OFFICE OF HIPAA COMPLIANCE
CENTRAL MICHIGAN UNIVERSITY

HIPAA Guidance: Accessing Your Own or a Family Member's Medical Record

This guidance applies to all CMU HIPAA workforce members. It outlines when access to your own or a family member's record is permitted, when it is not, and which CMU policies govern such access.

When Access Is Permitted?

Accessing Electronic Medical Records (EMRs) is permitted only under the following circumstances:

1. Access as part of assigned job duties:
    a. You are viewing patient information necessary to perform your official job functions.
2. Access as a patient or legal representative:
    a. You are reviewing your own record or a family member's record for whom you are the legal representative, through the patient portal (MyChart), using standard patient access procedures.

When Access Is Not Permitted

Accessing EMRs without a job-related need or outside of authorized channels is strictly prohibited. You may not use your CMU-issued EMR credentials to access records for personal reasons, including:

1. Out of curiosity:
    a. You are viewing your own lab results in Epic instead of through a patient portal such as MyChart.
2. To help or check on a family member or friend:
    a. You are looking up your child's imaging results, appointment details, or provider notes.
3. For personal convenience:
    a. Printing a copy of a family member's immunization record for school or personal use.

Supporting CMU policies

The following CMU administrative policies provide the foundation for this guidance. These summaries do not replace a full review of each policy.

Policy 12-6: HIPAA – Use and Disclosure of Protected Health Information (PHI)

1. Use and disclosure of PHI must be limited to the minimum necessary to perform assigned job duties.
2. Any non-routine disclosure must be reviewed by the unit's HIPAA Representative to ensure it is permissible.

Policy 12-11: HIPAA – Individual Rights

1. Individuals have the right to request access to or copies of their own PHI.
2. Such requests must follow the approved process and be appropriately documented and reviewed.

Policy 12-13: HIPAA – Risk Management & Security Standards

1. CMU maintains safeguards to prevent, detect, and correct unauthorized access or misuse of ePHI.
2. Routine system activity monitoring is conducted to identify potential unauthorized access.