Confidentiality and Remote Psychoanalytic Work

The Confidentiality Committee of the IPA has prepared this brief advice for IPA members who may be concerned about confidentiality while undertaking psychoanalytic work remotely. It revises and updates an earlier version that was published in April 2020.[1]

In early 2020, at the start of the COVID-19 pandemic, many psychoanalysts had to adapt rapidly to using remote technology, without any preparation or warning, in order to stay in contact with their patients and to have the option of continuing to offer mental healthcare. In the stress, uncertainty, and strangeness of the new situation, IPA members had to draw upon their internal resilience as well as the support of colleagues.

In the months that followed many analysts and patients have become more familiar with remote working and have adapted to it to varying degrees, but many difficulties are still experienced and the communication environment is constantly evolving. Analysts and patients across the world are using a variety of physical devices (phones, tablets, computers, routers, etc.), operating systems (Windows, MacOS, iOS, Android, Chrome, etc.) and software services (Skype, FaceTime, WhatsApp, Teams, Zoom, Signal, etc.), often with little or no access to technical support.

Confidentiality is essential to psychoanalysis. Maintaining confidentiality depends on protecting the privacy of communications between patient and analyst, and also between analysts when they discuss clinical material. Unfortunately, no communications technology is fully secure. The probability of a loss of privacy 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. Interception of any modality of communication is possible: video, audio, email, text messages, social media, etc. Privacy may be breached either within the internet itself or at the 'end-points' where analyst and patient (or analyst and analyst) are respectively located:

The risks of interception within the internet can be greatly mitigated by 'end-to-end encryption' (E2EE). This means that the content of communication is encrypted everywhere in the internet apart from the end-points, where it has to be intelligible. Properly administered, this ensures that communications intercepted in the internet will not be intelligible to any third party. Some systems use E2EE, and some don't. There have been false claims to use it (e.g. by Zoom in early 2020), so that whether a provider can be trusted is an important consideration in choosing which system to use.

The end-points of communication, where content is unencrypted, are harder to protect. End-point security involves protecting the devices that are used by each person (their computers, tablets, smartphones, etc.), as well as the local environments in which they are being used (e.g. a home or office), and restricting who has access to them. 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, however, this is not the case; their end-point security is *ad hoc*, and dependent on what equipment they can provide, and what arrangements they can make to protect themselves. For example, software is readily obtainable that

[1] Available here. This revised version takes into account advice provided by Ross Anderson FRS, Professor of Security Engineering at the University of Cambridge. Professor Anderson's full report is available here.

can record the keystrokes made on a device, or audio or video captured by its microphone or camera. Covertly installed on a device, such 'stalkerware' can breach end-point security.

General Tips for Improving the Protection of Confidentiality on the Internet

- Ensure that the *physical setting* at both ends is private, with no risk of analyst or patient being overheard or intruded upon. This may be more difficult to arrange for the patient than for the analyst, depending on their circumstances.

- If possible, use only systems that provide *end-to-end encryption* (E2EE).

- If possible, use *open-source software*, i.e. software whose code is made public and thus open to scrutiny by the global community of software engineers. Open-source software is less likely to include hidden 'back doors' that could allow eavesdropping.

- *Keep all software updated*. Software providers generally try to 'patch' new vulnerabilities as soon as they are found; hackers will exploit any left unpatched.

- Enable any *optional security features* of the communication service you are using, such as: in video-conferencing, locking meetings after everyone has arrived; using waiting rooms to vet attendees; requiring passcodes to enter meetings.

- Use *strong passwords*, both for your devices and for any applications or services you use. Your intuitions about the strength of memorable, non-random passwords can be wrong. Never use a simple, obvious password, however convenient. Consider storing your passwords in a password manager or in your browser. Further advice about passwords can be found in several of the links mentioned below.

- If possible, use a *dedicated device for communication with patients* and a separate device, which is never connected to the internet or only briefly as necessary, for administration, storage of notes, book-keeping, and so on.

- Keep to a minimum any confidential and/or identifying information that is communicated via the internet. Wherever feasible, use *pseudonyms or numeric codes* instead of actual names or other identifying details.

- Limit the risk of unauthorised access to devices or software by using *two-factor authentication* (2FA) where possible. For example, this involves requiring a user to login both on the device being used and on a separate device such as a cellphone.

- When working in-person in the office/consulting room, be aware of the possibility that any cellphone in the room, whether belonging to the patient or the analyst, could covertly be used as a monitoring or recording device, without the owner's knowledge, and possibly even after it has been powered off.

- Think through your arrangements for backup and recovery, and test them to make sure they work. You might need them one day if your system is hacked. Backups should be encrypted.

Steps like these will reduce the risks to confidentiality, just as hand-washing, social distancing, and ventilation reduce the risks of viral infection, but they cannot reduce them to zero. If you are uncertain about how to do any of them, seek help if possible from someone who does.

Becoming better informed

In general, the situation is complicated and constantly changing. The suggestions made above reflect our best current thinking but they could go out of date at any time. For this reason, and because the available expert advice is not always univocal, the more IPA members can find out about cybersecurity generally, the better able they will be to protect themselves and their patients. Further helpful guidance is widely and readily available on the web, and a selection of relevant links is appended.

Alternative clinical approaches to management of the risks

Psychoanalysts remain responsible for ensuring clinical confidentiality, even when they lack relevant understanding of the technology. The technology introduces a parameter which may affect a patient's trust that confidentiality can be maintained. Each analyst has to make a clinical judgement about how to approach these questions with each patient. Some will wish to discuss the situation with the patient, perhaps acknowledging both the impossibility of guaranteeing confidentiality and the limits to their own understanding of the technology. Others will prefer open-ended listening, exploration, and interpretation as ways of dealing with these issues, just as with any other aspect of the analytic situation. Psychoanalytic treatment online is too recent, and too much still in flux, for us to be confident in stating any general rules about how to make such choices in the here-and-now of ongoing treatments.

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*

Some useful links

BSI (Germany): *Home-Office aBSIchern? Geht ganz einfach*.
https://www.bsi.bund.de/DE/Themen/Kampagne-einfach-absichern/Home-Office/home-office_node.html

CCCS (Canada): *Cyber Security at Home and in The Office*
https://www.cyber.gc.ca/en/guidance/cyber-security-home-and-office-secure-your-devices-computers-and-networks-itsap00007

Ciberseguridad.com: *Guía de Ciberseguridad en el Sector Sanitario*
https://ciberseguridad.com/guias/sanidad/

CNCS (Portugal): *Cidadão Ciberinformado*
https://www.cncs.gov.pt/recursos/cidadao-ciberseguro/

EFF: *Surveillance Self Defence*
https://ssd.eff.org/

ESET: *Cómo crear una contraseña fuerte en un minuto y proteger tu identidad digital*
https://www.welivesecurity.com/la-es/2016/05/06/crear-contrasena-fuerte-un-minuto/

Gouvernement (France): *Conseil aux usagers*
https://www.gouvernement.fr/risques/conseils-aux-usagers

IPA: *Report of the IPA Confidentiality Committee* (2018)
https://www.ipa.world/IPA/en/IPA1/Confidentiality_Report_public_.aspx

NCSA (USA): *Stay Safe Online*
https://staysafeonline.org/stay-safe-online/

NCSC (UK): *Cyber Aware*
https://www.ncsc.gov.uk/section/information-for/individuals-families

NSA (USA): *Telework and Mobile Security Guidance*
https://www.nsa.gov/What-We-Do/Cybersecurity/Telework-and-Mobile-Security-Guidance/

OSI (Spain): *Empodérate: mantén seguros tus dispositivos y protégete en Internet*
https://www.osi.es/es/actualidad/blog/2021/03/08/empoderate-manten-seguros-tus-dispositivos-y-protegete-en-internet

First published 27th April 2020; this revised version published 10th May 2021