CATHOLIC MEDICAL CENTER
HUMAN RESOURCES POLICIES AND PROCEDURES

CONFIDENTIALITY OF DATA

This policy describes the principle of confidentiality and the consequences if a breach of confidential data is committed.

Effective: 03/01/96
Date Last Reviewed: 10/12/19
Date Revised: 5/18/2020

Catholic Medical Center is committed to the principle of fair and ethical business practices and ensuring the utmost security and confidentiality of records and related information for all patients, employees, and organizational/administrative operations. To avoid any compromise of this principle, Catholic Medical Center will take necessary action with regard to any employee who views, discusses or reveals without authorization or valid business purpose, any information on patients, employees, or the organization.

All employees who have access to information pertinent to patients, employees, or organizational operations which is confidential in nature, is prohibited from discussing or revealing such information in an unauthorized manner. This includes, but not limited to, employee records, files, information gained from serving on Catholic Medical Center committees, inquiries from family and friends about patients, external agencies, media, automated or computer generated information, and, generally, any source of information an employee may encounter in performing the duties of their position.

Any breach of confidentiality, including, but not limited to, unauthorized discussion or revelation of information related to a patient, employee, or Catholic Medical Center operation, represents a failure to meet the professional and ethical standards expected of all employees, and constitutes a violation of this policy. Accessing, displaying, transmitting or communicating information for which there is no valid or authorized business purpose is considered a breach of this policy irrespective of its use. A breach of confidentiality need not take the form of a deliberate attempt to divulge confidential information, but will include the casual, unnecessary, or unauthorized, accessing discussion, exchange or communication of confidential information in any form.

Records and data which are expressly protected under this policy include, but are not limited to: medical records, appointment scheduling, payroll and personnel records, billing information, contracts, demographics, financial records, marketing and fund development strategies, and present or future business plans.

Logon IDs, access codes and passwords are strictly confidential and may not be disclosed or shared by anyone, except when a legitimate business need requires the temporary disclosure of a workstation password to allow an authorized person to access data resident within a device’s storage area.

Methods of disclosure include, but are not limited to: data transfer or transmission, verbal or written disclosures, news releases, faxes, documents left in full or partial view, including unattended, connected computer workstations. Employees with workstations in public areas must invoke password protected video display protection or logoff from their workstations when leaving the immediate area.

The Information Systems (I.S.) Group has implemented systems designed to maximize protection and minimize exposure to outside access while promoting valid commerce and communication with other institutions and individuals outside the organization. Examples of activities that could be in violation of data security and this policy include:

- Auto-forwarding work email to a non-CMC email address
- Use of a Virtual Private Network (VPN) client to bypass the system's firewall security
- Copying files from company systems to removable media (i.e., USB drive or CD) without approval of I.S.
- Syncing or copying files from company systems to cloud storage not managed by CMC (e.g., DropBox, OneDrive, or iCloud) without approval of I.S.

Employees will be reviewed annually on adherence to this policy and will be asked to sign a statement of understanding at the time of their performance evaluation.

Any violation of this policy will result in disciplinary action up to and including immediate termination of employment.

Questions regarding this policy should be directed to the Human Resources Department.