

## CONFIDENTIALITY STATEMENT FOR PRACTITIONERS

***I, \_\_\_\_\_, understand that it is my responsibility as a Practitioner to protect, preserve, and maintain the confidentiality of patients and other Maui Health business information.***

### **Patient Information:**

All practitioners are responsible for maintaining the confidentiality of patient information and for preventing the unauthorized disclosure of any such information in accordance with the Health Insurance Portability and Accountability Act of 1996, P.L. 104-91 ("HIPAA") and the Privacy Rule issued by the Department of Health and Human Services (45 CFR Subparts 160 and 164) as well as other applicable State of Hawaii and federal laws and Maui Health policies and procedures.

The discussion or narration of any patient information of a personal nature, medical or otherwise, is strictly prohibited except as required in the regular course of work/placement. Such conversations should not take place in any public or semi-public area such as cafeterias, elevators (including staff elevators), lobbies, or waiting rooms, where one without a professional need to know might overhear. Such conversations should be held in a professional manner, only as appropriate and necessary to provide patient care, and never in the spirit of gossip or personal curiosity.

Accessing patient information (charted, computerized, etc.) is allowed only for the direct performance of the practitioner's duties. All other uses of such information are in direct violation of patient confidentiality, regulations, and policies. Patients have the right to expect all of their medical and other written information to be handled in a confidential manner at all times.

Maui Health practitioners, when utilizing the organization's medical services, have the same rights to confidentiality that other patients have.

### **Maui Health Business Information:**

No practitioner shall disclose information that by policy is not available to the public and/or that is acquired in the course of his/her work/placement with Maui Health. Medical staff member may not use such information for personal gain or for the benefit of another, such as another practitioner, a friend, spouse or relative.

If a practitioner is assigned a computer User Sign-on Code(s), in the performance of his/her duties, he/she is required to maintain the confidentiality of this code(s) under all circumstances.

### **Failure to Maintain Confidentiality**

I understand that any violation of these health care and business ethics constitutes grounds for disciplinary action, up to and including discharge (termination). In addition, Maui Health shall have the right to a) equitable and injunctive relief to prevent the unauthorized use or disclosure of confidential information and to b) damages resulting from disclosure and unauthorized use of same.

---

***I acknowledge, understand, and agree to abide by the foregoing and statements indicated on the supplemental document below.***

Print Name: **Last:** \_\_\_\_\_ **First:** \_\_\_\_\_ **MI:** \_\_\_\_\_

Title: \_\_\_\_\_

Signature  \_\_\_\_\_ Date: \_\_\_\_ | \_\_\_\_ | \_\_\_\_

***I AGREE THAT:***

1. I will protect the privacy of our patients, employees, and business information.
2. I will not misuse confidential information of patients, employees, or Maui Health (including confidential business and personnel information) and I will only access information I have been instructed or authorized to access to do my job. With respect to Protected Health Information, I will only access or use such information as it is necessary to provide medical care to the patient or as necessary for billing and payment or MHS operations.
3. I will not access my own or my family members' PHI. Instead, I will follow the same procedures that apply to all patients.
4. I will not share, change, remove or destroy any confidential information.
5. I understand that inappropriate or unauthorized access, use or disclosure of PHI may result in legally required reporting to governmental authorities, including my name.
6. I know that confidential information I learn on the job does not belong to me and that Maui Health may take away my access to confidential information at any time.
7. If I have access to electronic equipment and/or records, I will keep my computer password secret and I will not share it with any unauthorized individual. I am responsible if I fail to protect my password or other means of accessing confidential information.
8. I will not use anyone else's password to access any Maui Health information system.
9. I will lock my computer when I step away to prevent someone else accessing the computer under my logon. I understand that I am personally responsible for any accesses under my logon.
10. If I leave Maui Health, I will not share any confidential information that I learned or had access to.
11. When no longer being a practitioner with Maui Health, I will promptly return to Maui Health all originals and copies of documents containing Maui Health information or data in my possession or control.
12. I understand that I am responsible for my access, use, or misuse of confidential information and know that my access to confidential information may be audited.
13. I understand that the Medical Staff Office and/or the Compliance Office/Hot Line are available if I think someone is misusing confidential information or is misusing my password. I further understand that Maui Health will not tolerate any retaliation because I make such a report.
14. I understand that patient privacy and security is included in various training programs within Maui Health (for example: Annual Compliance Training), and by taking such training, I understand the obligations of confidentiality.
15. I understand that failure to comply with this agreement may result in disciplinary action up to and including termination of membership or other relationship with Maui Health. I understand that I may also be subject to other remedies allowed by law.
16. I understand that I must also comply with any laws, regulations, and other Maui Health policies, including the Code of Conduct, that address confidentiality.
17. By attesting, I agree that I have read, understand, and that I will comply with this Confidentiality Agreement.

**EXAMPLES OF BREACHES OF CONFIDENTIALITY (What I should NOT do)**

These are examples only and do not include all possible breaches of confidentiality.

- Unauthorized reading of patient account information.
- Unauthorized reading of a patient's chart, medical record, or medical information.
- Unauthorized access to my own medical information.
- Accessing medical information of friends, co-workers, family members, or anyone else, unless it is required for my job.
- Discussing confidential information in a public area such as a waiting room or elevator.

- Discussing or otherwise sharing confidential information with anyone in my personal life, including family members or friends.
- Accessing records for any reason other than for a legitimate business purpose.
- Accessing records of family, friends, co-workers, patients discussed in the media, well known political figures, celebrities, or anyone else about whom I am curious.
- Sending confidential information to my personal e-mail account, unless I am authorized to do so and the information is transmitted in accordance with required procedures (e.g., encrypted).
- Saving confidential electronic information to a MHS-owned or non-MHS-owned flash drive, CD, or any other removable or transportable storage device unless I first secure permission as outlined in the Secure Electronic Storage provisions of the MHS Information Security Policy.
- Saving confidential electronic information to a MHS-owned or non-MHS-owned workstation, laptop computer, personal digital assistant, or any other mobile computing device unless I first secure permission as outlined in the Secure Electronic Storage provisions of the MHS Information Security Policy.
- Using personal devices (digital cameras, camera phones) to take photographs that may include confidential information as the primary subject or in the background.
- Documenting or referencing confidential information on any social networking site, such as Twitter, Facebook.
- Telling a co-worker my password so that he or she can login to my work or workstation.
- Telling an unauthorized person, the access codes for employee files or patient accounts.
- Being away from my workstation while I am logged into an application, without locking my system to protect confidential information.
- Unauthorized use of a co-worker's password to logon to a Maui Health System information system.
- Unauthorized use of a user ID to access employee files or patient accounts.
- Allowing a co-worker to use my secured application\* for which he/she does not have access after I have logged in.

*\*secured application = any computer program that allows access to confidential information. A secured application usually requires a username and password to log in.*