**Module 8 – Bringing it all together, some myths and help with workshop scenarios – transcript**

[Spaces indicate when the slide changes, and some timings are included where these are captured by the software]

[00:00:02] This is the final GDPR module in which we're going to bring it all together. Hopefully we're going to explore and dispel a few myths. And also I'm going give you a little bit of help in how to work through the issues in some of the workshop scenarios that I’ve been encouraging you to have a look at throughout the series of modules.

[00:00:19] First of all, here is a list of a few of the questions that we and the Regulatory Support Center have been asked by researchers and research managers since GDPR has been implemented. If you spend a little bit of time to have a look through them. I think now knowing what you now know having listened to these modules, you can see that yeah a lot of them are based in really quite fundamental misunderstandings of GDPR, some of them, and some of us have nothing to do with GDPR at all, they have more to do with the common law of confidentiality.

[00:00:51] So I'm hoping now you do feel empowered, that if you hear any of those particular questions you will be able to dispel the myths. They're all myths. They're all based on some misinterpretation or some misunderstanding. And just to really reaffirm that and to consolidate what we've learned and to really bring it all together, and as I say also to explore those workshop examples that I kept pointing you towards, let's go through and summarise what we've learned in the preceding modules.

[00:01:18] So we started off by looking at the common law of confidentiality and we ascertained that information was subject to the common law if it was: identifiable; if it was no longer in the public domain; and if it was given with the expectation that it be kept confidential. And we determined that keeping things confidential is not quite the same thing as keeping a secret.

[00:01:38] Because particularly, say within an NHS setting, there will be a whole group of people, an entire care team who will be party to confidential information about their patients. And that care team can be made up of many different types of members of staff, many different disciplines, administrators, sometimes researchers, all sorts of people could be in the care team. And everyone within the care team does have a duty of confidence towards their patients and that duty was established implicitly. It's what patients expect. It never had to be made explicit within a research context.

[00:02:13] Quite often the relationship a research team has with their research participants is perhaps slightly different in that there's no implied relationship or duty of confidence. We actually make that quite explicit because we get consent from most of our research participants, and as part of that consent we ask people if it's okay for us to access confidential information about them, and therefore we manage their expectations and we have developed duty of confidence in a very explicit manner with our research participants. The same law applies whether the duty of confidence was formed or established implicitly or explicitly, still the same things are required: that you only share information confidential information within that duty of confidence and you do not disclose it outside of, in this case, the yellow circle.

[00:03:05] We've also talked about if you do need to disclose information beyond the duty of confidence, a way of doing it is to anonymise it. It’s no longer confidential if it is anonymised.

[00:03:14] And there are technical ways of ensuring that researchers only access anonymised information. This could involve those who do have a duty of confidence doing some kind of very highly technical linkage, say, of information and only passing anonymised information out to the research team. So a research team can still conduct research. In that instance there is no disclosure in terms of the common law because no information is passing outside of the duty of confidence towards the research team. None of that is identifiable. Therefore none of this is confidential.

[00:03:49] Talking about identifiability. We talked at length I think in Module 1b, about what constitutes identifiability. It is a very difficult thing it's like nailing jelly to the wall, identifiability as a kind of grey smear going from truly anonymous through to screamingly identifiable. The law is binary and we're expected to work somehow with a very binary definition. Information is subject to the common law if it's confidential, not if it isn't. Data would be considered personal data if it's identifiable, not if it isn't. So we have to work in a binary sort of situation given that grey smear of identifiability. Remember what determines whether something is identifiable or not, it is whether or not identification is reasonably likely by a motivated intruder. And just remember the example we gave of Her Majesty the Queen's information.

[00:04:43] A breach in common law is if anyone were to receive confidential information that the individuals concerned were not expecting or would be surprised by. So if researchers were to acquire confidential information and their participants were surprised, that would constitute a breach.

[00:05:02] And that would include, it's not just information passing between a researcher and research participant, it includes when we publish information. We know there is a massive ethical imperative, I almost don't have to say this, to publish research findings. We have to place in the public domain the things that we have discovered. Otherwise decision makers, whether that be people making decisions about their own individual health and lifestyle choices, or whether that be policymakers making decisions about the provision of national services, if all evidence is not available to them they're making decisions on only part of the evidence. So we have a massive ethical imperative to publish everything, and we would normally always publish non-identifiable information because otherwise publishing confidential information to the world would be a breach in the common law because people are not expecting it. However, if we do want to publish identifiable information we can do it in line with a common law, provided we got consent provided we've managed our research participants expectations, and they know that was the deal. They took part in the research study on an understanding, a clear understanding, that the research outcomes would be published in a fully identifiable form. They understand the risks involved and the implications for them personally, and they gave consent. And anyone who was unhappy with that didn’t take part in the research. So you can publish identifiable stuff, but you must do it in line with a common law, you must get consent and manage expectations accordingly.

Equally in this day and age, it's not just publishing batch statistics and research findings, we are now expected often to make raw data, person level data, available. That doesn't mean just sticking person level data on the Internet for anyone to have a look at, because as we've talked at length: what renders information identifiable is not just the content of it but also the context. And in this day and age, it is very difficult, given the contexts that we all have access to the Internet, and the internet contains vast amounts of information about many of us; it is very difficult to put person level data in the public domain without it being identifiable. So open access does require us to make person level information available, but to do so in a managed way with adequate protections in place, ensuring there is no breach in the common law. And this is a very big part of the so-called transparency agenda, transparency is one of those words that I've used a lot in GDPR, because transparency is important in GDPR. Transparency in this way of using it is being transparent about the research you do and the findings you have, and being open to scrutiny by collaborators and your peers who can analyse and examine your data to ensure they also come to the same conclusions that you did. There are implications for publishing identifiable data when it comes to GDPR in terms of exemptions. You don't want to worry too much about that but I would speak to your DPO if you are intending to publish identifiable data. But as I say publishing is very much about making sure you're publishing in line with a common law. You're not accidentally disclosing identifiable confidential information to the world.

[00:08:28] OK, so as I say, a breach in a common law not acceptable if participants are surprised if it's against their expectations, and that is the measure really of a breach if it is not within reasonable expectations, they would be surprised.

[00:08:41] But having said that we have also explored the fact that there are legal avenues which allow disclosure, even though research participants, or other individuals, would not expect it. And I'm not going to talk about those at length. Suffice to say in Scotland we have one system; in England and Wales we have another; in Northern Ireland we have another. But you know what those legal avenues are. And if you're not sure please revisit the module that covers that.

[00:09:06] But we don't just need to worry about common law when it comes to these myths or the workshops. We also need to think about GDPR. I always find it helpful to consider a common law first, because in some ways that is the sort of easiest less nebulous thing to apply to a particular situation, and once you've done that then you start to consider what the GDPR implications are. General Data Protection Regulation applies when you hold personal data.

[00:09:32] And just as a reminder, personal data is not the same thing as confidential information. It is structured information; it relates to or is about a living person (confidential information could be about dead people); and it's identifiable. And the definition of identifiability used a very similar one for personal data as for confidential information.

[00:09:51] As soon as you are collecting, using, holding (processing) personal data, you have to abide by the principles of GDPR. And here they are.

[00:10:00] And in particular we spent quite a bit of time talking about what fair, lawful and transparent processing would look like.

[00:10:08] Never forget these assurances, that this is what GDPR is really all about, providing the public with:

First of all the assurance that you are an organisation doing reputable things That you are, for example, a university does research. There's no big surprise there. They should have a lawful basis. Therefore the university is doing research. And yes there is a lawful basis written in law in GDPR, there are specific lawful bases which you as a researcher should always be able to rely on. And those are either: supporting a task in the public interest, if you work for a public body like a university; or for legitimate interests if you don't work in a public body. One or other will be your lawful basis. You should have a lawful basis like that because this provides the public with assurance about your organisation and then about the activity that you're doing. The other assurance you need to provide people with is that they retain personal control over their data, that you will be transparent and that you are fair with them and treat them fairly.

[00:11:11] And we talked quite a bit about transparency. Transparency isn't about informing people in consent alone (that can form part of transparency) transparency is a far bigger agenda than that. It's about organisations being really open and honest with the public, about what they do with data what sort of data they hold and why they're holding it, what people's rights are, where they can go if they've got a problem et cetera. And it's a real culture of openness, providing information that is understandable, that is easy to find. It is not, I reiterate, it is not just the information handed over during the consent process.

[00:11:50] We've looked at some other aspects in terms of the principles of GDPR. We know that research, provided it is safeguarded appropriately, is never an incompatible purpose, which means that we can use data collected for one purpose for a new secondary use. But we do have to be sure that our secondary use is not a new purpose. And by that I mean we have to be transparent and ensure that people do know and have access to information about all the uses that data could be put to including research, and in perhaps a bit more transparent, detailed, specific terms than simply ‘oh and we do research’.

[00:12:28] We know that often providing this transparency for secondary uses can be really difficult because often it's data that was collected a long time ago, and now, I don't know 10 years later, we would like to reuse it for research. So we have to use best endeavours to try and be transparent, and actually best endeavours is the standard we always apply. We do our absolute best to make sure we are being as transparent as is possible, given the situation, given the context. Best endeavours will look different depending on the specific circumstances. But we always have to be transparent and we always have to use best endeavours to be so.

[00:13:03] We also know we can keep data indefinitely, provided that it conforms with certain safeguards which it probably will. But if you're unsure, again revisit the module on what those safeguards are. So you can keep research data in an identifiable form indefinitely. And we know that you only have to keep personal data up to date when that is necessary.

[00:13:25] Here’s a very quick blast on safeguards, but I'm not going into them in massive detail. But these research, especially safeguarded research, that I've just alluded to here, this is what you have to have in place. You've got to implement additional technical and organisational measures; the research processing of data must not cause substantial distress or damage; and the research processing doesn't lead to making any significant decisions about the participant, and if you feel it does, you get ethics approval (that's not the only reason why you get ethics approval). But if you can provide those three ticks to those three safeguards, then you can hold data indefinitely, you can say that research is never an incompatible purpose.

[00:14:06] And you can apply some of the exemptions. The exemptions were complicated. These are the rights that people have, that we all have actually under GDPR. There are exemptions available for researchers. I would be very careful, as a jobbing researcher, applying those exemptions on my own, do not do it. Speak to your data protection officer, speak to your research governance office. Work with other people to work through which exemptions you have available, which ones you're actually going to use, what safeguards you do have, and, as I say, the exemptions to these rights do relate to the research safeguards that I just spoke about, but they do demand other safeguards in addition.

[00:14:45] Having said that, I hope I have clarified further and you will still agree that all of those questions that I posed at the beginning are mostly based on total myth. I think there's one question which may be a little bit more nuanced.

[00:15:00] The one that says I don't need to worry about GDPR because the only data I ever see never has any names in it. Well names are not the only identifier and actually you may still be holding personal data. It's not whether you've got people's names in it, it is: could you identify an individual from it. Anyway, I hope that all helps.

[00:15:20] In the future, please feel free to revisit these modules. We will be developing further e-learning once everything has sort of bedded in, and we've had a bit of time. And also in the meantime, please visit our website. We have a lot of guidance notes, frequently asked questions, animations, all sorts of things, a growing wealth of things to help you out, to help you get on with your day job and to work effectively, keeping in line with both the common law of confidentiality and with GDPR and the new Data Protection Act. All the best and good luck, thank you.