‘Everything can be hacked’ – protecting your clinical records

Tom Warnecke, EAP General Secretary

We live in a time of increasing digital record keeping, as well as a growing market for digital (“AI”) note taking services. Unfortunately, digital recording, or information processing of confidential informations also creates new risks for psychotherapists, and for our patients or clients. Major hacking incidents are frequently reported in the news and we have learned that “everything can be hacked”. Experts tell us that there is no fail-safe protection from “digital burglaries”. Due to the limited criminal gain opportunities, any digital records kept “in-house” by individual psychotherapists will most like only get exposed accidentally, rather than some hacker’s effort. But accidents do happen unfortunately so we should be diligent and never ignore such risks.

Large databases on the other hand are seen as “profitable targets” for hacking attempts, and not just in search of any financial information. To date, there has only been one reported psychotherapy-records hacking incident, the “Vastaamo” data breach in Finland, when the confidential records of 33.000 psychotherapy patients ended up in the public domain. The hacker was eventually found and jailed but the damage was done (patient records are reportedly still “out here”). But the damages and consequences were horrific. Numerous patients reported blackmail extortion incidents, at least one patient suicide is linked to this scandal, and the Finnish private psychotherapy provider company lost their business.

With increased use of digital media and a growing market of companies offering digital psychotherapy note taking or patient record services, the Vastaamo data breach will most likely not remain an isolated case unfortunately. Psychotherapist should therefore not only exercise great care with regard to digital records but also ensure that any services they contract should carry comprehensive liability insurance. Such corporate liability insurance should be designed to cover psychotherapist’s damages arising from any financial claims for damages (e.g. awarded by some civil lawsuit) against them in the event of a data breach.

We would also recommend that psychotherapists only use comprehensively encrypted cloud services for any confidential data backup storage, which offer significantly better security compared to “free” cloud service providers (such as “free” google or dropbox storage for example). Fully encrypted services come at a price but typically shield your records even within the hosting provider service itself (from a rouge employee for instance) and should be a worthwhile practice expense. Another common recommendation is to only keep confidential information stored on some removable medium (such as a USB stick) that can be easily removed to provide an additional security layer. Further information or recommendations can be found in references list below.

12 February 2026

References:

1. Wikipedia: https://en.wikipedia.org/wiki/Vastaamo_data_breach
2. *A faceless hacker stole my therapy notes – now my deepest secrets are online forever* - https://www.bbc.co.uk/news/articles/c62nzxqw45eo

3. *When confidentiality fails – lessons from the Vastaamo therapy records scandal* https://www.nelsonslaw.co.uk/when-confidentiality-fails-lessons-from-the-vastaamo-therapy-records-scandal/
4. Looi et.al. (2024) *Cybersecurity lessons from the Vastaamo psychotherapy data breach for psychiatrists and other mental healthcare providers*. Australas Psychiatry 33(1):106–110. doi: 10.1177/10398562241291340