Confidentiality in the Administration of Psychoanalytic Practices Using the Internet

In response to the spread of Covid-19, a great many analysts moved to online forms of treatment and supervision. Some have returned to in-person meetings but with successive waves of the disease, many analysts continue to work online with some or all of their patients. Moreover, while administration of psychoanalytic practices had been done online in part or in whole by many analysts for some time, COVID has greatly accelerated the move to online administration. One result is that personal identifying information is now routinely transmitted online. This presents new and often unfamiliar threats to confidentiality.

The main administrative activities in which personal information is transmitted on the internet are:

- Making and changing appointments.
- Sending appointment reminders.
- Sending addresses and directions.
- Submitting forms and information.
- Billing for sessions.
- Paying for sessions.
- Sending receipts.
- When done on the internet, upkeep and storage of patient files.

In all these activities, some personal information is conveyed, at the very least the analysand's name and email address. Other kinds of identifying information that are communicated include: Names of patients; postal addresses; phone numbers; amounts of money involved; dates; kind of treatment (easily discerned from the name of the treating analyst); sometimes summary reports on diagnosis and treatment; and so on. Anyone who intercepts such internet transmissions will have access to highly confidential identifying information.

To manage the administration of their practices, analysts are more and more using commercial software packages ('apps') or packages available through professional associations and the information generated is often now stored on central servers, for example cloud computing sites. Thus, more and more, analysts are using similar administrative apps and the same central storage sites. This increases the risk of third-party intrusions because breaking into ('hacking') the app on one computer or one account on a central server gives the hacker everything needed to break into hundreds or even thousands of others.

In addition, many analysts use group or centralized book-keeping, billing, scheduling, and banking. These practices, too, are considerably riskier than the traditional single practitioner setup because a lot of personal information is stored all together in one central site. For example, in the Vastaamo case in Finland , a private psychotherapy clinic with thousands of patient records from hundreds of clinicians stored in an electronic data bank was broken ('hacked') into and this led to extortion directed at patients.[1] No psychoanalytic records were involved but easily could have been. Moreover, sometimes, as in this case, third-party centralized facilities have very poor security.

Individual patients will no doubt vary in their confidentiality requirements. Some will expect only the details of their financial transactions with their analyst to remain confidential while others will not

[1] See for example *The Guardian,* Oct. 26th, 2020 https://www.theguardian.com/world/2020/oct/26/tens-of-thousands-psychotherapy-records-hacked-in-finland/

wish anyone outside the analytic dyad even to know that they are in analysis, perhaps for reasons connected with personal relationships or because their job or profession would be threatened, or could be at some future date. Some patients fear (and others do not even realize) that any indication of mental health issues could cost them a security clearance, their job, prospects of promotion, or eligibility for insurance. Moreover, many analysts will regard all such information as confidential, even when the patient or a third party does not.

To sum up, electronic communications used in the administration of psychoanalysis almost always contain personal identifying information that must be protected. Even when the contents of communications are protected as well as possible, by sophisticated encryption for example, often at least the names of the therapist and patients will remain available for interception.

Risks can come from many directions. In some countries, governmental surveillance is a real risk. Surveillance is part of everyday life in some countries where new psychoanalytic groups are forming, as it has been in recent history in some areas of the *old* psychoanalytic world, and democratic governments can quickly become less so. Family members and friends who have access to the computer or other device that an analyst or patient is using for remote therapy or who can overhear conversations are a risk, probably the largest immediate risk for most analysts in times of COVID. Some government or private health insurance systems require reports from analysts that are stored on systems to which many others have access and over which the analyst has no control. Finally, some patients are in serious conflict with other individuals for personal or political reasons. In these cases, the risk is that such individuals with resources could intercept internet communications to and from the patient.

Because of the many risks, we recommend that analysts using the internet in the administration of their practices carefully consider confidentiality, taking into account individual patient's needs and interests, the physical arrangements at both ends, and the background socio-political environment.

Some IPA members are aware of the risks to their privacy online but are resigned to it, a kind of learned helplessness. Many other analysts feel that the internet is more private than it actually is – a feeling that social-media firms go to some lengths to engineer. Some just avoid the question. None of these attitudes leads to optimal protection of confidentiality.

This document has identified problems but has not offered solutions. See the document *Confidentiality and Remote Psychoanalytic Work* for practical tips for reducing risk here and in work on the internet in general.

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 10th May 2021