Guideline on Data Privacy for Tele-practice

Version	Effective Date
1.0	31/08/2023

Document Number	**HKIST-ST-GDPTP**
Author	**HKIST Education Subcommittee**
Custodian	**Chairperson of HKIST Education Committee**
Approved / Endorsed By	**HKIST Professional Council**
Approval Date	**31/08/2023**

Content

1. Introduction

Traditionally, the face-to-face model has been considered the 'gold standard' of service delivery among both patients and health care professionals. Despite scientists have advocated for years digital health technologies as not only an alternative to face-to-face service delivery but also a solution for improving service coverage, tele-therapy in Hong Kong was considered not necessary given the easy transportation within the city. The pandemic has inevitably accelerated the acceptance of tele-therapy in Hong Kong, as during the lockdown, tele-therapy was taken as the 'mainstream' service delivery mode in different clinical settings. Since then, the advantages of conducting therapy online, such as extended service coverage, reduced costs, and improved flexibility of therapy time, has been identified. The wide acceptance of tele-therapy is also evidence by the fact that many stakeholders expressed their interests to extend the use of tele-therapy in Hong Kong even in the post-COVID-era. While practitioners and patients enjoy the benefits brought by the increased popularity of tele-therapy, there are also increased discussion regarding the potential risks associated with telehealth. One potential risk concerns the data privacy of tele-practice.

2. Risks

Data security and confidentiality issues are major concerns for both speech therapists and patients when telepractice is used. There are different common types of data security threat in telepractice:

(1) Data breaches

- Data breaches can be caused by malware, social engineering, phishing and ransomware attacks where hackers threaten to release sensitive or personal information. If there is an increase in the amount of patient information accessible through telemedicine services, then the probability of a potential data breach becomes higher.

(2) Insider threats

- Insiders who are within the organization of the speech therapists are another major threat to data security because they have legitimate access to patient information. Software glitches, human error, negligence, or rogue employees can result in data breaches or expose patient information to unauthorized users. To mitigate this threat, organizations should have strong monitoring, auditing, and reporting procedures in place to track and analyze insider activities.

(3) Denial of service attacks (DoS attacks)

- DoS attacks are cyber-assaults designed to take an organization's computer networks offline by overloading them with fake traffic. Hackers can take advantages of DoS attacks as a diversionary tactic for obtaining patient information illegally.

(4) Phishing scams

- Spoofing or faking a website which is known to the public is one of the tactics for phishing attacks. Such attacks trick users into giving up sensitive information under the guise of contacting their security provider to fix the problems which are non-existent.

(5) Malicious email attachments

- Malicious email attachments can be disguised as important documents, invoices or advertisements. These emails often encourage users to download the attachment to view, tricking them into opening the malicious file to infect user’s computers with malware which can cause data breaches.

(6) Advanced persistent threats (APT)

- APTs aim to steal data through malware placed on computer networks. APTs are usually designed by organized crime or high-skilled hackers. Proxies and other techniques are usually adopted by cyber-attackers to launch multi-phase attacks and maintain access to a network persistently.

(7) Mobile threats

- Phones and other portable devices are easy targets for hackers looking for easy access to protected health information due to users’ consistent use of them daily. Files with patients’ information that are not encrypted, and insecure web browsing can often lead to threats of data privacy.

(8) Unsecured devices

- The popularity of telepractice could expose more devices to hacking attacks if they are not properly protected, especially when the devices are not installed with firewalls and other data security measures.

(9) Internet of Things (IoT) threats

- Internet of Things (IoT) is a network of physical items implanted with electronics, software, and sensors that enable them to gather and share data. Improperly-protected devices which are within IoT may become a target for hackers that could cause leakage of patient information or other sensitive data.

3. Practical Recommendations

3.1 Client consent and education

- The therapist should obtain informed consent from the clients for telepractice clinical services.
- The therapist should inform the clients about the benefits, limitations, potential risks, and risk-prevention methods of telepractice clinical services.
- The therapist should check the genuine identity of the clients before beginning each clinical service; likewise, the therapist should educate the clients to check the genuine identity of the therapist before disclosing clinical information.
- The therapist should educate the clients to stay at a safe and private location when doing the telepractice session to protect their privacy, which could include: a private room at home, an appointment room at a school or institute, etc.
- The therapist should educate the clients to use a safe network, secure hardware devices, and to ensure security on network, cloud storage, and local computers (see below for details).

3.2 Legal obligations

- The therapist should refer to the Personal Data (Privacy) Ordinance (Cap. 486), and could refer to the following page for implementation principles: https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html
- The therapist should remain aware of the clients' right to access their personal

data recorded in whatever forms of telepractice communication.

- Any clinical data and records could be valuable than ever; and clinicians should restrain from using telepractice data and records for reasons not solicited with the clients.
- When working with clients outside Hong Kong, the therapist should comply with the law governing speech therapy services in the relevant jurisdictions where the clients receive the services. The therapist should check whether the Professional Indemnity Insurance covers the liability of their professional work conducted via telepractice and for clients located outside Hong Kong.

3.3 Choice of Network

- For both clinician side and client side: Never use public network for telepractice service, e.g.
  - Wi-Fi.HK
  - Café Wi-Fi even with password
  - guest or public Wi-Fi at schools or libraries
- For both clinician side and client side: Use firewalled network, and/or VPN
- For both clinician side and client side: Use Private Sim Card Cellular network to provide Hotspot Wi-Fi

3.4 Data at different stages

There are different types of data that must be kept secure:

a) Data in motion—data moving through a network (e.g., e-mail, data transferred during the video conference…)
b) Data at rest—data that is kept in clouds, servers, USB flash drives, etc.
c) Data in use—data that is in the process of being created, retrieved, updated, or deleted
d) Data disposed—data that has been discarded

3.4.1 Data in motion and in use Encryption (protection during data use or data transfer)

- The therapist should choose settings with encryption over the data in motion. Some reference pages are listed:

https://support.zoom.us/hc/en-us/articles/360048660871-End-to-end-E2EE-

encryption-for-meetings
https://www.hkcert.org/tc/blog/hkcert-proposes-10-measures-to-secure-zoom-meetings

3.4.2 Data at rest Encryption (cloud storage security)

- The therapist should pay attention if the telepractice clinical sessions are being audio- or video-recorded and stored on the Cloud, or stored in a local computer:
- For cloud storage, the therapist should ensure good encryption (i.e. even hacked, the coded data are not comprehended by the hacker)
- For local computer storage, the therapist should have clear understanding of the storing folder location, and have proper password protections for the recorded data

3.4.3 Data disposed Completion

- The therapist should pay attention if the data disposed is not recoverable by any third party (e.g. the files in Windows Recycle Bin are deleted permanently)

3.5 Routine computing behaviours

- The therapist should work from a private location such as the office or an appointment room. When working in a public location (never for telepractice clinical work), precautions should be made to protect clients' information.
- The therapist should store client information with password protection, even within privately owned computers or mobile devices.
- The therapist should set password to a strong, complex password, and change the password in a regular basis
- The therapist should update the computer system and video conference tools regularly
- The therapist should keep devices protected with updated antivirus software.
- The therapist should never open unrecognized emails or other instant messages, and never download from unknown websites or hyperlinks, to prevent hacker attacks or malware threats.
- The therapist should check the genuine identity of email senders before viewing the information; malicious emails commonly disguise themselves to

have important documents, invoices, or reputable brand names.

- The therapist should keep up with the latest knowledge and skills to ensure computer, data, and network security.

4. References

Bassan S. (2020). Data privacy considerations for telehealth consumers amid COVID-19. *Journal of law and the biosciences*, *7*(1), lsaa075. https://doi.org/10.1093/jlb/lsaa075

Office of the Privacy Commissioner for Personal Data Hong Kong. (2022). Privacy & Data Security in Digital Healthcare Environment. BMEG3103 Big Data in Healthcare.

Pool, J., Akhlaghpour, S., Fatehi, F., & Gray, L. C. (2022). Data privacy concerns and use of telehealth in the aged care context: An integrative review and research agenda. *International journal of medical informatics*, *160*, 104707. https://doi.org/10.1016/j.ijmedinf.2022.104707

Rosemol. (2021). “Data Security in Telemedicine: What You Need to Know”. https://www.cabotsolutions.com/data-security-in-telemedicine-what-you-need-to-know

The Medical Council of Hong Kong. (2019). Ethical Guidelines on Practice of Telemedicine. *Newsletter Issue No. 26.*

U.S. Department of Health and Human Services (HHS). (2023). “Telehealth privacy for patients”. https://telehealth.hhs.gov/patients/telehealth-privacy-for-patients