don't tick this box, people will not tick the box because people won't do something unless there's a really good reason for them to do it. They won't take that action. You've got to give them a really good reason to want to stay on your marketing list. I can't give you any easy answers to that.

Simon Butler: A good reason is a free treatment.

Steven Bruce: That [crosstalk 01:30:39] regularly. We haven't much time left, I can have a quick look through the notices of the things that I put out for you. There are three documents, as I said, on the website, which you can download. They are very much draft documents. The GDPR privacy notices. I've put in red on these documents thing that don't apply to us as small businesses. I'm going to check with Simon before we go any further, after the broadcast that that is correct. What we will be doing, as I said, is we'll be updating those documents and we will send you, I'll do this before the 25th of May so you don't have to opt in, we will send you the updates to those documents so that you can comply with the GDPR as simply and efficiently and as effectively as possible and the notes from this broadcast will be transcribed and put as a summary document very, very soon. Hopefully, we are helping you out as efficiently and as effectively in a simple language as best we can.

The next broadcast is with Matt Walden, it will be Matt Walden the next time out. We are talking to Matt about nutrition so do joint us for that one. That will be the, whenever the next one is, I've forgotten. The first Wednesday of next month, so join us for that broadcast. I hope you've enjoyed this evening, hope you've got lots of useful and informative material from it. If you've got questions keep sending them in because we will find the answers for you and will promulgate that to everybody.

In the meantime, I thoroughly enjoyed myself this evening, which is amazing considering there were two lawyers in the studio. Simon, it's been a delight. Thank you so much for coming.

Simon Butler: It's a pleasure, thank you.

Steven Bruce: Paul, as always. It's been a great pleasure having you in the studio.

Paul Grant: Thank you.

Steven Bruce: Join us next time. That's it for this evening. Thank you.