CATHOLIC MEDICAL CENTER
HUMAN RESOURCES POLICIES & PROCEDURES

CONSEQUENCES FOR INAPPROPRIATE ACCESS OR DISCLOSURE OF PHI AND OTHER CONFIDENTIAL INFORMATION

This policy provides guidelines and outlines the consequences for violations of CMC HIPAA, Information Security, and Confidentiality Policies.

Effective Date: 1/20/14
Last reviewed: 10/05/17

The purpose of this policy is to determine appropriate consequences, if any, for violation(s) of the Catholic Medical Center HIPAA, Information Security, and Confidentiality Policies. This policy applies to all CMC employees. For non-employed Medical Staff members, refer to Medical Staff Bylaws, Rule and Regulations, and Policies and Procedures.

Once a violation of a HIPAA, Information Security, or Confidentiality Policy has been ascertained, the following guidelines should be considered in determining appropriate consequences, if any.

NOTE: Immediate suspension of the violator's access to confidential information should be considered on a case-by-case basis, after consultation with Human Resources.

Definitions:

"HIPAA" is the Health Insurance Portability and Accountability Act and the Health Information Technology for Economic and Clinical Health Act, together with the implementing regulations including the HIPAA Privacy and Security Rules.

"PHI" or "Protected Health Information" includes all medical, personal, financial, and other information about a patient. This information includes, but is not limited to, the following:

- Demographic data, e.g., name, address, age, phone number, birth date, social security number, medical record number.
- Diagnostic/procedural data.
- Test results.
- All information and correspondence contained, or to be filed, in the medical record including notes, letters or reports concerning the examination, treatment and observation of patients, as well as conversations between patients and health care providers.
- Written correspondence and fax, E-mail or other electronic communication.
- Administrative and financial data.

Guidelines:

A. **Level I: Accidental minimal risk disclosures.**

Examples:

1. Improper disposal of PHI.
2. Leaving PHI in unsecured locations (e.g. paper medical records, laptops, jump drives, PDAs).
3. Not disclosing to Supervisor/HIPAA Privacy Officer any accidental disclosure or misplacement of PHI for purposes other than treatment, payment, or health care operations.
4. Failure to report a known or suspected privacy or data security breach.

Recommended Action

1. Retraining and re-evaluation of employee, with documented verification of each.
2. Verbal warning with discussion of policy and procedures.

B. **Level II: Accidental violation with associated potential for patient harm or harm to the organization.**

Examples:

1. Same as Level I above with the addition of: Accessing employee's own PHI or PHI of individuals for minors or others for whom an employee has health care authority.

Recommended Action

1. Retraining and re-evaluation of employee, with documented verification of each.
2. Written warning (including first and final warning if warranted), with discussion of policy and procedures.
3. Suspension or termination, if warranted, after consultation with Human Resources.

C. **Level III: Intentional violation with no associated potential for patient harm or harm to the organization.**

Examples:

1. Accessing or using PHI without having a legitimate need to do so (e.g., curiosity around a publicized case or about a person known to the employee or for any personal or private business reason), or specific patient consent (e.g., research).

2. Using another user's access code/password to access PHI.

3. Allowing another user to utilize an employee's own access code/password to access PHI.

4. Repeated Level I violations.

Recommended Action

1. Retraining and re-evaluation, with documented verification of each.

2. Written warning (including first and final warning if warranted) with discussion of policy.

3. Suspension or termination, if warranted, after consultation with Human Resources.

D. **Level IV: Intentional violation with associated potential for patient harm or harm to the organization.**

Examples:

1. Repeated Level II or III violations.

2. Disclosure of PHI to unauthorized individual or company.

3. Sale of PHI to any source.

4. Any use or disclosure that could result in harm to a patient.

5. Accessing the record of a patient without having a legitimate reason to do so and disclosure of this patient information.

6. Using another user's access/code password to disclose a patient's PHI.

7. Allowing another user to utilize and employee's own access code/password to disclose a patient's PHI.

Recommended Action

1. Suspension or termination, after consultation with Human Resources.

References:

Administrative Policies:

HIPAA related policies are listed in the Administrative Policy Manual and on the IS department intranet website.

Questions regarding this policy should be directed to the Human Resources department