Confidentiality and remote working during the COVID-19 pandemic.

The Confidentiality Committee of the IPA has prepared this brief advice for IPA members who may be concerned about confidentiality while working remotely

Because of the COVID-19 pandemic many psychoanalysts have had to adapt rapidly to using remote technology, without any preparation or warning, in order to stay in contact with their patients and to continue to offer mental healthcare. Analysts and patients are using a variety of physical devices (phones, tablets, computers, routers, etc.) and software services (Skype, FaceTime, WhatsApp, Zoom, etc.), often without access to technical support. In the stress, uncertainty, and strangeness of this situation, IPA members are having to draw upon their internal resilience as well as the support of colleagues.

Confidentiality is at the heart of psychoanalysis. Unfortunately, no technology is fully secure. The risk of a breach of confidentiality may often be small but virtually all internet communications can be intercepted, material can be stolen or altered, and the consequences of a breach can be serious. Meeting regulatory requirements such as HIPAA (in the USA) or GDPR (in Europe) can help but it does not make the technology fully secure.

Simple steps can be taken to reduce the risk

These include:

- using strong passwords and changing them often;
- using a firewall; installing anti-virus software and keeping it updated;
- enabling any optional security features of the communication service you are using.

Steps like these will reduce the risk to confidentiality, just as hand-washing and social distancing reduce the risk of infection, but they cannot reduce it to zero. If you don't know how to do any of them, seek help if possible from someone who does.

Becoming better informed

The more IPA members can find out about cybersecurity, the better able they will be to protect themselves and their patients. Further useful information is widely available on the web, including in Section 4 of the *Report of the IPA Confidentiality Committee*,[1] and on the Surveillance Self Defence page of the Electronic Frontier Foundation.[2]

Transparency

Members may wish to discuss the confidentiality situation with their patients. One option could be to acknowledge openly both the impossibility of guaranteeing confidentiality and the limits to their understanding of the technology.

[1] https://www.ipa.world/IPA/en/IPA1/Confidentiality_Report_public_.aspx
[2] https://ssd.eff.org/

Further recommendations for improving security:

For those members who already have some knowledge of remote technology, the following additional notes may be helpful:

- Strong end-to-end encryption of all data (including live audio and video) is a desirable feature of any communication software or service. This means that information is disguised ('encrypted') while passing over the internet in a way which makes it difficult for anyone (e.g. a software supplier, service provider, 'hacker', or government agency) to have access to the intelligible content of a communication, even if they can successfully intercept it.

- Open-source software is preferable. This means that the source code of the software has been published and is open to scrutiny by the global community of cybersecurity professionals. It is therefore less likely to harbour hidden vulnerabilities, such as a built-in 'back door', than is software whose source code is kept private for commercial reasons.

- Effective end-point security is important. This refers to the security of the physical devices used by both analyst and patient, and is independent of any particular software or service being used for communication. In a corporate environment such as a hospital or university, where devices are supplied and managed by a central IT service, end-point security can be relatively well-controlled. For most analysts and patients this is not the case, so that their end-point security is *ad hoc*, and dependent on what they themselves are able to provide. The simple steps described above, of using passwords, a firewall, and anti-virus, and keeping exclusive control of personal devices, will close some of the gaps.

- Regulatory compliance (e.g. HIPAA or GDPR) should be treated with caution as indicators of relative security. For example, the HIPAA Security Rule only protects e-PHI (Electronic Protected Health Information), which does not include live audio or video communications. Genuine HIPAA-compliance may also impose considerable administrative and technical burdens on the practitioner, although these are being partially relaxed during the COVID-19 emergency.

Queries or comments?

If you have any queries or comments about this advice, please send them by email to the IPA Confidentiality Committee: *confidentiality@ipa.world*

First published 27th April 2020