Michael M. Zanoni, L.Ac.
Practitioner of Oriental Medicine and Acupuncture
3465 Waialae Ave #101
Honolulu HI 96816
(808) 225-2754

Patient Confidentiality and Electronic Medical Records Security Policy

January 2014

1. All patient records and information is held in confidence *as per* federal and state regulations. No current or historical medical or personal identifier information is released without your permission, or as required by law. If you are being treated as a result of a motor vehicle collision I may release medical information about the incident to your insurance carrier as allowed by your contractual agreement with them. If you are seen as a result of a work related injury I may release information to your employer's worker's compensation carrier and/or to the referring physician as allowed by statute.

2. If you are being seen by me and your treatment is covered by health insurance, with your permission I may release personal identifier information, appointment dates, treatment received, and diagnostic codes in order to send billing to the insurance carrier.

3. In cases where mandatory reporting laws apply, I have no option but to report certain situations without your permission to appropriate authorities. These are situations such as suspected child abuse, elder abuse, or neglect of the disabled.

4. When you are first seen as a patient, a paper record is created containing personal identifier information and your signature on an informed consent document. These records are stored in a locked cabinet away from my office.

5. The possibility of someone gaining access to your electronic medical records is quite remote. All chart notes and copies of correspondence are kept in computer files; no paper chart notes are created. These files are maintained at my office on a computer that is password protected and kept in a locked room when I am not present. Besides the computer being password protected, patient records are individually password protected and encrypted. Files are backed up online to a service where an additional password is necessary for access. For someone to gain access to your medical records by stealing the office computer, they would have to break the computer password and then break the password on the encrypted file. To gain access to your information from the online backup storage facility, someone would have to first break the password to the backup service, and then break the password to your file. I am the only person who knows the passwords, and they are not written anywhere.