

Boston Medical Center: HIPAA Privacy Awareness

The Health Insurance Portability and Accountability Act of 1996, (HIPAA) Privacy Rule, requires Boston Medical Center (BMC) to safeguard the confidentiality and privacy of the medical records and other individually identifiable health information. The Privacy rules reinforces the values of BMC and builds on protections that BMC already considers important---: protecting the privacy and confidentiality of health information is a responsibility of every member of the BMC workforce. Whether you work directly with patients, perform another role or volunteers at BMC, you are responsible for respecting patient rights to privacy and for maintaining the confidentiality of the information. The purpose of this document is to remind you of some of our key practices and how to obtain resources to answer your questions or concerns.

Key Points

Protected Health Information (PHI) includes information about a patient or an individual in any form (oral, paper or electronic). This is information about one's identity, physical condition, emotional and financial status. We are allowed to use (internally) or disclose (exchange information with anyone outside the BMC workforce) PHI for purposes of *treatment, payment, healthcare operations and other situations as required by law only*. For any other use or disclosure, a HIPAA compliant authorization is required. Otherwise, patient information should only be disclosed or shared on a *need-to-know* basis only, that is, the information is needed in order to perform one's job responsibility.

In addition to the above, please be aware of the following:

- Conversations about or with patients should be conducted whenever possible behind closed doors, curtains, or at a minimum in lowered voice levels when others are present
- If you access patient information on BMC computer systems, never share your passwords, logoff whenever you leave the monitor, and wherever possible, keep the monitor screen facing away from public areas
- PHI should not be left out in the open, on counter tops, or where others without a need- to-know might see it.
- Personal databases containing PHI is prohibited unless: they support TPO, contain "de-identified information (as per HIPAA definition) or has IRB approval
- Data should be on secure machine or network file area—not the "C" drive
- E-mail containing patient identifiable information is not secured when sent via the internet unless both parties are using encryption technology
- Fax machines are the least controllable type of communication, it is critically important when faxing information: to verify the sender has the correct fax number, the fax machine is in a secured location and/or the receiver is available to collect the information immediately.
- Likewise, when receiving faxed patient information, immediately remove the fax transmission from the fax machine, and deliver it to the recipient. If information is sent in error, immediately inform the sender, and destroy the faxed information (deposit in shredding bin, ripped up document)
- Your responsibility for protecting patient privacy and confidentiality does not end with your work shift: Don't divulge any patient information when in an informal or social atmosphere. When asked, reply by saying, "I'm sorry that information is confidential".
- For additional Privacy Resources: visit the BMC Intranet, Privacy @ Work, BMC Policy & Procedures, (Administrative section) HIPAA Alert newsletter, BMC Employees Dos & Don'ts, Training Resources
- Internet Sites: Dept. of Health & Human Services, <http://aspe.hhs.gov/ocr/hipaa/whatsnew.html>, <http://library.ahima.org>
- Mass Health Data Consortium, <http://mahealthdata.org>

Contacts:

If a patient has a question or an issue:

Please refer all patient complaints to the BMC Patient Advocacy Program: 4-4970. Please refer all patient questions to either your supervisor or the Privacy Officer, 4-1800 or Privacy Officer@bmc.org

If you have question

For information, please see your supervisor, or check the BMC Intranet, @Work. The BMC Privacy Officer is available to answer any questions and address concerns: 4-1800 or PrivacyOfficer@bmc.org