The role of confidentiality and security for working online – our responsibilities as psychotherapists & counsellors Philippa Weitz

In this short paper I consider some of the principles (in no particular order) regarding confidentiality and security for working online. This is a position paper considering where we are now – please note this is like shifting sand and is for guidance only, and should not be considered as advice. Only the Information Commissioner's Office (ICO) can fully advise you, your professional member organisation, together with advice from your professional indemnity insurer.

Some of the information included is based on a detailed conversation I had with a representative from the Information Commissioner's Office in May 2014, which has been confirmed as correct on 20th June 2014, and email correspondence with Microsoft/Skype (June 2014).

1. Nothing is 100% secure, as the Snowden case has shown us, but it is our duty to ensure we show by good example the highest quality of service to our clients.

2. Following a conversation with the ICO in May 2014 which I wrote up and send to the ICO, the ICO confirmed on 20th June 2014 that this is accurate and represent the facts (see below). Note: whilst I have had two matching viewpoints given by the ICO, others have had slightly different versions. *There is not a clear picture at the moment, and perhaps there will always be shades of grey.*

3. Microsoft / Skype have responded 19th Jun 2014, correspondence available on request) with a very clear statement about Skype in particular, that it is not HIPAA compliant, and for its instant messaging in particular (used a great deal for online therapy) it is not totally secure and is accessed via their servers. The video-conferencing part is more secure. *What is the issue with using Skype?* In my lay woman's terms although Skype is encrypted at both ends it is not secure along the route on Microsoft's server, Microsoft being the owner of Skype. They access a large proportion of the Skype data passing through their servers, and although I am sure they are not at all interested in psychotherapy it therefore means that there is a breach of confidentiality. **This is the core issue.**

4. A book and ebook "**Information Security Policy Development for Compliance: ISO/IEC 27001, NIST SP800-53, HIPAA Standard, PCI DSS V2.0, and AUP V5.0**" by Barry L. Williams CRC Press, Taylor & Francis Group (2013), lists the compliance requirements - he deserves a medal for the detail.

5. From my conversation with ICO in May 2014 the following emerged and was reconfirmed as accurate by the ICO on 20th June 2014:
    i. Every psychotherapist working in private practice needs to be registered with the ICO. If a psychotherapist works for an organisation they are covered by that organisation's registration.
    ii. Every psychotherapist is a "data controller" (his choice of words, not mine). All data/client information in a therapeutic session remains the property of the client.
    iii. In the opinion of the person I spoke to at the ICO, the problem is with the "data controller", the psychotherapist because many are not using media suitable for the confidentiality of patient information.
    iv. It is the data controller's responsibility to ensure that the method of communication, setting etc is fit for practice and suitable. They need to investigate the suitability of a product to do a job and that how they use it is secure. For example, a very small point, but ensuring that any computer screen does not face a window. To expand this point he used the example crossing the Andes in a car, and how an old Ford Cortina would not be suitable whilst a specially adapted LandRover might be. In other words, it's about using a product that is fit for purpose, and not just going over the Andes in an old Ford Cortina because we're more used to this.
    v. He pointed out that we as counsellors and psychotherapists have a RESPONSIBILITY to lead the way in "best practice". He added that it was not OK to use any online platform that isn't

sufficiently secure even if the psychotherapist had pointed out the issues with it within their informed consent and agreement, and the client had agreed to this.

vi. He emphasised (and I write this in capitals and he was very assertive about this) that the OBLIGATION is with the DATA CONTROLLER, the psychotherapist, and that DATA SECURITY (client material) is paramount for all psychotherapists.

vii. Separately to the issue of online platforms, we also talked about working cross-border:
   a. In the UK the locks (ie the security) must be good (ie as set out above).
   b. In Europe, each country has a data commissioner who is more or less saying the same thing. Eventually the EU Data Commissioner will provide a homogenous Europe-wide policy.
   c. For the rest of the world, it's our responsibility to get advice before charging in. We all know not to work in the USA or Canada. There may be other countries.

viii. His final point was that using platforms and unsuitable methods of communication (etc) leads to REPUTATIONAL DAMAGE for the whole profession. His final words were that we, as being in the know, are leading the way and must lead by example.

I am currently researching various online platforms (see the accompanying PowerPoint presentation) that are compliant internationally so that we would then be practising ethically and safely as required within the various ethical guidelines etc. I have a list of the platforms which I am updating regularly.

All the above points would naturally come out in any risk assessment carried out by the data controller/ psychotherapist.

The question in this context would be "**what safeguards is the psychotherapist required to undertake to ensure the confidentiality and security of client information**?" This would include the safety of records (in all contexts), and a reminder that the data/information belongs to the data subject (the client).

Some useful links on the Information Commissioner's Office website:

Health	http://ico.org.uk/for_organisations/sector_guides/health
Privacy & Electronic Communications Regulations	http://ico.org.uk/for_organisations/privacy_and_electronic_communications
What security measures should I take to protect the personal data I hold?	http://ico.org.uk/for_organisations/data_protection/security_measures
Can I send personal data overseas?	http://ico.org.uk/for_organisations/data_protection/overseas

This paper is posted at http://www.pwtraining.com/resources/. Any updates that arise once the way forward is clear will also be posted. The author can be contacted at info@pwtraining.com.

Disclaimer: This paper was presented at the UKCP conference Psychotherapy 2.0 on Saturday 21st June 2014. The views and opinions expressed in this paper are those of the author and do not reflect the official policy or position of UKCP. They are based only on very limited and open source information and the entire content of this paper should be considered as "work in progress" and should in no way be considered a definitive answer. It is provided to help guide you in thinking about how you ensure the confidentiality and security of your client material in the light of newer and always changing media. The author declines any responsibility for any errors; this paper is put together in good faith. You should always consult your professional membership organisation, the ICO and your insurer for any specific advice.

THANK YOU I'd like to acknowledge Alexandra Chalfont, Máire Stedman and my OLT tutors Mieke Haveman, Babs McDonald, Gill Jones and Jan Stiff who have all supported and encouraged me in my exploration of these issues.