



## ***Information and Systems Confidentiality and Usage Agreement***

It is the policy of Boston Medical Center to protect all patients' rights of privacy. BMC is committed to its responsibility to always maintain full patient confidentiality as required by federal and state laws and regulations. In addition to patient health information, the Hospital has proprietary information, essential to its continued success; the confidentiality of this information must be protected as well. It is the responsibility of all person providing services at BMC to hold all this information in strict confidence.

### **No One Will Be Granted Access To Any Computer System Until This Form Is Signed.**

- **Confidentiality of Patient and Hospital Information**

Information known or contained in the patient's paper or computerized medical record shall be treated as confidential and will be released in appropriate circumstances only with the written consent of the patient or legal guardian. All persons providing services at Boston Medical Center who have access to information concerning patients including employees, staff, students and volunteers, must hold this information in strict confidence.

- **Communications:** Discussions and conversations regarding a patient's care and treatment are inherent in the provision of care, however, discretion is very important. It is the responsibility of all employees, staff, students and volunteers to refrain from discussing patients in inappropriate places, e.g., elevators, the hospital cafeteria, or electronic conferences. This information should not be discussed with anyone in the Hospital unless it pertains directly to his job, and then the discussion should be held away from public areas. Confidential information should never be discussed with anyone outside the hospital. Added discretion must be observed when communicating via E-mail or facsimile as these are not secure methods of communication. It is considered a breach of patient confidentiality to transmit patient information over the internet and the user will be subject to disciplinary action
- **Medical Records:** *The unauthorized possession, use, copying, reading or transmitting of paper or computerized medical records or the disclosure of any information contained in the medical record to unauthorized persons (including unauthorized employees, staff, students, or volunteers) is strictly forbidden.* Information generated through contact between patients and healthcare providers at the Hospital is privileged and confidential. This privilege extends to all forms and formats in which the information is maintained and stored, including, but not limited to, hard copy, photocopy, microfilm, or automated/electronic form. All persons accessing patient records must adhere to the following guidelines:
  - a. The information in a patient's record cannot be disclosed without the patient's knowledge and consent, however, there are occasions when there is a legal obligation or duty to disclose information. Requests for patient information from external sources must be directed to the Medical Records Department.

- b. Paper medical records must be signed out by an authorized person whenever they are removed from the department.
  - c. All paper records must be returned to the Medical Records Department.
  - d. Medical records must not be left unattended where unauthorized persons might read them
- **Hospital Information:** Access to patient, employee, and business information is a privilege granted on a need-to-know basis. Every user must sign the *Information and Systems Confidentiality and Usage Agreement* before access to any Computer system will be granted -- this includes medical students, volunteers, Boston Healthnet employees, consultants, business partners, and vendors who access our data. Some departments may require additional permission before access to a specific system is granted.

## II. BMC Computer Resources

Network and computer resources that access the BMC computer network are intended to be used for Hospital business. All policies that relate to acceptable and appropriate behavior at BMC apply as well to an employee's behavior when using computer resources, whether these resources are accessed from BUMC or from a remote site. **Anyone violating these policies shall be subject to disciplinary action up to and including termination.**

**Protection of Vendor Confidential Information** - BMC has acquired most of its hardware and software resources through purchases and licenses with outside vendors. Our agreements with these vendors legally obligate us to maintain the confidentiality of information identified by the vendors as confidential. It is your obligation not to disclose such information.

**Password Protection** - BMC uses individual password assignments to ensure the security of its information systems. It is your responsibility to protect the confidentiality of your password at all times. **Passwords must not be shared with others!** Anyone who knowingly allows another person to use his or her password, including another employee, staff or volunteer, will be subject to disciplinary action up to and including termination of employment. If you believe that your password is known to another person, it is your responsibility to notify the **Information Technology Client Services Help Desk at (x44500)** immediately so that the password may be changed.

BMC tracks system access and transactions using usernames/passwords and other means. Users are responsible for all transactions originating from his/her individual account. Audit trails created by user passwords will be used to determine accountability for confidentiality or privacy breaches..

Contractor access shall be in accordance with the *User Access Policy for Vendors And Business Partners*. Contractors, business partners, vendors, and other consultants will be issued temporary access. This access must be renewed every ninety (90) days.

**Willful Destruction of Data** - The data contained in the BMC information systems is vital to the operation of the Hospital. Any BMC employee or agent who engages in the willful destruction of data through deletion, alteration, or manipulation will be subject to disciplinary action up to and including immediate termination of employment or termination of the agency contract as applicable.

**Violation of Software Copyright Laws** - BMC abides by all commercial software copyright protection laws. Employees and agents of the Hospital may not violate any of these laws by illegally copying software that is so protected. Random and unannounced audits of BMC personal computers may be made at any time. All employees and agents are expected to fully cooperate with BMC authorized audits.

**Unauthorized Access** - Any unauthorized attempt to gain access to BMC computer systems or its network is considered a breach of security. Employees, staff, students and volunteers are prohibited from loading unauthorized software on any Hospital computer system. This includes computer viruses and any software application which interferes with the normal operations of the network or any computer system. Any BMC employee or agent who knowingly introduces a computer virus or attempts to breach system or network security will be subject to disciplinary action up to and including immediate termination of employment or termination of the agency contract as applicable.

**Use of the BMC E-mail System** - E-mail is a valuable means of communication which may dramatically enhance the quality of patient care. The confidentiality of patient and BMC proprietary information must be maintained in all E-mail communication as correspondence via E-mail is not guaranteed to be private. The BMC provided E-mail system is considered a hospital resource and is intended to be used for Hospital business purposes only. BMC treats all messages sent, received, and stored either on its E-mail system, or on the internet using its computer resources, as business records and reserves the right to access, review, copy and delete any messages. An E-mail message should be treated as if it is being sent under the BMC letterhead and with the understanding that it may be printed, forwarded, duplicated, and subpoenaed in legal proceedings.

**Use of the Internet** - BMC provides access to the internet at its expense to support and enhance its business, academic, and research pursuits. The internet offers the opportunity to communicate and collaborate with colleagues around the world faster and at a lower cost than traditional means. Access to the internet is considered a privileged use of a Hospital resource and is intended for business uses only. Use of the internet may be monitored for security and network management reasons.

**Some examples of prohibited use of BMC computer resources:**

1. Impersonating another person by sending forged messages.
2. Soliciting non-hospital business for personal gain
3. Intentionally interfering with the normal operation of the network, including introducing and propagating computer viruses and sustained high volume network traffic such as chain letters
4. Using the E-mail system for illegal or unethical purposes
5. Revealing or publicizing any proprietary or confidential information such as patient information, financial information, or system or network access codes.
6. Sending, receiving, or storing any messages or files that are discriminatory, offensive, obscene, defamatory, pornographic, or harassing.

## **USER AGREEMENT**

I agree to comply with the Boston Medical Center **Information and Systems Confidentiality and Usage Agreement** and with the specific terms of any contract governing my relationship with Boston Medical Center.

I agree to restrict my use and retrieval of information to information that I have been specifically granted access under the terms of any contractual agreements with Boston Medical Center.

I will not use or knowingly permit the use of any access control mechanism (e.g., log-in ID, password, terminal ID, user IDs) for any purpose other than that required to perform authorized duties.

I agree that any access control mechanism issued to me is for my exclusive use. Further, I agree that I shall not share my access control mechanism with others nor shall I delegate its use to others.

I will not use any access control mechanism which has not been expressly assigned to me by ITS.

I have read the above **Information and Systems Confidentiality and Usage Agreement**. I understand my responsibilities and will abide by all the provisions set out in this policy.

**Name:** \_\_\_\_\_

**Institution:** \_\_\_\_\_

**Signature:** \_\_\_\_\_

**Date:** \_\_\_\_\_

**Telephone:** ( ) \_\_\_\_\_

**Beeper:** ( ) \_\_\_\_\_

**Employee Number or Agency Agreement:** \_\_\_\_\_

*If you need assistance, please call*

**BMC Information Technology Client Services Help Desk @ (617) 414-4500,**

OR visit our online page: <http://internal.bmc.org/helpdesk/>