VIOS PRIVACY POLICY

GOOD FAITH EFFORT

Best Practices Guidelines to Ensure HIPAA/GDPR Compliance in Global Telemedicine

INFORMED CONSENT

An informed consent/waiver from every patient is taken digitally prior to selecting the calendly link of each provider.

A link to the legal documents of ViOS, Inc. which displays terms of use, compliance, diligence and related materials are provided to the patient via email prior to and upon confirmation of appointment booking.

DATA

Patient may request to delete any stored data in the mailing list of ViOS, Inc

Patients have been communicated that their personal data (eg. email addresses) may be used for providing billing invoices and/or digital marketing materials from time to time.

Providers who have undergone the initial virtual orientation training session will be permitted to be a part of the VIOS Provider Platform.

LOCATION SETTING

The scheduled session should take place in a private room such as the Provider’s study room or bedroom (that has been designated as a home office space)

There should be an obstructed view of screen i.e. not facing a door or window

Use of headphones during sessions may allow for added privacy during the scheduled sessions.

Laptop/PC that is being used should have separate user login and logout functions.

PROFILE ACCOUNTS

Personal mobile device (smartphone/tablet) with personal pincode/biometric access with auto screen lock features enabled when not in use.

The Providers' Gmail/Calendly/Zoom account must have a separate user login and logout feature.

The Provider must practice due diligence when utilising their devices for personal web browsing and downloading media.

The Provider must ensure timely software security upgrades of their devices as and when such security patches are made available.

Provider's full name and designation should be displayed on the Zoom profile as per their description in their provider bio page - Patient may choose to display their username as they wish.

Recommended reset of unique alphanumeric password every 30 days

RECORDING

No recording app/device must be activated in the background - patients and their chosen providers will receive a recorded zoom link after the session by their emails. This will ensure data localisation and portability to the geographic location of either party.

DATA

Patient health data can be shared only from the Patient's side - using the zoom chat box. This may take the form of a typed note, image file, PDF or a shareable link (eg. google drive/dropbox folder) from the Patient's side.

Providers are not to share any such data with any third party during or after a session is concluded.

Providers must discard any health data (PDF, data sharing links, image files) that has been shared to them, by shifting the data set into the recycle bin and immediately erase it within a period of 7 days has elapsed since the last communication with the patient.

NOTES

Providers may keep a handwritten journal during or after the session, for record keeping or further analysis if they choose to, this document should be written either during the session or immediately afterwards. The journal must be stored securely in the Provider's own desk space (under lock and key) or in a safe deposit box (you may treat this document as a bank cheque book).

The Patient may request for a copy of any notes that may have been taken by the Provider during the course of a session. The Patient should request a verbal request towards the end of the scheduled video session (prior to 30min duration) that they would like a photo scan of the Provider's notes.

The Provider can take a photo scan of any handwritten notes and upload via the Zoom chat box if the scheduled time permits, however if not possible, the Patient must book a follow up appointment to receive the previous session notes via the upload image function of the Zoom chat box.

This image file must be discarded by the Provider within 7 days from the device memory in entirety (i.e. permanent delete)

This professional journal may be maintained for a maximum duration of 6 Months, after which the provider is requested to discard the document in entirety by complete paper shredding, safely burning it or soaking in water until the ink is dissolved.

EXTERNAL COUNSEL

Providers are not to discuss VIOS Patient cases with any other healthcare provider, unless patient confidentiality is maintained by altering/omitting any personally identifiable data (using initials, synonyms etc) while seeking appropriate counsel.

Providers are requested to not accept or open any email correspondence from VIOS Patients with regards to medical/health data - only the ZOOM infrastructure has the appropriate HIPAA compliance via signed BAA (business associate agreement) with ViOS, Inc.

BREACH

Any incident of a data breach (eg. email hack) of any form should be communicated with ViOS, Inc via suitable means eg. secondary email or linkedin message with a representative of ViOS, Inc i.e. Dr. Ismail Sayeed within 72 hours of detection. An appropriate data breach communication will be undertaken by ViOS, Inc to concerned parties.

Any voluntary data breach by a Provider will require a disciplinary action to be taken on the offending party, related to ceasing all associations or legal repercussions as appropriate.

AUDIT

A data privacy audit will be carried out by ViOS, Inc by contracting out to a third party firm on an annual basis.

UPDATES

An annual privacy policy update will be made available to all parties as required.