## Consultancy report by Professor Ross Anderson FRS

*Towards the end of 2020 the Confidentiality Committee of the IPA commissioned a report by Ross Anderson FRS, Professor of Security Engineering at the University of Cambridge. Professor Anderson was asked to review the contents of two documents published by the Committee which relate to confidentiality and cybersecurity in remote working by psychoanalysts, and to recommend any necessary or advisable changes. This document consists of Professor Anderson's report followed the specification to which it was written.*

*John Churcher*
*Chair, IPA Confidentiality Committee*
*14th January 2021*

## Confidentiality in Remote Clinical Practice

I have been asked by the International Psychoanalytical Association for help in updating the guidance given to members about the privacy, confidentiality and security of remote consultation, which has become rapidly more widespread as a result the pandemic.

I am asked to comment on two existing policy documents, and to suggest ways forward.

The context of the pandemic is of course new. People in the clinical and other professions have suddenly got a lot of experience in online consultation; it will take time to collate, analyse and synthesise our new knowledge of what works well, what works less well and what breaks. While preparing this document I therefore talked to a number of psychotherapists and other clinical professionals in the UK and overseas. I am Professor of Security Engineering at Cambridge and have worked at various times in the past 25 years on the safety and privacy of health IT as well as on surveillance and safety in multiple contexts. My CV and publications can all be found on my web page [1]. Much of my relevant experience has been systematised in my textbook ‘Security Engineering’ of which chapter 10 covers clinical systems and chapter 11 the difficulty of anonymising data [2].

### 1. The Interim Guidance

The first document on which I am asked to comment is the interim guidance the IPA issued in April 2020 [3]. This contains generally sound advice but could usefully be updated in the light of experience.

> 1. It is welcome that the guidance stresses the need for effective end-point security. This could be given more emphasis. Most attacks will involve compromise of either the patient’s privacy or the therapist’s rather than of the communications between them, and many compromises will not be technical. A child psychologist said her most frequent privacy concern was often whether a parent, step-parent or other adult was in earshot, or even in the room out of view of the camera. A surgeon noted that he had twice done phone appointments with patients who took an expected call in rather unexpected places: one in the supermarket, and the other while driving in their car. A GP noted that consultations often stray unexpectedly into psychological territory, and when the consultation is remote the clinician must be much more guarded if others may be present.
>
> 2. The most extreme threats to confidentiality that a therapist will encounter in practice are also likely to come from people close to the patient. Intimate partner abuse affects one in three women at some time in their lives (as well as one in six men); the patient may be a

victim of abuse, or even a perpetrator. If your abuser knows all your passwords, and your password recovery questions too, then passwords no longer authenticate you but them too. If your abuser can install stalkerware on your devices, whether by force or by fraud, things are even worse.

3. Much of the standard security advice becomes worthless or even counterproductive in such cases [4]. Deleting abusive messages destroys evidence that might be needed later in court. Disconnecting a compromised account and opening a new one can place the victim at immediate risk of serious harm. If a victim leaves a social network to escape, that may cut off social support on which they rely psychologically, and perhaps also their source of income. Patient privacy may also be compromised or constrained in less severe ways by non-abusive households. It is therefore desirable for a psychotherapist to understand each patient's vulnerability in detail.

4. Confidentiality may also be compromised at the therapist's end. The most serious reported case in 2020 was in Finland, where the Vastaamo clinic – offering psychotherapy to several tens of thousands of patients in twenty towns – had a server taken over by ransomware. After the owner declined to pay a ransom, the criminals contacted several hundred patients asking for ransom payments for their records; one victim was an MP. This got publicity in both Finland and Sweden in October 2020 [5]. We might consider this to be the reasonable worst-case scenario.

5. A compromise may also happen via the communications medium itself. This will normally only be a concern if the patient is of serious interest to a police or intelligence agency – such as a politically exposed person, someone in a sensitive government job, or someone suspected of serious crime. For practical purposes we can consider media to fall into three classes of vulnerability to wiretapping.

> a. At the first level is the 'plain old telephone service' which is not encrypted. As Snowden disclosed, it is common in many jurisdictions for governments to record phone calls and keep them for a week or so in case the police want to look back in time after a terrorist incident, drug bust etc.
>
> b. At the second level are services such as Skype and Teams which encrypt the communications from the endpoint device to a central server. The police can get access to such traffic with a warrant, but in most circumstances the access is targeted and not retrospective.
>
> c. At the third level are services such as WhatsApp, Signal and Facetime which encrypt traffic end-to-end in an attempt to resist even warranted collection.

6. In her book 'Screen Relations', Gillian Isaac Russell talks of a patient whom she treated in person while he was a diplomat posted at the US embassy in London, and then by Skype when his next posting was elsewhere [6]. Diplomats are routinely targeted by rival countries' intelligence agencies, so for such a patient it would be prudent to use Facetime or WhatsApp rather than Skype or Teams. One missing factor from the guidance is that the therapist should ideally anticipate whether a patient might be the target of attention by a capable motivated opponent.

7. In that case, just using Facetime instead of Skype might not be enough. An intelligence agency could try to install malware on either the analyst's device or the analysand's, or to gain access to whatever system the analyst used to keep notes. The analyst needs to think about endpoint security anyway, because of the risk of ransomware on their device or stalkerware on the patient's; but if the patient has capable motivated opponents then greater care is needed at both endpoints as well as with the choice of communications channel.

8. For clarity, it may be best to explain to analysts that there are, broadly speaking, four ways to keep sensitive records.

> a. First, notes may be kept under the analyst's sole control and on the premises using a well-understood physical mechanism, such as on paper in a safe.
>
> b. Second, notes may be kept in a computer on the analyst's premises, in which case control is more complicated: what combination of full disk encryption, automatic software update, AV software, and backup is sufficient given present and reasonably foreseeable threats?
>
> c. Third, notes may be kept under the analyst's control in a computer that is not on their premises, such as Office365. This may offer better technical protection, but may break local law if the records are held outside the jurisdiction. I will discuss this at greater length in the next section.
>
> d. Fourth, the analyst who is remunerated via a national health service, an insurance system or a private healthcare provider may be required to keep records on the purchaser's system.

9. The scope of the guidance should therefore be wider. Rather than just the security features of the communications service in use, the therapist should consider the environment at both endpoints, and any systems that record sensitive personal information. These environments may be less than ideal. In lockdown conditions, patients may have to take calls at home with earshot of other household members, or else while going for a walk. Therapists paid by insurance firms or a national health service may have to keep notes on systems to which many others have access, and over whose management and governance they have little say as individuals. One NHS employee even suggested to me that all sessions should be recorded for medico-legal reasons – which would create lots of very sensitive data with no obvious future use in the patient's interest. The growing incidence of ransomware attacks on healthcare providers worldwide makes such collections ever more a hostage to fortune, and they would need a solid legal and ethical basis. Professional associations can always push for compliance with privacy standards such as HIPAA in the USA and GDPR in Europe, as well as with applicable case law such as I v Finland; but these only go so far, and the gap that remains is a matter for ethics.

10. The pandemic has led to many healthcare organisations producing guidance on remote consultation. A number of these documents suggest that a clinician should always ask at the start of a call whether the patient is comfortable and private, whether there are others in earshot, whether they're using a speaker phone, and so on. When redrafting its own guidance, the Committee might care to look at some of the better examples offered by others [7].

11. Privacy is both a fact and a feeling (as discussed in the committee's report, chapter 2). Both matter, and they often diverge. What's more, the environment in which people take privacy decisions is not neutral; there are multiple interested parties and indeed there are deceptive players on all sides.

> a. Research shows that many if not most people are aware of their lack of privacy online but resigned to it, in a form of learned helplessness [8].
>
> b. One psychiatrist suggested to me that it's not just patients: many therapists are in denial about the general lack of trust in devices.
>
> c. People may often feel that an environment is more private than it actually is – and social-media firms go to some lengths to engineer this feeling, so that their users will volunteer ever more private information that can be used to target advertisements.
>
> d. In other circumstances people may be worried about surveillance where none exists, and with some patients this can be pathological. Some employers, and some governments, may exacerbate this by pretending that their surveillance capabilities are greater than they actually are.

12. The one recommendation in the Interim Guidance to which most security engineers would probably object is the advice to change passwords regularly. It has been known for many years that password aging policies tend to lead to weak passwords, such as 'kevin06' for June, 'kevin07' for July and so on. Unfortunately, in 2003 the US National Institute of Standards and Technology issued a standard calling for password aging, which the Big Four accountancy firms then tried to impose on their audit clients worldwide. Following substantial pushback from the security usability community, NIST recanted. It retracted its wrong advice in 2017, but the Big Four are still catching up. The IPA can be reassured by the fact that GCHQ's advice to system designers and operators is unequivocally against password aging [9].

13. The recommendation that people use anti-virus software is relevant for both therapists and patients using a device running Microsoft Windows, but is not that relevant for phones, tablets and Macs. It's important that all devices have their software updated regularly, and even for Windows laptops this is more important than running antivirus software (which can be got free from Microsoft). Modern phones and tablets restrict applications so that one application cannot interfere with another, so there's not much work that an antivirus program can do. The real risk is using an old device that no longer receives security updates.

14. One useful maxim is from Dame Fiona Caldicott: that in order to maintain trust, there should be *'no surprises for patients'* [10]. I might give three examples:

> a. The IPA's confidentiality project was prompted by a patient who sued after a description of their case appeared at a conference in a recognisable form;
>
> b. A patient who works as a diplomat should not be surprised by their security officer reprimanding them for having therapy over Skype;
>
> c. A patient in an abusive relationship should not be surprised by their abuser discovering the therapy via stalkerware installed covertly on their phone.

15. If the analyst is to avoid surprises, maintain trust and discharge their duty of care to the patient, then they need both cognitive and emotional sensitivity to the patient's circumstances and vulnerabilities, so that any privacy mechanisms (and rituals) can be tailored to their human needs. This sensitivity should include an awareness of the likely threat actors, given the patient's circumstances, be they hostile household members or hostile intelligence agencies. The former are by far the more likely.

16. Once the therapist understands the patient's context, and knows what privacy mechanisms may be appropriate, they need to know what the different available products can offer. The guidance might usefully spell out that its advice to support end-to-end encryption means "use Google Meet or WhatsApp or Signal rather than Skype" while advising people to use open-source software means "use Signal rather than Google Meet or WhatsApp". The framework suggested in 5(a)–(c) above may be helpful as a basis for developing such advice.

17. For advice to be useful, it also has to be actionable. And given that the privacy threats are more to the endpoints than to the communications between them – and given the rising level of ransomware attacks on healthcare providers – it's at least as important to consider the protection of machines on which records are kept. Here the framework in 8(a)–(d) above may be of some value.

18. All such advice needs to be kept up to date. For example, Zoom claimed to use end-to-end encryption but didn't, though now they say they've fixed that for one-to-one calls using the latest client software. (I discuss this in more detail in the next section.)

19. The real trade-offs between privacy and usability are quite subtle. Many clinicians prefer using a plain old telephone to an encrypted app, because the lack of delay and drop-out makes interaction and empathy easier. Others prefer a desktop app to a phone app because a laptop is more convenient than a phone. Others move from paper notes to computer so they can type as the patient talks, even though this might break their concentration.

20. For those patients for whom the very fact of a therapeutic relationship might be compromising, protection may have to extend to payment records too.

21. If a therapist decides to adopt the 'precautionary principle' of treating every patient as if they could be a current or future target of a capable motivated adversary (whether a state actor, a criminal gang or a tabloid newspaper), then this will place prudential constraints on the usable media (Signal rather than Skype), on usable devices (iPhone or iPad rather than Android), on patient record-keeping (paper rather than Office365) and potentially on payment mechanisms too. Even a traditional consulting room would have to be swept regularly for bugs.

22. A more realistic strategy is situational awareness: understanding when more caution is prudent, what form such caution might reasonably take, and the nature of the trade-offs not just in terms of cost and convenience but potentially in the quality of care and in the possibility of adverse consequences for the patient.

My recommendation is that the next version of the guidance should emphasise the need for the therapist to take a patient-centred view of privacy, considering both the reality and the perception of the threats in each patient's case. Many of the recommendations will be similar but they should be reframed make them more actionable in the setting of a real practice.

The guidance should also be designed to provoke thought and engagement by the analyst, rather than providing a checklist to be worked through as a ritual.

2. The Report of the IPA Confidentiality Committee: section 4.

The second document on which I have been asked to comment is the 2018 *Report of the IPA Confidentiality Committee*, and particularly Section 4. These comments expand in a number of respects on the comments made in section 1 above. Rather than giving extensive footnotes, I refer the reader to my *Security Engineering* textbook for more detail of the technical aspects of both privacy compromise and privacy protection.

This document notes in section 4.2 that where covert local surveillance is a fact of everyday life, privacy has always been more difficult to achieve. That used to be the case in repressive countries; the rapid growth in popularity of smart speakers, smart TVs and other devices with speech and gesture interfaces has led to the presence of microphones and cameras in most inhabited spaces on earth. Such sensors are more likely be more of a threat to privacy for most individuals than attacks on communications.

Section 4.3 notes that even in a traditional consulting room, the patient may be carrying a phone that has been compromised by spyware installed by their partner. It is reasonable to expect a psychotherapist to understand when a patient is exposed to such a risk. Devices can in theory be excluded from the consulting room, but even this might be inappropriate if it creates an atmosphere of paranoia rather than one of safety. Womens' refuge charities warn of abused women being ordered to take a phone into a GP consultation with an app set to record everything that's said; committee members might care to think through exactly how they would deal with such a situation were they to suspect it in their own consulting practice.

Where the patient is at home, they may have difficulty in achieving acoustic privacy even if they can find a place and time when they will be out of earshot of other household members. How does one deal with innocuous presence, such as young children coming into the room where the patient is talking on the phone to their therapist?

Section 4.3 notes the vulnerability of communications to interception and the fact that while most modern communications products support encryption, some are so poorly designed as to be easy to break, others lie about security, while many others offer law- enforcement access. It follows that an analyst and patient who are apprehensive about the authorities overhearing a session may wish to pay some attention to with the capabilities and operational practices of the police in their country (or countries). I discussed the options above on p2 at 5(a)–(c), and I can expand those comments now.

- The plain old telephone system (POTS) is unencrypted, while 2G mobile networks used weak encryption; 3G, 4G and 5G support law-enforcement access. Snowden and other whistleblowers have disclosed that the agencies have on occasion routinely stored domestic voice calls for a week and international calls for a month; calls to or from people of interest may be stored forever (as the report notes at section 4.5).

- Zoom initially lied about having end-to-end encryption but when people challenged them on this, they hired a security team and wrote new client software. Zoom now appears to be end-to-end encrypted when there are two people on a call and both use the Zoom client rather than a browser. Its products do still however rely to a concerning extent on servers in China.

• Skype used to offer end-to-end encryption but that stopped after Microsoft bought it; Microsoft complies with law-enforcement warrants worldwide (even in China). The committee's 2018 report noted Snowden disclosures of NSA access to Skype calls via Prism; this is an FBI facility for obtaining warranted access to data held by the US tech majors, and which was described in the Snowden papers as the NSA's most important single source of intelligence.

• Google and Facebook do not comply with Chinese warrants, because China demands access to everything regardless of probable cause. As a result, Google and Facebook are banned in China. Microsoft and Apple are not; Apple users in China have their data stored in iCloud services under Chinese control.

• It's not clear whether Google Meet offers end-to-end encryption of the kind that would resist a warrant. In view of the NSA/FBI access to Skype via Prism, it is quite possible that they have served a FISA warrant on Google to get similar access.

• Of the Facebook products, Messenger has encryption from the endpoints to Facebook's servers, and can therefore be collected with a warrant. WhatsApp currently has end-to-end encryption and causes problems for law enforcement. As a result, the EU has been pushing for access in the form of an 'upload filter' – essentially that content on WhatsApp should be scanned by the client software for child sex abuse material and potentially anything else on the local government's block list. Facebook is resisting this and talking about extending the end-to-end encryption used in WhatsApp to Messenger as well.

• The product used by security professionals is Signal. This uses end-to-end encryption and, unlike the other messaging and video-calling products mentioned here, is open source. This means that anyone can inspect the code to verify that the Signal team has not been compelled by a secret warrant to install a back door.

In short, it's complicated, and it changes frequently. It is very sensible that the Interim Guidance refers analysts to the EFF surveillance self-defence page [11]; the EFF has the expertise and the resources to keep up with developments.

Where a patient is politically exposed, or fears that they might be, it might be prudent to use Signal, Facetime or WhatsApp, instead of a more vulnerable product, and to take care that the devices used for both messaging and for record-keeping are patched up to date. Some celebrities and politically exposed persons might request that the practice records refer to them by pseudonyms. Where exceptional processes are invoked, the analyst should weigh not just the inconvenience but also any potential degradation in the quality of care.

Many analysts are therefore likely to communicate with most of their patients using phone calls, or by making video calls on laptop-friendly media such as Skype and Teams. There are also products designed specifically for healthcare use; the market winner in the UK appears to be AccuRx, as it provides a single portal for a clinician to deal with a patient using text, phone calls, photos and video, and without exposing the clinician's mobile phone number to the patient. Services such as Skype, Teams and AccuRx are vulnerable to warranted wiretapping by government agencies, but this often doesn’t matter; in the case of NHS patients using AccuRx, the authorities have complete access to their NHS records anyway.

For a confidential audio call, it is preferable to use Facetime, WhatsApp or Signal, as the call is then encrypted end-to-end. A determined investigator may still compromise one of the endpoints, but strong encryption transforms the problem from one of bulk collection with near-zero marginal cost per subject,in to one of a targeted attack that will only be undertaken for a reason. It also excludes the threat vector of government agencies trawling through billions of phone calls using speech-recognition software to index them for content and speaker-recognition software to identify speakers.

However the quality of an encrypted call may vary, and this is the case regardless of whether the encryption is end-to-end (as in WhatsApp) or merely from the device to the server (as with Skype). Sometimes it may have the immediacy of a normal phone call, while on other occasions there may be delay or drop-out. Rapport with the patient may therefore be degraded. If the patient does not have WiFi, encrypted calls will typically go over 4G and may cost the patient money.

Section 4.3 is quite right to note that endpoint security is critical, intractable, and frequently overlooked. As I discussed in the section on the Interim Guidance, this has to be considered at the patient’s end, and the therapist’s too. I noted the ransomware attack in Finland which affected tens of thousands of patients. There was also the UK care.data scandal where the records of about one billion NHS consultant episodes were sold to 1,200 organisations worldwide, ranging from university medical departments through drug companies to consultancies. The health sector is top of the league table in security breaches in the UK most years, and healthcare providers have been an attractive target worldwide for ransomware gangs who have scaled up their activities very rapidly since 2019.

Psychotherapists who are paid by national health or insurance systems, and are thus required to store patient notes on the purchasers’ systems, might have their professional associations investigate the security of these systems, particularly in view of the catastrophic failure of trust in Finland. This is not just a matter of technical testing and audit but of the architecture and the access control rules. Does everyone have access to everything? If that’s the policy, then enforcing it vigorously might not help much. It may be worth noting that many NHS systems give very wide access, and the reason that I v Finland became an important legal precedent is that, in the early 2000s, a hospital system in Helsinki let all clinicians see all patients’ records. The plaintiff in that case was a nurse who was HIV positive and was hounded from her job after her colleagues noted that she was seropositive. The decision of the European Court of Human Rights, in 2010, was that we Europeans have the right to restrict out personal health information to the clinicians who are involved directly in our care. It is a human right to be able to opt out of the use of one’s data for secondary uses such as research and service planning.

Analysts in private practice have to take full responsibility for their information security, despite the doubt expressed in section 4.7 of the report as to whether they have the skills. As discussed in 8(a)–(d) of my comments on the Interim Guidance, the options are to keep notes on paper and lock them up, to keep them in a computer on the premises, or to keep them on a cloud-based service such as Office365. To expand on this third option, many countries have regulations that restrict the overseas storage of some personal health information; Britain’s NHS is an example. The fact that Google does not possess a UK data centre means that everything stored on Google Docs or G Suite is overseas – this was one aspect of the care.data scandal. Microsoft used to offer the option of keeping Office365 data in the EU, but this is not relevant to the UK post-Brexit. National psychoanalytic associations might care to investigate local rules, explain them to members, and lobby for changes if need be.

The partial protections discussed in section 4.8 of the report are a mixed bag. Auditing with penetration testing is advisable for hospital systems used by hundreds of clinicians; but for an individual therapist in private practice, having a separate device for clinical audio and video calls may be a simple and robust strategy. As for case notes, it may be simplest to keep them on paper; if they're in a computer on the premises, it had better be properly protected. Any device used for clinical purposes, whether for communications or record storage, had better have its software patched up to date; older devices for which support has ceased should not be used for anything sensitive.

We might expect that the most common endpoint compromise of consultation privacy will occur at the patient's end rather than the therapist's. The most likely threat is acoustic, in the form of listening by the patient's household members or others nearby. The second most likely threat is targeted second-party surveillance by a current or former household member, which typically these days involves stalkerware installed on one of the patient's devices, but could also involve another device in the room. Given that an increasing number of devices have speech and gesture interfaces, most inhabited living spaces are starting to have multiple microphones and cameras, some of which can be abused for surveillance. Other threat actors in the patient's environment, such as third-party surveillance by the government or the press, are likely to come a fairly distant third to household members. A significant number of the psychotherapists and other clinical professionals to whom I spoke mentioned listening family members as a present concern; and there is increasing research into intimate partner abuse involving stalkerware.

If a patient might be a target of state surveillance, then the countermeasures required in the face of state-level threats are nontrivial. Even if the therapist and patient use encrypted communications, government agencies hack people's devices to listen in. In June we had press stories of how the French and Dutch police hacked over 40,000 'Encrochat' mobile phones which were largely used by organised crime, tapping their users for two months before they closed the system down. Thereafter hundreds of people were arrested in the UK for serious offences including the possession of drugs and firearms. It was also reported how the Crown Prince of Saudi Arabia hacked the iPhone of Amazon founder Jeff Bezos and disclosed his adultery, leading to the world's most expensive ever divorce.

Such exploits are unlikely to be directed at the typical residents of a democratic country. The operating rules of agencies such as GCHQ and the NSA oblige analysts to disregard personal information that is not relevant to an intelligence mission. And in democracies under the rule of law, one would also expect police investigators to disregard psychotherapy unless it were believed to be related to serious crime such as homicide.

It is true that democratic governments can quickly become less so; the lessons of Hong Kong, India, Poland, Hungary and indeed the USA should be noted. The UK is likely to leave the EU's data protection regime in practice, even if the government pretends for a while that UK law is equivalent. In such cases, the seizure of central record-keeping systems is a much more likely channel of large-scale oppression than the mining of stored telephone communications. It's a very much easier way to get sensitive data at scale.

In the case of celebrities, substantial threats can come from tabloid newspapers. If a patient is politically or culturally exposed, or likely to be a target for other reasons, then the therapist should pay attention to relevant resources, such as the surveillance self-defence page of the Electronic Frontier Foundation – which the interim advice already mentions. Section 4.6 of the report also correctly mentions the advisability of excluding all electronic devices from the consulting room for face-to-face meetings. (As I noted above, this may be easier said than done, once one thinks through likely use and abuse cases.)

All that said, the typical therapist should invest more time in thinking about patients who are, or might become, victims of privacy invasion by current and former household members – at all levels of seriousness from minor embarrassment through to serious threats to life.

Regardless of whether the threat is a suspicious stepfather or a suspicious state, some vulnerable patients might wish to keep secret the content of a consultation, while others will want to conceal the very fact of a therapeutic relationship. A controlling family member might see psychotherapy as an attempt to gather courage for an escape attempt. Some patients may fear that any indication of mental health issues might cost them their security clearance, their job, their prospects of promotion, or their ability to get insurance. In the traditional setting, such patients could walk to the therapist's office and pay cash. The electronic equivalents are not entirely straightforward.

Finally, even where the privacy concerns are modest, there is also a matter of security hygiene. The therapist and the patient should agree sensible rules of digital conduct that support effective therapy and privacy at the same time. There are many routines developed in the context of online medical care; for example, one GP phoning a patient will always ask the patient who they are (so they don't speak to a family member by mistake) and whether they're alone. If this is done every single time, then it's easy to handle the case where the answer is "My husband is with me" and the husband then asks "why did you ask that?" If either the therapist or the patient is distracted by multitasking on a device, or by other people in the room, this breaks empathy – on both sides. Having other apps open is also a direct privacy threat, as they may record audio. Doubtless many other considerations will emerge as we synthesise the experience of remote working during the pandemic.

Just as a therapist tries to create an analytic space in a familiar consulting room, it makes sense to try to create a virtual analytic space where there are no external surprises.

## 3. The Report of the IPA Confidentiality Committee: other sections.

I understand that the confidentiality committee was established following a case in which a patient saw details of their case discussed at an IPA conference. Outraged at the breach of confidentiality, they sued the IPA and won damages.

Section 3 therefore discusses sharing confidential material with colleagues after changing the details somewhat in an attempt to make the patient anonymous. This is very much harder than it seems; see chapter 11 of my book 'Security Engineering' for an up-to-date survey. Anya Proops' 2017 opinion for the IMA [12] notes that anonymised data could sometimes be shared under the pre-GDPR data protection regime; this goes back to the Source Informatics case. There, I was the BMA expert who examined the Source Informatics system: it protected the privacy of doctors in drug prescribing by making available only summary statistical information that had been carefully scrubbed to prevent inference not just about individual patients' prescriptions but about individual doctors' prescribing habits.

Such statistical database security techniques do not apply here as case data are too rich. It does not surprise me that 'despite a presenter's best efforts at disguising a case … some vital aspect of an analysand's identity will pop through.' This issue is discussed at a number of other points in the report (e.g., 2.4, 10.5) and I have experienced many similar discussions in other health IT contexts, and more than one other case where a patient came across a supposedly anonymous case study that was clearly and identifiably theirs or that of a family member. This can not only break the principle of not surprising the patient; it can destroy trust completely and lead to angry litigation. I noted above the I v Finland precedent in the European Court of Human Rights that patients have a right to requested that personal health information be limited to the clinicians performing their treatment. This is founded in s8 of the European Convention on Human Rights and applies to all Council of Europe countries (so it continues in force after Brexit). This is why UK NHS systems give patients an opt-out from the use of their data for secondary purposes including research and planning. Since 2018, the implementation of the General Data Protection Regulation (GDPR) has introduced a requirement that consent be explicit.

If a patient's case history is to be the subject of academic publication or professional training, then my understanding is that their consent must be sought not just as a matter of courtesy and of integrity, but – in European countries – of law. New patients in the NHS used be told something like *"we sometimes use patient data in research and may publish anonymised case studies. If you are not comfortable with this, please tick this box."* Thanks to GDPR, consent must now be explicit, in EU countries plus the UK. It is just a fact that some proportion of patients will insist that their material not be shared even in anonymised form. My experience both in security practice, in NGO work and on our university's research ethics committee leads me to side with examples 1 and 5 on pp 10–11 and against examples 2–4. The suggestions on pp 14–15 are not in my view adequate. I should state that I am not a lawyer, and that perhaps the IPA might care to obtain fresh legal advice to inform members on the state of play in the light of GDPR, and of the separate incorporation of the GDPR rules into UK law by the Data Protection Act 2018.

Section 5 discusses warranted access to patient records. It may be worth bearing in mind that if records are kept on a system controlled by someone else – whether an electronic health record system controlled by a hospital or insurer, or a cloud-based system such as Office365 – then the authorities can serve the warrant on the data controller or service provider rather than on them. If therapists want to ensure that all warrants are served on them in person, then they must be the only people with actual access to the notes.

Section 9 contains the report's recommendations. Those in section 9.1 relating to research presentations of clinical materials need to be rewritten to make clear to members that anonymisation is much harder than it looks, and in consequence case studies will usually require the patient's consent for their public presentation to be lawful. Those in section 9.2 relating to communications security should be rewritten to emphasise the security of both the patient's and the analyst's endpoints, and section 9.5 should also refer to the maintenance of adequate technical security mechanisms if records are stored electronically.

## 4. Ways forward.

It is sensible for the committee to update the Interim Guidance now that we all have much wider experience of remote psychotherapy and mental health care. As I discussed in section 1 above, the guidance might usefully become more patient-centric and concrete, encouraging therapists to try to understand their patients' individual risks and fears so that they can be dealt with in such a way as to maintain trust.

The confidentiality committee's report is comprehensive and thoughtful, and section 2 above has my detailed comments. The report's conclusions move generally in the right direction, though there is one serious misconception. It is wrong to believe that changing the details of a case slightly is enough to render a patient anonymous. For a security engineer, this is the most striking issue with the report. It is telling that a lawsuit from a patient whose personal information was exposed in this way was the spur for the report's creation. As I discussed in section 3 above, the IPA's response needs to be more thorough.

In 2018, the committee suggested a biennial review, to which this note is a contribution. I would encourage the IPA to solicit feedback from members about the experience they have gained during the pandemic with remote consulting. This might be more than just a reprise of the exercise reported on pages 43-45 of the report. Over a billion people now have experience of remote working, and over the next year or two we will be figuring out what worked better and what didn't. There will be much to learn beyond how threats to privacy, and attitudes to privacy, may have evolved. Remote working does indeed help some people (the shy, the excluded, the physically isolated), while some things are harder (rapport, empathy, team building). The IPA's members may have uniquely valuable insights to contribute to this learning process. This may be a great opportunity for psychanalysis to engage with the wider community, as recommended in section 9.6 of the report.

Ross Anderson

Cambridge, December 21st 2020

---

[1] See [https://www.ross-anderson.com](https://www.ross-anderson.com) or https://www.cl.cam.ac.uk/~rja14

[2] *'Security Engineering – A Guide to Building dependable Distributed Systems'*, Ross Anderson, 3rd edition, Wiley 2020

[3] *'Confidentiality and remote working during the COVID-19 pandemic',* IPA, April 27 2020

[4] 'Privacy threats in intimate relationships', Karen Levy, Bruce Schneier, *Journal of Cybersecurity* v 6 no 1 (2020)

[5] 'Therapy patients blackmailed for cash after clinic data breach', Zoe Kleinman, *BBC News*, 26 October 2020

[6] *'Screen Relations'*, Gillian Isaac Russell, Routledge 2015

[7] '*Principles for supporting high-quality video consultations by video in general practice during Covid-19'*, Royal College of General Practitioners, 20 Aug 2020, v2; NHS approval reference 001559; *'Oakley Health Group Remote Working Policy'*, Dr Neil Bhatia, 22 October 2020; *'Oakley Health Group AccuRx Photos and Video Consultation Policy',* Dr Neil Bhatia, 9 July 2020; *'A Practical Guide to Video Mental Health Consultation'*, Mental Health Online / Swinburne Institute of Technology, v1, 23 Mar 2020; *'Towards making the pandemic response data changes safe for the longer term*', MedConfidential.org, Sep 2020

[8] Security Engineering, above, section 8.6.7, pp 305ff

[9] '*Password administration for system owners*', National Cyber Security Centre,

*https://www.ncsc.gov.uk/collection/passwords/updating-your-approach*, downloaded 15 Dec 2020

[10] 'NHS data watchdog calls for 'no surprises' rule in use of patient info', Sam Trendall, *Civil Service World*, 26 June 2020

[11] See https://ssd.eff.org/

[12] 'In the matter of the International Psychoanalytical Association: confidentiality and informed consent in the context of a psychoanalyst's practice and their relationship with patients', A Proops, 7 April 2017

**Specification of a one-off consultancy**

*Consultant: Ross Anderson, Professor of Security Engineering, University of Cambridge*

(1) Review in detail the content of: (a) the short document *Confidentiality and remote working during the COVID-19 pandemic*, and (b) Section 4 of *Report of the IPA Confidentiality Committee*. Links to these documents are appended.

(2) Indicate any alterations that you consider necessary or advisable, with explanation of the reasons for each of these. An annotated version of the short document is attached, with specific questions which should be included among the points addressed.

(3) Provide a written report documenting your review. This should be written primarily for members of the IPA Confidentiality Committee, but it could eventually be made available to IPA members generally.

(4) The work to be completed as soon as possible, and not later than 15th December 2020.

John Churcher
Chair, IPA Confidentiality Committee
17th September 2020

-----------------------------------------------------

(a) *https://www.ipa.world/IPA/en/News/remote_confidentiality.aspx*
(b) *https://www.ipa.world/IPA/en/IPA1/Confidentiality_Report_public_.aspx*

| **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. | [See below re HIPAA, GDPR, etc.] |
| **Simple steps can be taken to reduce the risk** | |
| These include: | |
| • using strong passwords and changing them often; | Is there a simple, brief way of explaining 'strong' in this context?<br>If frequent changing of passwords is no longer advisable, why is this?<br>What advice can we give about password managers? How can someone choose a good stand-alone password manager?<br>Any other advice about passwords? |
| • using a firewall; installing anti-virus software and keeping it updated; | Is this still relevant? |
| • enabling any optional security features of the communication service you are using. | In what ways, if any, should this advice be more specific? |

| | |
|---|---|
| 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. | What does 'reduce the risk' mean here, how is it likely to be understood, and how might it be misunderstood? |
| **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] | Is the EFF document the best example to give here? Are there better ones? If we were to give 3 or 4 examples, which should they be? |
| **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. | |
| | |
| **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. | Do we need to distinguish between different 'kinds' of end-to-end encryption? Following the Zoom debacle, is the phrase 'end-to-end encryption' being used consistently and reliably by providers? |

[1] https://www.ipa.world/IPA/en/IPA1/Confidentiality_Report_public_.aspx

[2] https://ssd.eff.org/

| | |
|---|---|
| • 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. | Is this statement generally correct? Does it need qualification (e.g. with respect to choosing between operating systems)? |
| • 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. | The fact that most psychoanalytic practice takes place outwith a corporate environment is unlikely to change, so we have to assume that this *ad hoc* diversity of hardware and software provision will continue. Given this fact, is there anything more we can say about end-point security? |
| • 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. | Is this advice correct? The IPA is currently giving contradictory advice to its members about HIPAA-compliance: we are here drawing attention to its limitations, while a different committee is stating that it "assures confidentiality". We would like to ensure that IPA members have a realistic, consistent and well-informed understanding of this issue. |
| **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* | |