The Information Commissioner's Response to the Health & Care Professions Council (HCPC) consultation on revised guidance on confidentiality

The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 ("DPA"), the Freedom of Information Act 2000 ("FOIA"), the Environmental Information Regulations ("EIR") and the Privacy and Electronic Communications Regulations 2003 ("PECR"). She also deals with complaints under the Re-use of Public Sector Information Regulations 2015 ("RPSI") and the INSPIRE Regulations 2009. She is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where she can, and taking appropriate action where the law is broken.

The Information Commissioner's Office (the "ICO") welcomes the opportunity to respond to this consultation on revisions to the HCPC's guidance on confidentiality. The content of guidance on confidentiality is generally not something for the ICO to comment on as the regulator responsible for the DPA. However we do wish to comment on the context in which that guidance will apply.

The legal regime that applies to confidential information operates in parallel with the DPA, and we are keen to ensure that the guidance acknowledges that HCPC registrants must take the requirements of the DPA into account as well as those of confidentiality, where the information processed is personal data (in many cases, "sensitive personal data" as defined by the DPA[1]).

References to the ICO and the DPA

We are pleased to note that the guidance does mention the ICO and the guidance that we produce. We also acknowledge that the HCPC has made a decision not to go into detail about specific pieces of legislation. However, the guidance does not make clear the difference between the DPA regime and the confidentiality regime. The reference to the ICO and our guidance may therefore be somewhat confusing in its current form, as registrants may take this to mean that the ICO regulates the duty of confidentiality and produces guidance about it when this is not the case.

[1] Sensitive personal data is defined in section 2 of the DPA 1998, and includes personal data relating to the "*physical or mental health or condition*" of a data subject

In view of this, we would suggest that the guidance makes a clear and explicit reference to the fact that registrants will also have to take into account the requirements of the DPA where the information processed is personal data or sensitive personal data. We would also request that the revised guidance clarifies that the ICO regulates the DPA, not the duty of confidentiality. These two points could be combined into one section (i.e. something to the effect of "*Registrants must also comply with the requirements of the DPA. The ICO regulates this and produces advice and guidance"*).

Consent

The concept of "consent" exits under both the duty of confidence and the DPA. However, there are some key differences in the way consent is handled under both regimes. Registrants will therefore need to be aware that consent for the purposes of the duty of confidence may not be valid for the purposes of the DPA.

The *"Consent and confidentiality"* section of the revised guidance states that it is important for registrants to *"…get the service user's permission, or 'consent', before you share or disclose their information or use it for reasons which are not related to the care or services you provide to them."*

The DPA's approach is different; under the first data protection principle[2], personal data can be disclosed if it is fair and lawful to do so, and a condition within schedule 2[3] of the DPA can be satisfied (and, in the case of sensitive personal data, a condition within schedule 3[4] as well). Collectively, we refer to these as the "conditions for processing", and they provide the bases on which organisations can process personal data (a disclosure being an act of processing). Consent is one of these conditions for processing, but it is not the only one and does not carry any more or less weight than the others. For either schedule 2 or 3, if another condition in the relevant schedule can be satisfied then consent may not be required at all.

The revised guidance also explains that, under the duty of confidentiality, a registrant can rely on *"express consent"* where the service user has given specific permission for the registrant to do something, or *"implied consent"* where consent is not expressly written or spoken but can be *"taken as understood"* in some circumstances.

[2] See Schedule 1 of the DPA for the data protection principles
[3] See Schedule 2 of the DPA for the conditions for processing any personal data
[4] See Schedule 3 of the DPA for the conditions for processing sensitive personal data

The guidance explains that, for the purposes of the duty of confidence, consenting means that that the service user understands and does not object to the disclosure or sharing in question. The guidance then goes on to explain that this consent can be *"express"* or *"implied"*.

Again, the DPA's approach is different; consent is more specifically defined and the circumstances in which it can be used are narrower.

Under the DPA, consent is defined as:

"…any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed"[5].

The requirement to *"signify"* consent means that an individual must take a positive action to indicate that they give their consent to their personal data being processed in a certain way (such as it being disclosed or shared). Consent cannot be inferred or taken to be understood from a lack of action, such as a failure to object or tick an "opt-out" box. Effectively, for consent to be valid under the DPA, it must be equivalent to "express consent" under confidentiality rules.

This means that in cases where a registrant is relying on "implied consent" to disclose information, this would not qualify as consent for the purposes of the DPA. This does not mean that the registrant cannot make the disclosure. However, the registrant would need to be able to satisfy one of the other conditions under schedule 2 (and, if necessary, schedule 3) of the DPA.

In practice, this means that the processing undertaken by HCPC registrants will often not, for the purposes of the DPA, be reliant on the service user's consent (for example where the registrant is relying on "implied consent" for confidentiality purposes). Instead, that processing is likely to be reliant on a different condition, for example condition 8 of schedule 3 which allows the processing of personal data when necessary for medical purposes as long as that processing is undertaken by a health professional or a person who, in the circumstances, owes a duty of confidentiality equivalent to that owed by a health professional.

It is therefore important that registrants understand the differences between "consent" under the confidentiality regime, and "consent" as one of the conditions for processing within the DPA. Registrants should be

[5] Consent is not defined within the DPA. Instead, the definition comes from Article 2(h) of Directive 95/46/EC of the European Union. The DPA implements the Directive within the UK.

clear about the conditions that they are relying on to comply with the DPA and make sure that any processing is fully explained to service users in a clear and easy to understand manner.

Disclosing information without consent

This section of the guidance lists the situations in which a registrant could disclose or share personal data without the service user's consent.

Under the *"Public Interest"* section, the revised guidance states *"Even where it is considered to be justified in the public interest to disclose confidential information, you should still take appropriate steps to get the service user's consent (if possible) before you do so."* However under the DPA, if consent is sought and refused, to disclose the personal data in question anyway would be considered "unfair" and therefore a breach of the first principle. If it is anticipated that the disclosure has a legal basis to take place anyway, regardless of consent, then for the purposes of the DPA another schedule condition should be applied and consent not sought. Instead, service users should be clearly informed that the disclosure will take place, to whom and why.

It should also be noted that the DPA does not provide a condition for processing, or an exemption, for disclosures made "in the public interest". Therefore, if a registrant wishes to make a disclosure *in the public interest*", they will still need to be able to satisfy a condition for processing under schedules 2 and, if appropriate, schedule 3.

Finally, registrants should bear in mind that individuals have a fundamental right to respect for their private life under Article 8 of the European Convention on Human Rights (the "Convention") and Article 7 of the Charter of Fundamental Rights of the European Union (the "Charter"). Article 8 of the Charter also gives individuals a fundamental right to the protection of their personal data. Where the processing of personal data (such as disclosing it) would infringe these rights, the infringement must be justified and proportionate. The greater the intrusion caused by the processing, the stronger the justification will need to be.

The ICO is keen to ensure that the HCPC's guidance helps registrants to understand their obligations, both in terms of their duty of confidentiality and their obligations under the DPA. To this end, we are happy to engage further with the HCPC in relation to this guidance if necessary. We are also keen to continue working with the HCPC more generally to raise awareness of, and improve compliance with, the DPA within the sector.