



## HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) COMPLIANCE AND VIOLATIONS

The Sponsoring Institution endorses the Health Insurance Portability and Accountability Act (HIPAA) regulations, which protect the privacy of individually identifiable health information and set national standards for the security of electronic protected health information (PHI).<sup>1</sup>

1. **HIPAA Privacy Rule:** The HIPAA Privacy Rule protects the privacy of individually identifiable health information, called protected health information.<sup>2</sup>
2. **HIPAA Security Rule:** The Security Rule protects a subset of information covered by the Privacy Rule, which is all individually identifiable health information a covered entity creates, receives, maintains or transmits in electronic form.<sup>3</sup>
3. **HIPAA Breach Notification Rule<sup>4</sup>:** The Breach Notification Rule requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

All residents who perform clinical duties for their residency program sites are healthcare providers and members of the workforce of the program site (the healthcare provider facility/office) and thus are directly governed by HIPAA. Accordingly, each resident is responsible for understanding and fully complying with the HIPAA policies for the healthcare provider facility/office where the resident is assigned.

### **Security and Privacy Requirements**

Residents are required to follow the security and privacy measures in place at the program sites, Sponsoring Institution, and the employer, including but not limited to the following. Residents may be required to sign confidentiality and other agreements with these organizations that include these requirements. The obligations under these agreements will continue even after residents' association with the residency program has ended.

1. **Workforce Training and Management:** All incoming residents are required to attend a training session on HIPAA provided by the clinical sites.
2. **Information Access Management:** Use and disclosure of PHI is limited to the "minimum necessary". Access to PHI is authorized only when it is appropriate based on the user or recipient's work role.
3. **Workstation and Device Security:** Access codes/cards must not be given to any other individual. In addition, appropriate safeguards will be taken for any confidential information that is used for educational purposes; for example, facially de-identifying information to be used/removed for educational purposes, appropriate use of computer passwords, and appropriate destruction of materials.
4. Residents may not use, disclose, maintain, store, or transmit PHI in any manner that would violate the requirements of HIPAA.
5. Residents will not transmit PHI by email, fax, telephone, using a mobile device, over the

Internet, or by any insecure or open communication channel unless the transmission is encrypted using standards in compliance with HIPAA.

6. Residents must report activities by any person that he/she suspects may compromise the privacy or security of PHI. Reports made in good faith about such activities will be held in confidence to the extent appropriate for compliance needs.

### **Procedure for Addressing HIPAA Violations/Breaches**

1. ***As soon as an incident and/or breach is known*** (for example, misrouted patient information, misplaced patient list, stolen or misplaced laptop/iPad), the following persons ***must*** be notified:
  - a. Program Director/Program Administrator
  - b. Office of the DIO
  - c. Compliance Officer for the program site
  - d. Any other personnel of the Sponsoring Institution as may be provided for under the policies of the Sponsoring Institution
2. For stolen property, law enforcement officials such as the Honolulu Police Department should be notified, and the police report completed.
3. If electronic devices were stolen, misplaced, or otherwise compromised, passwords must be changed as soon as possible. In addition, all data on the device should be remotely deleted from stolen devices and as circumstances may warrant.
4. The incident and its circumstances must be documented.
5. Residents should be aware that Breaches of Unsecured Protected Health Information are required to be reported to the patient and to the Secretary of the Department of Health & Human Services within 60 days after discovery of the breach. The Compliance Officer for the program site will address according to the site's policy and procedures.

### **Sanctions for HIPAA Violations**

Violations of HIPAA requirements, including applicable policies of the Sponsoring Institution and/or applicable employment policies will subject the resident to disciplinary action, which will be imposed based on the nature of the violation (including, but not limited to, severity, whether it was intentional or unintentional, and whether the violation indicated a pattern or practice of improper use or disclosure). Penalties may include, but are not limited to, suspension or termination of residency participation or of access privileges at the healthcare provider's facility/office and personal legal liability. Disciplinary action may also be imposed by program sites.

At minimum, residents will be placed on Academic Notice for 90 days. With satisfactory performance during that period, a follow-up letter will be placed in the resident file stating that the resident has satisfactorily completed the period of Academic Notice. In addition, the residency program of the affected resident must provide HIPAA training to all their residents within 60 days of the breach.

**References:**

1. Health Information Privacy. <https://www.hhs.gov/hipaa/index.html> - Accessed January 14, 2022.
2. Summary of the HIPAA Privacy Rule. <http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html> Accessed November 1, 2021.
3. Summary of the HIPAA Security Rule. <http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html> Accessed November 1, 2021.
4. Summary of the HIPAA Breach Notification Rule. <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html> Accessed November 1, 2021.