OLIVIA WHITCROFT

"The questioner and I were in the virtual room alone together. Or were we?"

We all have an implicit understanding of what "confidential" means, but in practice it's open to misunderstanding – fortunately, the law can help

I was taken by surprise on Teams the other day with the question: "Please may I speak to you about a confidential matter?" As a solicitor, one of my professional duties is to keep the affairs of my clients confidential, and I am used to confidential discussions. So the request itself was not unusual. The surprising factor was that it was being asked in a meeting attended by 20 people.

It was during a break in a training course, and I was sharing a picture of a cup of tea. The other delegates had their cameras and mics switched off, so presumably had retired to their real kitchens to enjoy a real cup of tea. The questioner and I were in the virtual room alone together. Or were we? Maybe some of the other delegates were forgoing their hot beverage and were instead lurking in the background listening. Perhaps some had taken their laptops with them to the kitchen. Maybe some worked in an old-fashioned office and were broadcasting the session to colleagues.

I said that this was perhaps not the best environment for such a discussion, but that I would be happy to speak about it after the meeting.

It got me thinking: what environments are suitable for confidential discussions, and how can I meet my duties of confidentiality?

Keeping it confidential

What better place to clarify my obligations of confidentiality than the guidance from the Solicitors Regulation Authority (SRA)? "This duty of confidentiality exists as an obligation under both common law and data protection legislation as well as being one of the core professional principles set out in section 1(3)(e) of the Legal Services Act 2007 and professional standards in our Codes." Okay, so not just a gentle "You must keep things confidential as it's in our Code of Conduct", but "You must keep things confidential – it's in two statutes, we've put it in our Code, and don't forget common law, too".

Olivia is principal of the law firm OBEP, which specialises in technology contracts, IP and data protection
@ObepOlivia

I read on.

"…Note the need to distinguish… professional obligations of confidentiality from… legal professional privilege… confidential information may be disclosed where it is appropriate to do so but privilege is absolute, and privileged information cannot therefore be disclosed."

Goodness me, there's another layer. A lot of records I hold may be not just confidential, but privileged, which means they need to be kept even more confidential.

"A lot of records I hold may be not just confidential, but privileged"

"Good luck, Olivia", you may think, rubbing your hands together in glee that you went down a different career path. But "ha ha!" I say, as other professions also have duties of confidentiality under common law and codes of ethics, such as doctors to patients, accountants to clients, and directors to their companies. And data protection legislation doesn't just apply to me, which is fortunate for my career as a data protection lawyer. All UK organisations handling personal data are subject to the UK GDPR, which is riddled with references to confidentiality. There's even a whole principle named after it: the "integrity and confidentiality" principle.

BELOW Don't label all your records as confidential or it will lose its meaning

Sources of confidentiality obligations aren't limited to those listed in the SRA guidance. Confidentiality is a pillar of information security, just as information security is an important part of maintaining confidentiality. Statutory and regulatory rules on information security apply to organisations in many sectors, including financial services, communications, critical infrastructure and digital services.

Now let's add contractual confidentiality obligations within non-disclosure agreements (NDAs) or as part of services or settlement agreements. Contracts may require adherence to security standards, such as ISO27001 and Cyber Essentials. Sometimes a duty of confidentiality may be implied, such as within employment contracts.

Where there is no contract, we can look to common law and action for breach of confidence. This arises where information has the necessary quality of confidence (including not being widely known), it is shared in circumstances indicating an obligation of confidence (such as "Please don't tell anyone else about this") and it is used without authority to the detriment of the person who shared it (for example, published online causing financial loss). This has close links with other laws protecting confidentiality, such as trade secrets regulations, the tort of misuse of private information, and human rights laws (including the right to respect for a private life).

And in the unlikely event you're never subject to any of these, consider the wider business drivers to keep information confidential: staying competitive, maintaining good relationships and protecting intellectual property, to name a few.

So thank you for your good luck wishes. Good luck to you, too.

Weighing up the risks

As is clear, the legal need to maintain confidentiality arises from a variety of laws, codes and contracts. Trying to analyse the different rules and how to comply with each one separately is likely to get your head into a spin.

Let's look at the reason for having them to start with: to protect against the impacts of a loss of confidentiality. These may include financial and business losses, emotional or physical harm, discrimination and reputational damage. A loss of confidentiality for material protected by legal professional privilege may also prejudice a client's legal position.

In applying the rules, we're trying to minimise the risks of these consequences occurring. The precise nature and severity of the impact may vary depending on the type and scope of information, and who or what it relates to. The environment in which information is discussed, stored or used may affect the likelihood of the impact. Also bear in mind that if there

is a breach, it may be difficult to reel the information back in and re-instate its confidential status.

Take my Teams call again. When the questioner made their request, many factors whizzed through my head to assess the confidentiality risks. First, I didn't yet know the sensitivity of matter, but even if we stopped the discussion immediately after I found out, something confidential may already have been revealed.

There may have been 18 other people listening. The larger the group of people information is shared with, the higher the risks. None of them had agreed to keep content confidential and may not have even been aware of a need to. The meeting was a training session, so records may be used and shared with that purpose in mind.

The delegates were from a diverse range of organisations and locations, and I hadn't undertaken any checks on their reliability (or even that they were who they said they were). If they had all worked in the same place I may have had some assurance over their firm's confidentiality and security policies, but this wasn't the case here.

Risks in using the Teams platform also flashed through my mind. This was not just whether Microsoft has implemented appropriate technical security measures, but also whether I had sufficient understanding and control of the settings for the meeting. Would a recording of the meeting shortly be uploaded to the cloud?

All these factors fed into my conclusion that we should not have the discussion.

Labelling records

It may be tempting to rely on technology to address confidentiality risks. And yes, storing, using and communicating confidential information on systems with good security controls is an important step. However, as my example above shows, maintaining confidentiality is not just about the technological environment. We also need to consider the physical environment, the range of people involved, and their awareness and reliability.

It can be helpful to label records as confidential. This can assist with their legal protection, and those who access them will be aware that they need to be treated as such. But it is possible to go too far. I was advising a client that had decided to mark as confidential all records held by a particular department, to save time in going through them to determine which records were genuinely confidential in nature. However, they did not, in practice, treat all these records as confidential, as many of them were widely shared both internally and externally.

A concern was that the label of "confidential" had lost its intended meaning. If some records are regularly shared, that suggests it is acceptable to share all records with the same label. It would be preferable for the label to be applied only to genuinely confidential records, which may enhance their quality of confidence and clarify restrictions on access and sharing. If needed, a different label could be used to distinguish another layer of confidentiality, such as for records that are privileged.

Labelling records by reference to their permitted use can also assist. When I'm engaged by a client, they give me confidential information to provide them with legal advice. I would be risking that confidentiality were I to use the information for another purpose; let's say because it would make a good story for a Real World Computing column in a well-known technology magazine.

Contractual measures

I was reviewing a software development contract with a two-way confidentiality provision; each party had an obligation to keep confidential "Confidential Information" of the other party, and not use it for any purpose other than providing or receiving the services.

Confidential Information was defined along the lines of: "(i) all information about the software deliverables; (ii) business information, including product plans, know-how, and software; and (iii) any other information that is disclosed to the receiving party, which is designated by the disclosing party as confidential".

ABOVE Beware of confidentiality risks in videoconferencing meetings

"The larger the group of people information is shared with, the higher the risks"

My first concern: which party's "Confidential Information" is the information about software deliverables? If neither party is permitted to use it except in connection with its development, this might make it difficult to exploit the software in practice.

My second concern: the scope of information is so wide! The first two aren't limited to information that is confidential in nature, and "business information" could include anything. Then we have (iii), which mops up anything else that is designated as confidential. Does this mean that something labelled "confidential" must be treated as such, without the need for it to have a quality of confidence?

To add to the confusion, there was a provision requiring the receiving party to return all Confidential Information at the end of the agreement. Who is returning what to whom, and does the customer need to return the software it has just paid for? Even with clarity on this point, it would be problematic returning information needed for purposes such as invoicing and essential record-keeping.

My suggestion was that, rather than trying to interpret the practical impact of this poorly drafted provision, both parties would benefit from additional clarity to achieve what is intended: maintaining the confidentiality of genuinely confidential information.

BELOW Confidentiality agreements must be well drafted so obligations make practical sense

Unanswered questions

To my disappointment, the questioner from my Teams meeting never did get in touch to discuss their matter. On the upside, I suppose there's no risk of me breaching a duty of confidentiality for information I don't know. Perhaps they were worried I'd tell everyone about it in this column.

olivia.whitcroft@obep.uk