Security, confidentiality and jurisdiction for the online counsellor and psychotherapist

INFORMATION SHEET

May 2015

What UK counsellors and psychotherapists need to know and do about digital security, confidentiality and jurisdiction to work online therapeutically

QUIZ

Want to test your digital skills and knowledge and see how appropriate they are for your private practice?

Why not try our 5 minute quiz? If you get less than 25 points in the quiz you may need some help

http://pwtraining.com/quiz-test-your-digital-skills/

Editor's Opinion

Counsellors and psychotherapist need to have a general understanding about how to protect the risks to the privacy of their clients. They sign up to this when they adhere to the ethical principles of their chosen professional membership organisation.

However, as the reader will spot when reading on, the emergence of digital technology is a complicated and completely beyond the scope of the average private counsellor and psychotherapist.

I believe it is the duty and responsibility of the professional membership organisations to work together, as they did for conversion therapy, to provide a safe framework of guidance and tools for therapists to work in online.

We need all to lobby our professional membership organisations to undertake the necessary research, final the solutions, provide guidance and create tools for members so that practitioners can work with clients knowing they have received the best advice available to ensure they comply with the required levels of confidentiality and security.

What this Information Sheet Covers

This Information Sheet covers frequently asked questions, examples and tips.

Did you get less than 25 points in the quiz and need some help?
Do you want to train to work online?
PWT can mentor you and / or train you to work professionally online.

T: **+44 (0) 1273 700 911**
M: **+44 (0) 7880 501 116**
E: **info@pwtraining.com**
W: **www.pwtraining.com**

Providing mental health training since 1997

PHILIPPA WEITZ TRAINING
Specialists in Mental Health
Consultancy, Training, Publications, Online Counselling

UK Counselling Online and Online Counselling 4 Brits, and PWT are trading names of Philippa Weitz Training Ltd; Registered in England; Company No. 3477157; Registered Office: 85 Church Road, Hove BN3 2BB

01 Risk assessment plays an intregal part in my private practice, what do I need to do?

As with all areas of our practice, whether face to face or online, good and detailed risk assessment is essential to the health management of our practice. We talk usually about undertaking clinical assessment when taking on a new client, but when working online we need to go far further before beginning any clinical work to ensure that we have carried out three types of risk assessment:

- **Business**: such as ensuring you have confidentiality agreements with any staff or suppliers, secure international payment system, ensuring your professional liability insurance covers you to work both online & outside the UK, estblishing your jursidiction
- **Practical**: such as the organisation of your practice, ensuring your emails are secure, you have a digital policy, your screen can't be seen through a window, your computer and its data storage are secure
- **Clinical**: a form of assessment we are used to carrying out as part of our therapeutic work, but for working online you may need to add extra criteria such as being sure your client is over 18, establishing whether the client is suitable for online work

TIP The easiest way to do implement a full risk management is to use a risk assessment check list to identify your risk strengths and weaknesses as related to your own private priace. I include three risk assessment tools on my website: http://pwtraining.com/resources-for-working-online/risk-assessment-for-your-online-private-practice/. Please feel free to use them.

What are these three risk managements tools?

- **ISO 27001** related This might interest you if you decide to voluntarily adopt ISO 27001 or ISO 27002
- **HIPAA** compliance related
- A specialist online **PWT Risk Assessment tool that I have devised** covering all three types of risk: business, practical and clinical

You'll spot when you start to study these risks assessment tools that they each cover these three essential but broad and overlapping areas. The steps to take include:

TASK

1 Work your way through your chosen risk assessment tool
2 For each item write down the risks as they relate to your private pratice and work out the level of risk for yor each item, LOW, MEDIUM, HIGH
3 Work out an action plan as to how to reduce these risks, starting with the areas that you identify as HIGH RISK.

02 What's in a name and number? What is the difference between the ICO, ISO & HIPAA and what do they do? I'm confused!

In the UK why ISO and ICO and not HIPAA?

Confidentiality and Security for Working Online as a Counsellor or Psychotherapist

HIPAA - The US Federal Health Insurance & Accountability Act 1996	ISO27001 / 2 International Organisation for Standardization	ICO – The Information Commissioner's Office
USA	International	UK (linked with EU)
HIPAA is a set of regulations that governs how "covered entities" manage the security, privacy and exchange of protected health information (PHI) data. A "covered entity" is an organisation, corporation or individual practitioner that directly handles PHI or Personal Health Records (PHR) and is therefore required to be compliant with HIPAA. Under US Federal law you have no choice in the matter but to comply. http://health.state.tn.us/hipaa/ **HIPAA has no legal jurisdiction within Europe**	This International Standard provides requirements for establishing, implementing, maintaining and continually improving an information security management system [ISMS] that preserves the confidentiality, integrity and availability of information by applying a risk management process & gives confidence to interested parties that risks are adequately managed." (Joint Technical Committee ISO/IECJTC 1, Information Technology, Subcommittee SC 27, IT Security Techniques. 2013). We may need to consider including ISO 13485 regarding software for medical devices (including mobile phones). Organisations and individuals can become ISO 27001 compliant by implementing an on-going external audit. Organisations and individuals can voluntarily adopt the ISO standard. **ISO 27002, a simplified version, is suitable for counsellors and psychotherapists.**	The ICO manages the Data Protection Action 1998, which as counsellors and psychotherapists we are required to adhere to under UK law. With regard to security and confidentiality, as a very minimum you need to "..... encrypt any personal information held electronically that would cause damage or distress if it were lost or stolen ...." http://ico.org.uk/for_organisations/data_protection/security_measures Accessed 19/06/14 A provider of a public electronic communications service must take appropriate technological and organisational measures to safeguard the security of its services. **An appropriate measure is one that is proportionate to the risks it would safeguard against, taking account of the state of technological development & the cost of implementing the measure.** These measures must **at least:** **(a) ensure that personal data can be accessed only by authorised personnel for legally authorised purposes;** **(b) protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure; and** **(c) ensure the implementation of a security policy with respect to the processing of personal data.** http://ico.org.uk/for_organisations/privacy_and_electronic_communications/the_guide/security_of_services Accessed 19/06/14

Available at http://www.pwtraining.com/resources-for-working-online/

03 What is the ISO & what does it do?

The ISO (International Organization for Standardization) is an independent, non-governmental membership organization and the world's largest developer of voluntary International Standard. There are other similar bodies including CCITT and IEEE. I'm going to stick to the ISO standards.

There are two levels of ISO. Organisations can be externally certified with ongoing auditing. Organisations and individuals can voluntary adhere to the relevant ISO standards. In my opinion this is sufficient for counsellors and psychotherapists, whilst builders of software platforms and apps should be ISO certified.

04 I have heard about ISO 27000 series and other ISO numbers. Do I need to worry about these?

Short answer: you should be aware of these without getting too involved in the detail.

Opinion: This is where is gets complicated. I don't believe counsellors & psychotherapists should have to become security, confidentiality and jurisdiction experts. They should be able to rely on the professional membership organisations they adhere to, to provide them with accurate leadership and guidance. That's why we pay their membership subscription. In the similar way that recently these organisations have combined to give good guidance on conversion therapy I believe that they should provide clear guidance for security and confidentiality when working online therapeutically.

05 What is the ICO & what does it do?

The ICO (Information Commissioner's Office) is the UK's independent body set up to uphold information rights in the public interest. The Ministry of Justice is the ICO's sponsoring department within Government.
It's work includes:
Maintaining a register of data controllers (a "data controller" means "a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed". In this contect the data contrller is the counsellor or psychotherapist.
The Data Protection Act 1998 requires every organisation that processes personal information to register with the Information Commissioner's Office (ICO), unless they are exempt. Failure to do so is a criminal offence.
Handling concerns
Taking action - Data Protection https://ico.org.uk/about-the-ico/what-we-do/taking-action-data-protection/
Taking action - Privacy and Electronic Communications Regulations https://ico.org.uk/about-the-ico/what-we-do/taking-action-privacy-and-electronic-communications-regulations/
Taking action - Freedom of Information and Environmental Information International duties https://ico.org.uk/about-the-ico/what-we-do/international-duties/
The ICO manages the Data Protection Action 1998, which, as counselllors and psychotherapists ,we are required to adhere to under UK law.

Help is at hand! PWT has courses to meet your needs

Need some help with sorting out your risk management strategy?

Need some help to ensure your computer system is safe?

Need some help to develop a digital policy?

Need some help to develop a social media policy?

Want to work online?

Not sure where to start?

We at PWT can help you with all your digital needs and train you to work online therapeutically.

PWT offers three courses reflecting the three levels of training:

BRONZE, GOLD and PLATINUM.

If you are interested in joining one of these courses please contact us for the full course brochure including the syllabus.

PWT Course Name	Course Level	Minimum Time Requirements	Course Fees
Platinum	**Diploma Level** This fully professional 30 week course provides you with a solid basis as a professional online counsellor or psychotherapist	30 weeks course Approximately 200 hours of study and client practice; 10 hours personal therapy with an online therapist required	**Course fee:** £1350 **Early bird fee** (up to 2 months before the start of the course): £1200
Gold	**General Certificate** This 12 week course provides you with a basic grounding for understanding the work of a professional online counsellor or psychotherapist	12 weeks course Approximately 60 study hours, including role plays	**Course fee**: £650 **Early bird rate** (up to 2 months before the start of the course): £590
Bronze	**Computer & Digital Basics for Counsellors & Psychotherapists** Suitable for those considering working online or who just want to be sure they understand how digital issues might relate to their face-to-face practice.	4 week course 10 study hours including role plays	Course fee: £200 Early bird rate (up to 2 months before the start of the course): £160

06 What about jurisdiction? Surely if I say in my Terms and Conditions that I work under UK jurisdiction that's sufficient?

First of all it is obvious and sensible to ensure that in your T's & C's that you state that you work under UK jurisdiction and that any complaint would come under this jurisdiction. It would be wise to consult your professional indemnity insurer and your supervisor about the correct wording you should include.

There are ethical decisions to think about that may not be straight forward and may put your client at risk.

The example I often quote is of working with a gay man in Zimbabwe through an online format. Should you do so, you will be contracting to work with him knowing that it is illegal to be gay in Zimbabwe.

What would you do faced with this dilemma?

As we know, no encryption levels will stop the secret services spying on you if they think you are of interest to them. Working with this gay client under these conditions may put both him and his family at risk.

There is no easy answer to this dilemma about whether you should work with this client or not; at the very least it would be wise to discuss this with your supervisor before starting the therapeutic work.

A second consideration is that of data storage. The NHS Guidelines requires data to be stored within the UK. With cloud based service providers it is not always easy to be sure where your data is stored. **If you use cloud based storage read the small print and if necessary contact the company to find out where their servers are located.**

TIP

A third issue is that some of the online platforms available are not UK based. Many may even be US based (e.g. zoom.us) and this may mean that inadvertently you are routing your therapy services via the USA, and potentially requiring you to comply with HIPAA, which may have been furtherest from your intentions.

About the author:

Philippa Weitz is one of the leading experts in the UK on counselling and psychotherapy online, with a special interest in security, confidentiality and jurisdiction. She lectures and teaches widely around working therapeutically online.

Philippa Weitz is a qualified teacher, trainer and psychological counsellor with more than 25 years in the mental health sector. She is currently Clinical & Security Advisor at HealthBridge Technology, Commissioning Editor for the UKCP Book Series, Director of UK Counselling Online and Online Counselling 4 Brits, Managing Director of Philippa Weitz Training Ltd. as well as author/editor of **Psychotherapy 2.0: where Psychotherapy and Technology Meet**

Philippa can be contacted at info@philippaweitz.com +44 7880 501 116.

Disclaimer

Please note: The views and opinions expressed in this Information Sheet are those of the author and do not reflect the official policy or position of any other organisation. They are based on open source information. The content of this paper should be considered as "work in progress" and 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 and online practice 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.

A more detailed look at HIPAA

07 I hear a lot about HIPAA. Is it relevant to me as a UK practitioner?

Short answer: No, not usually, not directly, because it is a US Federal Act. The reason it is referred to so much in the UK is that it is the only healthcare guidance anywhere in the world that clearly tells us what to do regarding security and confidentiality. It is considered a model of best practice, a useful benchmark, for us in Europe, but without any jurisdiction.

HIPAA is The US Federal Health Insurance & Accountability Act 1996. As such it is only relevant to a health practitioner working in US jurisdiction. In addition, because of individual State laws you are highly unlikely to be working in the USA as you need to be registered within that State to practise.

I believe we hear a lot about HIPAA as it is a useful benchmark for us. It is written for health practitioners and covers how you should manage the security, privacy and exchange of protected health information (PHI).

There is a term that covers the list of those (under US jurisdiction) who should be compliant for HIPAA: those required to be compliant for HIPAA are known as "covered entities", whether a large business or private practitioner.

If you are required to comply with HIPAA you have no discretion in determining how you do this. It is prescriptive.

"The primary goal of the [US Federal] law is to make it easier for people to keep health insurance, protect the confidentiality and security of healthcare information and help the healthcare industry control administrative costs." http://health.state.tn.us/hipaa/

Recently HIPAA has stepped up its compliance & penalties in the USA for non-compliance can be severe for knowingly violating the HIPAA compliance requirements, fines of up to 50,000$ & prison, but there have been few prosecutions so far. In Europe although we have similar rules and regulations (see further on) but the USA system is much clearer.

Further on I cover Business Associate Agreements which also come under HIPAA.

Opinion: Many look to HIPAA as it gives us very clear guidance about what is acceptable or not acceptable. It is prescriptive and clear. In Europe we are given guidance and have to draw our own conclusions depending on our own practice. This leaves the responsibility with the organisation or private practitioner to work it out on their own, and this is where the major problem is:

it's such a huge subject that is it completely unmanageable.

To add to this, many practitioners feel it is completely overboard and unrealistic and consequently decide to ignore the ICO and EU directives.

The EU's Data Protection Directive and its General Data Protection Regulation apply to us in the UK.

Editor's Opinion: We really need very clear, profession specific, guidance from our own Information Commissioner's Office (linked with the European Union), and our own professional membership bodies, and perhaps sadly the only time that many will take it seriously is when there is a complaint that follows through to sanctions.

08 If not HIPAA where do we draw our guidance from in the UK for security and confidentiality when working online?

Short answer: The Information Commissioner' Office which manages the Data Protection Act. 1998

Whilst HIPAA is prescriptive, the ICO provides us with very useful guidelines which I would recommend all counsellors and psychotherapists read whether they work online or not, https://ico.org.uk/for-organisations/guide-to-data-protection/.

For those of us working online the Data Protection Principles are essential reading: https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/ especially Principle 7, "**Security**", & Principle 8, **International**, and concerns sending data outside Europe (EEA).

Because of its important I am quoting here the opening section of the UK's **DPA Principle 7, Security**:

> *"There is no "one size fits all" solution to information security. The security measures that are appropriate for an organisation will depend on its circumstances, so you should adopt a risk-based approach to deciding what level of security you need.*
>
> *In brief – what does the Data Protection Act say about information security? The Data Protection Act says that:*
>
> *"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."*

This is the 7th data protection principle. In practice, it means you must have appropriate security to prevent the personal data you hold being accidentally or deliberately compromised. In particular, you will need to:

- ☑ *design and organise your security to fit the nature of the personal data you hold and the harm that may result from a security breach;*
- ☑ *be clear about who in your organisation is responsible for ensuring information security;*
- ☑ *make sure you have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff; and*
- ☑ *be ready to respond to any breach of security swiftly and effectively."*

Editor's Opinion: Whilst these principles (and I have only listed the beginning here, please go and read the full text online) are extremely clear and helpful I believe many practitioners and organisations look at HIPAA as it provides a prescriptive way that is easy to understand and implement. The ICO wishes us to interpret the standard provided by the DPA within the context of our own business and practices, and of course the devil lies in the detail.

09 What does the ISO 27000 series do?

The **ISO 27000** (**ISO 27001** and I**SO 27002**) series of standards is a compilation of international standards all related to information security. **ISO 27001** standard has an **organizational focus** and details requirements against which an organization's Information Security Management System (ISMS) can be audited.

ISO 27002 http://www.iso27001security.com/html/27002.html on the other hand is more **focused on the individual**, and in this context **could be ideal for a counsellor and psychotherapist to adopt voluntarily**. It provides a code of practice for use by individuals within an organization. There is no such thing as ISO 27002 certification, it's there to provide guidance and best practice and leave you free to decide how to implement your risk assessment. [http://security.stackexchange.com/questions/76066/what-is-the-difference-between-iso-27001-and-iso-27002 Accessed 17/04/2015].

Organisations can voluntarily adopt ISO 27001 or they can ask to be certified. This is a robust audit programme externally completed. I would expect any platform, email system, software company, app, to have at least stated that they voluntarily have adopted ISO 27001, and all reputable companies should be certified. **At HealthBridge technology, where I am Clinical and Security Advisor, we have a company policy that all apps for mental health developed by us initially adopt ISO 27001 with the intention in each case to apply for externally audited ISO certification**. We believe this should be an industry standard.

10 Why do I need to know about ISO 27001, ISO 27002 and ISO 13485? Please give me an example!

It is extraordinary, given the level of ICO, EU, ISO and NHS guidelines on the subject, that few apps and software being developed for use in the UK for mental health, even some of those reputable ones on the NHS list, have this certification, or even any mention of voluntary adoption. The ISOs are an international benchmark that we can reply on to ensure that the service we supply to our client reaches the required standard within our Ethical Principles of our professional membership bodies. You need to know about these so that you can be critical of any software you are thinking of using, and know at least the benchmarks to look for. *Always read the security part of the terms and conditions of any software platform or app.*

Editor's Opinion: I believe in private practice we need to ensure that our security and confidentiality reaches the same gold standard as that required by the NHS.

To demonstrate this current security weakness in UK software and apps for mental health I am going to cover a leading mobile phone app, one that's currently winning awards, to show you how flimsy their confidentiality and security statements are.

Their security statement says: *"....what you write is completely confidential to you and your clients. Our security and encryption meets NHS information governing standards and is HIPPA compliant. [The app] complies with Caldicott Principles and all patient identity is hidden and encrypted. Our servers are based in the UK and all information is stored in the UK (complying with NHS standards). Our software sits on ISO27001 and ISO 9001 accredited servers/ providers with triple encryption of data (the same as online banking)."*

That might seem good at first glance, but the Caldicott Principles (http://en.wikipedia.org/wiki/Caldicott_Report) are general and not specific to the development of mental health based technology. So whilst to the amateur they may sound good, but they do not give detailed enough guidance here.

It's a small point but they have "HIPPA" spelt wrong (they have now corrected this since I pointed it out) – attention to detail everything in security and confidentiality. I made the point in my question as to whether HIPAA is relevant to us in the UK. Furthermore, it's good to know their servers are based in the UK (an NHS requirement) and that the servers themselves are linked to ISO 27001 and ISO 9001 ..... but it is not an accredited system but a certified one.

In fact the app itself needs to at the very least voluntary adopt the ISO 27001 standard and because of its status in the UK it should be certified independently for ISO 27001 (not just reply on their servers being certified)

I**SO13485 Medical Device:** in addition their policy statement makes no mention at all of ISO 13485 which covers medical devices – you many think this irrelevant for a smart phone app but when you drill down to the detail ISO 13485 covers any company or sole trader / practitioner developing a medical device which uses software (i.e. that drives all computers, smart phones etc). Here's a small part of the ISO 13485 text that sets out what a medical device is:

3.7 medical device

any instrument, apparatus, implement, machine, appliance, implant, in vitro reagent or calibrator, software, material or other similar or related article, intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the specific purpose(s) of

- *diagnosis, prevention, monitoring, treatment or alleviation of disease,*
- *diagnosis, monitoring, treatment, alleviation of or compensation for an injury, ..."*

[https://www.iso.org/obp/ui/#iso:std:iso:13485:ed-2:v1:en Extracted 17/04/2015]

Tedious? Yes! But the devil is always in the devil.

11 I have heard about Business Associate Agreements. What are these and do I need to worry about these?

Definition of a Business Associate: a company or individual who is involved within your business in some way externally, such as an accountant. I use this as a simple answer as we understand that an accountant will need to work with us, and that they are bound by their own code of conduct. But I hazard a guess that not one of us has a Business Associate agreement with our accountant.

Within the context of working online, when we sign up with an online platform, software provider etc, we need under the HIPAA regulations to have a Business Associate agreement. Recently the HIPAA Omnibus rule, a 563 page rule, came into effect in 2013, has ramped up the regulations. One implication of this is that not only do we as HIPAA "covered entities" need to have a Business Associate Agreement with any third party supplier providing with any service that involves data confidentiality and security, but FURTHERMORE, those third party businesses (such as Skype, VSee, zoom, Buddy Add, mappiness the list is endless but is only relevant if it relates to the States) that we use, themselves all need to have HIPAA compliance. This is just being rolled out at the moment, and you may have noticed that a number of platforms and software providers are starting to introduce Business associate agreements, especially for the paid services. I am sure this is direct response to the new HIPAA compliance requirements for Business Associates.

EXAMPLE

As an example Google has now announced a "Google HIPAA-compliant cloud", under the Omnibus rules, including Google Apps Vault, Gmail, Google Calendar, Google Drive and Google Docs , but choosing a HIPAA compliant service provider doesn't make you automatically HIPAA compliant, you are still required to ensure full compliance programme and sign a BAA with the service provider.

Another question you need answered by a service provider is where their servers are located. You will need to be sure that the data you are generating is at best store within the UK and otherwise within Europe. This is especially important if you are using cloud-based services. According to ComputerWeekly.com 14 April 2014 [http://www.computerweekly.com/news/2240218798/Most-cloud-services-pose-security-and-compliance-risks-to-European-businesses accessed 18/04/2015] only 1% of cloud-based services provide a sufficiently secure service, with 91% posing a security risk. Only 5% of cloud services are ISO 27001 certified.

12 We have survived 100 years since Freud without any of these rules, even Freud used the telephone and we never had any rules for this, so why should I take any notice of all this?

To answer this I am going to draw some parallels away from technology. The first is to say we can't put toothpaste back in the tube. what do I mean by that? Well, we should have had some guidance for telephone work, and telephone work plays a large part of some therapists work. But, it's something that simply wasn't thought about, and now we are in different times, and different times calls for different requirements. Just as you can't put toothpaste back in the tube, we are where we are now and the telephone has its part to play in the range of digital media. so very belatedly we are putting a framework of guidance in place for all things digital within the world of psychotherapy, and it will include the telephone.

I guess we'd all agree that seatbelts in the back of cars are an excellent thing and have saved lives, but not everyone in Italy will agree with you - Italians are apparently very resistent to the idea. It's just a parallel, no more!

13 What about the cost, I am just a private therapist and all this sounds expensive?

Most of the cost is your time. Taking the time to evaluate the risks in your practice, reflect on these, working out the level of risk, and deciding on a plan of action.

I hear people say so often, "I am happy with Skype, why should i change, my client likes and understands it too". Well the first point to make is that **if something is free, YOU ARE THE PRODUCT**. Skype don't charge you for using their service, but they access your data, track it, analyse it and work out what to sell you. We'll side step the Skype issue generally as it is not an issue - even Microsoft have confirmed in writing that it is not suitable for therapy purposes.

So the first cost that you'll need to take into account is the price of **paying for space of a secure online platforms for email, audio, video and chat**. Now a lot is changing in this field at the moment but over the next few months I would predict that we will start to see platforms, suitable for UK psychotherapists and counsellors to use, start to arrive. But they will not be free; someone has had to invest in these product, and I know from my own research that we are looking at a mnimium of £100,000 initial investment and thousands of pounds in ongoing and support costs. I guess we will see different proposals for pricing, some will be a fixed monthly fee, like when you go to the gym, others will be pro rata according to the number of clients you are seeing. But you will need to pay, and this really is not surprising. You are running a professional practice and you would expect to pay for a professional product, just as you would expect to pay for the rental of a consulting room in a face-to-face practice.

The second cost is related to ensuring that the software in your computer is fit for purpose, both the software you may be using for your work, and also the background software running ongoing virus checks, firewalls etc. If you need help with these there will be the cost for a computer specialist to help you.

The third cost will depend on your aptitude to some extent, and relates to training, probably your biggest initial cost. I include mentoring and consultancy in training, as some counsellors and psychotherapists may just need a "leg up", so to speak. They may want to use a mentoring session or two to checklist that they have covered all bases. Others who want to work online professionally will need to train, this is likely to cost you between £500 and £2000, depending on where you train and the level of qualification (see page 3 for more details of PWT's training).

The fourth cost relates to supervision. Amongst those trained to work online there is a widely held view that any supervisor supervising a therapist who is working online should have completed a specialised online supervision training course. Online supervisors can be found on the ACTO list: http://www.acto-uk.org/seeking-a-supervisor/

The fifth cost is the hardware. if you are still working on computers with Windows 95, Windows 98, Vista or XP its time to change your computer and software as they are not supported by Microsoft anymore which means that your virus checks, levels of encryption etc will not be sufficient.

The sixth cost relates to the type of organisation you are and the level of risk management and assessment you'll need to undertake. For the average UK based psychotherapist and counsellor, providing you use a risk management tool (see page 2) that fits your particular style of work and practice, the main cost is your time, unless you decide to ask for help with this. Sometimes it's good to involve someone else in the evalution of your risk management as we can be blind to the obvious, just as in a face-to-face practice we are used to walking round the cardboard box we put in the middle of the floor some months back but we know shouldn't be there!

14 Give me five tips to follow that will make my practice more secure

- **Pay a specialist in working online to go through the risk assessment for your practice.** It's amazing how helpful it is to have someone to bounce ideas off and you'll be astonished at how quickly you can make a big difference to your practice.
- **Implement an email policy straightaway.** This should include discussing with your client about how secure it is for them to receive emails. If it is not safe for them to receive emails then ask them to open a safe-mail.net account or a hushmail account. You can do the same, or send anything revealing in an attachment password protected Word document. You will get all the help you need for this at http://www.onlinecounselling4brits.com/resources/Tips+for+keeping+your+computer+safe+and+secure.pdf

  If you do have an email security breach you must inform all your clients immediately.
- **Make sure that you computer is password protected.** Keep all your passwords in a password protected Word or Excel document - that way you only have to remember one password!
- **Check where you are storing your data.** Make sure, if you are using cloud based services, that the servers are encrypted and based in the UK. If you are storing your client records in your computer make sure they are password protected, and likewise if you use an external hard drive.
- **Do a training.** You won't regret it as, whether you go for the bronze, gold or platinum level training you'll find great colleagues amongst your fellow students, and get heaps of help.

Not everything costs - three out of these five tips cost nothing to implement.

FINALE!

As you can see the issues of security, confidentiality and jurisdiction are complicated

This Information Sheet, a white paper, is designed to demonstrate that there is a lot of technical and policy detail involved, and a number of competing directions that you could take, which doesn't make the situaton any easier for the jobbing psychotherapist or counsellor, who just wants to get on with their job.

The technical detail relates to every aspect of software we are using in our online practices, and quite probably too, to some extent related to our face-to-face practice including the way we store our records or in the apps we are sharing with our clients, just as examples.

When we work therapeutically we need to know we have applied, as required by the DPA to the highest standards available. For example, when you are deciding which

cloud based solution to use for retaining your records you need to know where they are stored, and that there is the correct ISO certified certification for this.

Where there is competing advice the best advice I can give is it to take the best advice, the advice that demands the highest standard. Should you ever have a complaint against you for, say, not using a correct email protocol, you will need to demonstrate that when you undertook your risk management assessment that you thought through each of the issues concerning email communication, made a decision based of the level of risk, and implemented that decision.

As a further example you need to know that whatever video, audio, chat, forum etc context you are using to deliver your therapy that these comply to the required level of security. This is not necessarily obvious and you may need to read the small print and make enquiries. I withdrew from the Amercian platform mytherapy.net precisely because it was located in the USA and this meant that, without meaning to, even if I was working with British clients based in the UK via this platforms, I was somehow passing through American jurisdiction. This in turn brings its own issues as to work in any individual State in the USA you are required to have a State licence. It's just easier not to get involved in all that in the first place.

Furthermore we never know where we work in the world, (for example a client may tell you he is in Bath, but he mady be in Bahrain) and it is for this reason that I believe we need to ensure the software we use is ISO compliant to be protect our clients and their data wherever they may be.

The best advice I can give is for everyone working online or face-to-face to read tthe Data Protection Principles: https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/**.**

This Information Sheet has emphasised risk management and risk analysis. If you pay attention to completing of full and ongoing risk management policy you reduce your risks dramatically. If you feel you need help then ask for it, whatever you do, please do not bury your head in the sand.

A final point - nothing is FREE. Google sell all their data, Microsoft harvest all the data from Skype. These are just two examples of confidentiality breaches, and confidentiality is something that is covered within all the profssional membership organisations ethical principles and guideline : it is our duty to protect our clients' confidentiality at all times. Need I say more?