

Patient Confidentiality, Privacy, and Security Awareness

Boston Medical Center

Goal

This training module has been developed to help the Boston Medical Center workforce be able to articulate their duties and responsibilities with regards to:

- Patient Confidentiality
- Patient Privacy
- Secure Computing
- Breach Responsibilities

Confidentiality

Everyone in the organization is responsible for patient confidentiality

- Board members
- Executive leadership
- Clinical staff
- Physicians and nurses
- Administrative and clerical staff
- Students and interns
- Volunteers

***This helps us achieve our mission of
Exceptional Care. Without Exception.***

Confidentiality

The following is a list of patient information that must remain confidential

- **Identity** (e.g. name, address, social security #, date of birth, etc.)
- **Physical** condition
- **Emotional** condition
- **Financial** information

Confidentiality

Guiding Principles

- Access patient information only if there is a 'Need to Know'
- Discard confidential information appropriately
 - (e.g. Locked Trash Bins or Shredders)
- Forward requests for medical records to the Health Information Management Department.
- Do not discuss confidential matters where others might over hear.
 - (e.g. Cafeteria, Elevator, Buses, or Restaurants)
- Do not leave patients charts or files unattended
- Report suspicious activities that may compromise patient confidentiality to the BMC Privacy Officer

Privacy

State & Federal Laws that Protect Patient Privacy

- Health Insurance Portability & Accountability Act of 1996 (HIPAA)
&
American Recovery and Reinvestment Act of 2009 (ARRA) – HITECT
breach notification provisions
- Massachusetts regulations and statues
 - Patient Bill of Rights
 - 201 CMR 17.00 Standards for the Protection of Personal Information
- The Privacy Act of 1974

Many of our patients are also our neighbors, our friends, and our co-workers. Maintaining their privacy is essential.

Privacy

What is the purpose of HIPAA?

Improve the efficiency and effectiveness of the health care system

- Encourage the development of an electronic health record
- Establish national standards for electronic transmission of certain health information
- Establish national standards to protect health information

Ensure patient confidentiality

- Protect patient privacy
- Build loyalty and trust
- Provide exceptional customer service

Privacy

What is PHI?

PHI stands for Protected Health Information and includes demographic information that identifies an individual and

- Is created or received by a health care provider, health plan, employer, or health care clearinghouse.
- Relates to the past, present, or future physical or mental health or condition of an individual.
- Describes the past, present or future payment for the provision of health care to an individual.

Privacy

Who has to follow HIPAA?

Anyone who:

- Currently works directly with patients
- Currently sees, uses, or shares PHI as a part of their job
- Currently access any hospital systems, records, tools, and information that may contain PHI

The entire Boston Medical Center workforce is responsible for protecting the privacy of our patients and upholding all HIPAA Privacy & Security Rules

Privacy

HIPAA Defines these 18 Elements PHI Identifiers

1. **Name**
2. Full face photo
3. Finger or voice print
4. Telephone number
5. **Address/zip code**
6. E-mail address
7. Fax number
8. Internet Protocol (IP) address
9. Uniform Resource Locator (URL)
10. **Social security number**
11. Medical record number
12. Insurance number
13. Account number
14. All elements of dates
15. Vehicle identifier
16. Certificate/license
17. Device ID/serial number
18. Any unique identifying number, characteristics or code

Printed materials containing any of these identifiers should not be discarded in the trash. They should be either shredded or placed in locked recycling containers.

Privacy

Where is PHI Found?

- Medical records
- Patient information systems
- Billing information (bills, receipts, EOBs, etc.)
- Test results
- X-rays
- Clinic lists
- Labels on IV bags
- Patient menus
- Conversations
- Telephone notes (in certain situations)
- Patient information on a mobile device

Privacy

Permitted Uses and Disclosures of PHI Include:

- **Treatment** of the patient
 - Direct patient care
 - Coordination of care
 - Consultations
 - Referrals to other health care providers
- **Payment** of healthcare bills
- **Operations** related to healthcare
- **Research** when approved by an Institutional Review Board (IRB)
- **Required by law** (e.g. subpoena, court order, etc.)

Need-to-know

Employees should only use/access the “**minimum necessary**” information to perform their jobs

Privacy

Patient Rights

- **Right to Access**
 - Any information contained in their medical and billing record
- **Right to Amend**
 - Patients may request in writing, an amendment to their medical records if they feel it contains incorrect or incomplete information
- **Right to an Account of Un-Authorized Disclosures**
 - Patients have the right to receive a list of disclosures (information released outside of BMC), other than for treatment, payment, or operations
- **Right to Request Special Communications**
 - Patients may ask BMC to contact them via an alternative phone number or address

Privacy

Patient Rights (continued)

- **Right to Request Restrictions**

- Patients may request not to be included (opt-out) in the directory. Patient information should not be shared with clergy, friends, or anyone

- **Right to Receive a Notice of Privacy Practices**

- BMC is required to provide a written notice of how we will use and disclose our patients health information

- **Right to File a Complaint**

- Patients have the right to file a complaint without fear of retaliation

Security

- When we protect patient data, we help build trust between patients and providers.
- Ensure Protected Health Information (PHI) is not disclosed to unauthorized persons.
- Do not send email containing Protected Health Information (PHI) unless it is encrypted.
- Log off your computer if you have to leave your workstation.
 - To log off, press the **Control-Alt-Delete** keys at the same time on the key board and then choose **Log Off**.
- If you suspect someone is using your login ID, you must report it to the Help Desk (x 4-4500) **immediately**.

Security

Passwords are only effective if they are **NEVER** shared, and if the guidelines for creating a strong passwords are followed.

Strong passwords

- must be at least eight characters long
 - use mixed upper and lower case letters
 - incorporate at least one number
 - do not contain repeating or consecutive letters or numbers (e.g. 1243 or aaabb)
 - are not common words or phrases
-
- Do not share your password with anyone including co-workers, supervisors, or the Help Desk.
 - Do not write down your passwords or include passwords in emails.

Breach Awareness

A breach may have occurred if there has been an unauthorized acquisition, access, use or disclosure of PHI (written, oral, or electronic), that poses a significant risk of financial, reputational, or other harm to a patient.

*It is your **responsibility to report** incidents to your supervisor or the BMC Privacy Officer, if you suspect a patient's Protected Health Information (PHI) might have been acquired, accessed, used or disclosed without authorization.*

Breach Examples

- Employees viewing their own and their minor children's medical record
- Leaving patient identifiable information in public areas (by reception desk, visible computer screens, copiers)
- An employee checking a co-worker's record to look up a birthday or address
- Discussing PHI in a public place where it could be overheard by others
- Inappropriately accessing or disclosing patient information
- Lost, stolen or misplaced laptops and flash drives containing unsecured PHI.

Breach Consequences

Members of the workforce who fail to follow and uphold Boston Medical Centers privacy and security policies, will be subject to appropriate disciplinary action, up to and including **termination**.

Tips to Protect Patient Confidentiality, Privacy, and Security

Think before you Act!!

- Never look at a patient's record out of curiosity even with good intentions
- Follow the minimum necessary standard
- Double check names and phone numbers before sending PHI by fax or email
- Log out of your computer if you have to leave your workstation.
- Never share passwords
- Familiarize yourself with the organizations Notice of Privacy Practices

Contact Information

Email PrivacyOfficer@bmc.org

Website <http://internal.bmc.org>

For forms and information/news regarding
HIPAA:

Click on @Work, then click on Privacy at BMC

For company policies related to HIPAA:

Click on @Work, then click on Policies and
Procedures



Confirm that You Read the Presentation

I have read and understand the content of “Patient Confidentiality, Privacy, and Security Awareness.”

Signature Date

Printed Name

Return this sheet to the department who is hosting your observership.

Contact info:
Ana Bediako
The Office of Enrichment
B.U. School of Medicine
72 E. Concord St., A-302
Boston, MA 02118
617-638-4167
abediako@bu.edu