

# **Sample Health Information Privacy Policy**

## **1. Purpose**

This policy establishes rules governing the access, use, and disclosure of personal health information by staff members. The objective is to protect patient privacy while allowing necessary access for the provision of care.

## **2. Authorized Access**

Access to personal health information is permitted **only when required for the direct provision of care** or for authorized administrative purposes.

Staff members **must not access patient records** unless they are directly involved in the patient's treatment or have been granted explicit authorization.

Unauthorized access to patient records, including viewing information out of curiosity or without a clinical need, is strictly prohibited.

## **3. Minimum Necessary Use**

When accessing personal health information, staff must limit access to **the minimum amount of information necessary** to perform their duties. Accessing records beyond what is required for care or operational needs constitutes a breach of this policy.

## **4. Disclosure of Information**

Personal health information must not be disclosed to unauthorized individuals.

Staff must take reasonable precautions to ensure that patient information is **not overheard, viewed, or accessed by individuals who are not authorized**, including other patients or visitors.

Discussions involving patient diagnoses, test results, or treatment details should occur **only in private settings** and only with staff members who are authorized to receive that information.

## **5. Monitoring and Auditing**

All access to electronic medical records is logged and subject to audit.

Access identified through audit processes that lacks a documented clinical or operational justification may result in disciplinary action.

## **6. Enforcement**

Violations of this policy may result in disciplinary measures, including retraining, suspension, or termination, depending on severity.