Windows 10 and it's all change again

Four security tips for protecting client information (PHI) and your practice

Written by Philippa Weitz, with a lot of help from the Roy Huggins Person-Centred Tech website: https://personcenteredtech.com/

Those of us who have trained to work online are very aware of the security issues surrounding the care of our client data .... But the arrival of Windows 10 brings new challenges for ***all counsellors and psychotherapists*** and without thinking about these issues you might easily and inadvertently, compromise your client's confidentiality. We are talking about **Protected Health Information**, "PHI" for short. **These recommendations are for every counsellor and psychotherapist using Windows 10, whether you work online or not.**

So what's the problem?

Windows 10 is designed to give you a joined-up interactive experience fully integrated with Microsoft online servers. This is likely to be the future of all matters digital leading to the Internet of things[1]. This is great for everyone except counsellors and psychotherapists (and other mental health professions) - for us it's a nightmare because, unintentionally, it means you may be sharing protected client information, PHI, without knowing it.

The problem here is that client PHI confidentiality needs to be maintained at all times – even though we may know that there is little risk as software developers – those most likely to see the data, aren't interested in our client data; but the confidentiality rules are the rules. In the UK every therapist is required to adhere to the Information Commissioner's Office Data Protection Act 1998 Principles[2], especially principle 7 which outlines the security requirements:

> *"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. »*

The heart of the problem is that the default position within Windows 10 is that your online Microsoft account links with your computer ... and automatically shares information with the online servers.

We can resolve these issues easily – and you'll be relieved to hear that there's no cost involved, you can make the necessary changes yourself, and sleep at night knowing you've done your best (which is what is required of us by the DPA) to protect your client data – PHI.

The rest of this article concerns settings changes you'll need to make to Windows 10 to ensure you protect your PHI. Don't worry, you won't need to be a techie to do this. Ideally you want to do this before you start using your computer with Windows 10.

There are 4 settings you need to change before using Windows 10. *Please note this article does not apply to any of the Windows software prior to Windows 10.*

TIP 1) Turn off "Wi-Fi Sense"

The point of Wi-Fi Sense is that you can share your various Wi-Fi networks with your contacts list. How many times have visited a friend's house, asked for the Wi-Fi code and lost the will to live typing in a long code and getting it wrong several times? Wi-Fi Sense means you never have to do tis again. You also no longer need to supply all your visitors with the relevant Wi-Fi code: Windows 10 automatically shares your Wi-Fi network codes with those on your contacts lists. At first glance that's great, but the bad news is that Wi-Fi Sense not only grabs your contacts listed in say Microsoft Outlook on your computer, but also, and this is the scary bit, grabs all your Facebook contacts, anyone you have listed as a Facebook Friend. OMG. The consequence of all this is that it appears that the baddies can exploit Wi-Fi Sense and get into places they shouldn't be ... such as your computer.

Advice: **Turn off Wi-Fi Sense**

How? Select the search bar and type "**WiFi**". When that page opens select "**Change WiFi Settings**". On the right-hand right under Wi-Fi just over half way down you'll see "Manage Wi-Fi settings". Select this option. This takes you directly into the WiFi Sense settings page. Turn off "**Connect to suggested open hotspots**" and "**Connect to networks shared by my contacts**". (Please note I have used WiFi and Wi-Fi as on the demonstration – sometimes it has a hyphen, sometimes not). That's all you need to do to turn off Wi-Fi Sense.

---

[1] https://en.wikipedia.org/wiki/Internet_of_Things, accessed 20/09/15

[2] https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/, accessed 20/09/2015

Tip 2: Use a computer based account, not. Web-based account.

Cloud based systems synchronise your diary, contacts etc . I find this so very useful: you put your appointment on your iPhone and voila, it's appears automatically on your iPad and computer. This can happen because our data is kept on web-based servers. The issue here is that your diary entries for therapies sessions with "Joanna Smith", or if you list her in your contacts, for example, compromise PHI confidentiality. Again this is inadvertently, but intended or not, the client confidentiality is breached under the DPA Principle 7.

Advice: Side-step the issue by creating a local account not connected to the cloud in any way. Don't worry, you will still have the original account and you can always change user and go and consult that if you have already started working on Windows 10.

How? This is the most difficult of the four tips. So I will number each of the stages:

1) Select the search area and type in "**User**".
2) A page with "**User Accounts**" as a title will come up. Select that.
3) That will take you to a page titled "**Make changes to your user account**". What you should see on that page, to the right, is your account with an email address underneath it. This is the problem. You want to create an account with no email address attached to it so that Windows 10 cannot send your data to its online servers – the downside is that you'll no longer be able to synchronise all your gadgets.
4) Click on "**Manage another account**" (middle column, most of the way down).
5) Select "**Add new user in PC settings**" at the bottom of the window.
6) On the next page, the bottom half concerns "**Other users**". Select "**Add someone else to this PC**".
7) The page "**How will this person sign in**" will then come up. IGNORE the box where you are asked to enter an email address for this user, and instead select "**The person who I want to add doesn't have an email address**". Hit "next".
8) The next page, "**Let's create an account**". Ignore EVERYTHING and hit the link on the bottom line "**Add a user without a Microsoft account**". Hit "Next".
9) This leads to the page "**Create an account for this PC**". Under "**Who's going to use this computer**" put in a user name, add a secure password – you're asked to put this in twice, and add a password hint. Hit "Next".
10) On the next page we can see at the bottom left that we have created a local account (i.e. not on the internet) with your chosen user name. We want to log in using this account (the local account with no email attached) rather than the original one with your email attached to it. Close the window, select the "**Start"** button, go up to your current user name (the one WITH your email address), and sign out.
11) Once you have signed out, it will take you to the Login screen. All the users will be listed at the bottom left. The User in the middle of the page is set to the last user who logged in, but without the password in the password box.
12) Select the new local account (the one without an email address) at the bottom left of the screen. You'll need to put in your password.
13) Once you're in, you can check you are using the right User account by selecting "**Start**", and at the top left of the screen you'll see the current user displayed, that should be your new local account.

Phew – hope you got all that! Well done if you did!

Tip 3: turn off the feature that provides the software company with feedback when there is a software problem.

No doubt you have, over the years, experienced the situation where your software programme / app crashes and you are offered the opportunity to provide the company with the information about this crash, they say to build their database of faults and to eliminate bugs. So far you have given permission for this but under Windows 10 it's a completely different scenario where the feedback is sent automatically AND also includes sending as much data as possible without any participation on your part, including sending your client PHI. Whilst the software company may not be interested in the data, here PHI, the security of PHI is compromised.

Advice: Change the feedback settings to "basic"

How: Select the Search bar. Type "**Feedback**". Under Settings select "**Feedback Settings**". On the next page under "**Diagnostic and usage data**", about half way down the page, change the option below from "**Full (Recommended)**" to "**Basic**". Just one word of caution, if your account isn't an administrator account you may need to ask the administrator to authorise this change.

Tip 4: Turn off sharing Profile information with apps

Again because you don't know how the apps are going to share information without requesting it, so it is a precaution to turn off this feature.

Advice: Turn off profile sharing

How: Select the Search bar and type "**Account Info**". Select "**Account info privacy settings**". Under Account info where it says "Let apps access my name, picture and other account info" change the setting to "**Off**".

Well done!

Find all this rather challenging? Help is at hand! PWT ACADEMY has courses to meet your needs

If you are interested in joining one of our courses or receiving some mentoring to get you up to speed, please contact us at info@PWTAcademy.Online