Report on Confidentiality for the Task Force on Psychoanalytic Training in Contemporary Times (TF2)

Written by the IPA Confidentiality Committee: Sarah Ackerman (chair), Susan Kattlove, Martin Teising (member until 31 July 2023), and John Churcher (consultant)

September 9, 2023

Confidentiality is fundamental to the psychoanalytic method in that without an analysand's awareness that her analyst is committed to protecting her privacy, both free association by the patient and evenly hovering attention by the analyst would be impossible. The protection of confidentiality is a dimension of ethics and is inseparable from our technique. Many aspects of our contemporary times, however, present potential impingements on confidentiality, both in "tele-sessions" and within the consulting room.

One profound risk to confidentiality is human error. Multiple, overlapping sources contribute to competing, unconscious drives that undermine our care for patient privacy, including narcissistic gratification and the pleasure of gossip, or the overwhelming burden of carrying our patients' secrets alone, or our own unconscious hatred of our patients or the work. Given these unconscious draws to breach patient confidentiality, we are prone to rationalizing our own infractions or enactments in this area. As we are exposed to breaches as candidates, where it is not uncommon for our own privacy to be compromised when the identity of our training analyst is often

widely disclosed, we then form our analytic identity along with an experience of porous boundaries around our own privacy. How are we able to support an ideal in which confidentiality is held sacred? Further, we have also all encountered analysts who succumb to the temptation to say too much about their patients, enacting micro-breaches of confidentiality that often fly under the radar and establish an unconscionable norm. The conventional waiting room, that liminal space between the analytic session and the outside world, presents a constant threat to patient privacy that is often disavowed. Additionally, there is the ever-present risk of technological parapraxes, where, for example, an email meant for one recipient can end up in someone else's inbox.

Along with this human dimension of the threat to our patients' confidentiality is the threat that emerges through the use of commercial web-based services to provide a platform for analytic sessions by phone or video. Just as there are unavoidable human risks to confidentiality due to unconscious processes that run counter to our overt intentions, there are systemic intrusions in tele-treatment that cannot be clearly identified, enumerated, or prevented—and that may not come to our attention until significantly later. Because the risks inherent in these platforms are not within the analyst's control, no action by the analyst can provide fail-safe protection against them. When third parties have access to stored data, the third party is essentially in the room. Recent history shows that there has been repeated misuse of stored data in the world

wide web even in high security areas (for example, the Pentagon). Confidentiality then is no longer a given in the space of the world wide web and therefore, psychoanalysis is radically compromised. With this in mind, we would like to declare that no treatment by phone or video platform can be resolved to be safe and secure. There are indeed growing analogous risks for in-person treatment, as our cellphones are increasingly susceptible to use as a surveillance procedure. It is our intention to raise awareness of the growing and evolving threats that emerging forms of technology pose to our psychoanalytic work.

Our recommendation regarding the use of technology to facilitate tele-analysis is that analysts be alert to the fact that these treatments are vulnerable to an array of threats. We are well aware that confidentiality exists within a group of ethical values, including an obligation to extend treatment and training to people who might otherwise not be able to access it—we see that we cannot only look at confidentiality as an isolated virtue. However, while there are undoubtedly cases in which the ethical precepts that might warrant tele-treatment could outweigh the unavoidable risks involved, analysts who use this technology should be ever attentive to and vigilant about the threats involved. In each instance, as an analyst clicks the link to begin the session, she should also be mindful of the possibility of an intrusion into the session, be it in from a government or other surveilling entity, or an eavesdropping family member or loved one at the patient's endpoint. The analyst should ensure that their software

complies with applicable regulatory requirements (e.g. HIPAA, or GDPR) and uses end-to-end encryption (E2EE), which 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, end-to-end encryption ensures that communications intercepted in the internet will not be intelligible to any third party. Skype is one example of a commonly used platform that has been thoroughly compromised in the past, is not automatically either HIPAA- or GDPR-compliant, and only provides E2EE as an option with limited functionality. We recommend that analysts rigorously keep abreast of evolving privacy, encryption, and confidentiality features of their preferred video platform, as revised standards can present an unexpected threat to the security of digital data. End-point security is an additional safeguard. This 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 (such as a home or office) and restricting who has access to them. Analysts must take responsibility for these technological dimensions of the work, and we believe that carefully considered, this responsibility should present a strong deterrence to offering tele-treatment. When appropriate, the risks inherent in tele-treatment should be addressed and thought through with patients.

Analysts might argue that the rigorous attention to technology that we recommend is beyond their skill set. To them, we would respond that if technology-

assisted treatment feels like a valuable opportunity, it also demands a broader skill set, one that includes attending to fine details surrounding encryption safeguards in the platforms that they utilize.

Confidentiality, which is constitutive of our work, is also—despite our best conscious efforts—always under threat. To protect it is a matter of ongoing effort, attention, and concern and not something that we can ever write off as adequately addressed. As threats to confidentiality multiply and grow in complexity, analysts may be susceptible to a corollary sense of fatigue, helplessness, or denial. We as a community of psychoanalysts need to find ways to disrupt this fatigue in order to promote best practices of attending to the ongoing and growing threats to confidentiality—within and beyond the consulting room. The Confidentiality Committee aims to highlight the risks that are endemic in tele-treatment, as many members of our community are not aware of them, nor attentive to the essential steps toward protecting confidentiality. These risks are often ignored or brushed aside, as we grow more comfortable—and more dependent—on the technology. More broadly, this committee wishes to encourage an ongoing concern with the "impossible" task of ensuring the privacy of our patients' most private conversations in contemporary times.