Boston Medical Center
HEALTH SYSTEM

Policy #:	09.18.000
Issued:	July 15, 2014
Reviewed/ Revised:	9/2017, 11/2020, 11/2023, 2/2025
Section:	Compliance

Code of Conduct and Compliance Training

Purpose:

To establish guidelines and requirements for the distribution and review of BMC Health System's (BMCHS) Code of Conduct and the completion of the orientation and annual mandatory Compliance training programs by the BMCHS workforce.

Policy Statement:

BMCHS is committed to maintaining a patient care and work environment that is respectful, caring, ethical, and compassionate. BMCHS's Code of Conduct and its compliance training programs provide information and resources to the BMCHS workforce regarding compliance-related issues and relevant federal and state laws and regulations. The Code of Conduct and the training programs also set forth the ethical standards that govern the conduct of the operations of BMCHS.

Application:

All members of the BMC Health System hospitals workforce and their subsidiary corporations, including, but not limited to, the Faculty Practice Foundation, Inc. and privileged members of the community health centers. For the purpose of this policy, "workforce" is defined as employees, Licensed Independent Practitioners (as defined in the Medical and Dental Staff Bylaws), interns, house staff, volunteers, and all others who work for or provide services on behalf of BMCHS including contractors and travelers.

Exceptions:

None

Procedure:

1. Code of Conduct Distribution: The Compliance Department shall provide each new member of the BMCHS workforce with a copy of, or electronic access to, the Code of Conduct. The new workforce member must review the Code of Conduct and attest that they agree to abide by the requirements of the Code of Conduct, BMCHS policies, procedures and standards, and the state and federal laws governing health care.
2. Training Program Design: The BMCHS Compliance Department shall develop, implement, provide, evaluate, track and maintain an orientation program, an annual mandatory compliance training program and specialized Compliance-related training and education programs. The Compliance Department shall obtain input from the BMCHS Compliance Oversight Committee and the Audit and Compliance Committee of the BMCHS Board of Trustees regarding the design and content of the training programs.
3. New Workforce Member Compliance Training: All new workforce members must complete the Compliance training program within 30 days after their orientation session. Workforce members who do not attend BMCHS's new employee orientation must complete the program within the first 30 days after they begin their employment or begin providing services to BMCHS.

4. Compliance Training for BMC Volunteers: All volunteers at BMCHS shall complete the compliance training program within 30 days after they begin providing their services to BMCHS. The Volunteer Department shall report all training completions to the Compliance Department on a monthly basis.
5. Annual Mandatory Compliance Training: All members of the BMCHS workforce shall receive access to and complete an annual mandatory compliance training every calendar year.
6. Failure to Complete Compliance Training:
    6.1. BMC Employees. If a BMCHS employee fails to complete any compliance training program within the prescribed period, the Compliance Department shall report the name of the employee to the employee's supervisor. The supervisor shall take appropriate action to obtain the employee's compliance with the requirements of this policy.
    6.2. Licensed Independent Practitioners (LIP). If an LIP does not complete the Compliance training program within the prescribed period, the Compliance Department will notify the LIP's Department Chair who shall take appropriate action to obtain the LIP's compliance with the requirements of this policy.
    6.3. All other workforce members. All other workforce members who do not complete the training within the prescribed period will not be permitted to continue providing services at BMCHS until they have completed the training.
7. Training Requirement for Workforce Members on Leave: Any workforce member who is on leave at the end of the annual training period and who did not complete the annual training prior to taking leave must complete the current year's annual Compliance training program within 30 calendar days of their return to BMCHS.
8. Records of Training Completions: The Compliance Department shall maintain records (in writing or electronically) of all workforce members who complete the new workforce member and annual compliance training programs.

Responsibility:

Compliance Department
Department of Human Resources
Department of Medical Affairs
Volunteer Services

Forms:

None

Other Related Policies:

07.13.000 - Employee Conduct
22.07.030 - Physician/Faculty Hiring Process

References:

None

Initiated by: Compliance Department

Contributing Departments: Human Resources

Information Security and Privacy Agreement

Policy #:	40.01.012
Issued:	March 2014
Reviewed/ Revised:	4/2022, 10/2025
Section:	Compliance

Purpose:

To establish policy that requires all users to read and sign a user agreement (the Information Security and Privacy Agreement), that confirms they agree to be personally responsible for complying with BMCHS security policies and procedures and for maintaining the security of all BMCHS Confidential[1] information (electronic, verbal or written) and other information resources.

Policy Statement:

Users will be required to execute an Information Security and Privacy Agreement that confers a personal responsibility to comply with applicable BMCHS security policies and procedures and to maintain the security of BMCHS information systems, information resources, and BMCHS Confidential information.

Application:

The workforce members of Boston Medical Center Corporation (BMCHS) and its subsidiary corporations, including but not limited to the Boston University Medical Group. and members of the BMCHS Medical Dental Staff.

Exceptions:

None

Procedure:

1. All workforce members are required to read and acknowledge the BMCHS *Information Security and Privacy Agreement* (Exhibit A to this Policy) as part of taking New Hire and Annual Compliance training. Business Associate (BA) personnel will not be required to sign this document if the BA has executed a Business Associate Agreement (BAA) with BMCHS.
2. All other non-employed users (other than BA personnel who will be granted access to BMCHS information systems under a BAA) will also be required to be under a written confidentiality agreement or contractual terms (directly or through their employer entering into a written agreement with the Facility or other BMCHS company).
3. Your acknowledgement of the *Information Security and Privacy Agreement* will be tracked through BMCHS' new hire and annual compliance training.

Responsibility

Chief Compliance Officer
BMCHS

Attachment:

(A) Information Security and Privacy Agreement

[1] BMCHS Confidential" – Refer to Information Classification and Handling Policy for definition and handling requirements.

Other Related Policies:
38.01.001 *Confidentiality and Use of Information*
38.01.003 HIPAA Minimum Necessary Standard
40.01.024 Appropriate Use of Technology

References:
45 C.F.R. § 164.308(a) (4)
45 C.F.R. § 164.312(b)

Initiated by: Privacy

Contributing Departments:
Information Technology Services

Boston Medical Center
HEALTH SYSTEM

Information Security and Privacy Agreement

Boston Medical Center Health System (BMCHS) and other BMCHS subsidiaries (collectively, "BMCHS" or "BMCHS companies") are committed to maintaining high standards of confidentiality. The responsibility to preserve the confidentiality of information in any form (electronic, verbal, or written) rests with each User granted access to BMCHS information systems who may have access to BMCHS Confidential[i] Information, including Protected Health Information (PHI), Electronic Protected Health Information (ePHI), employee information, physician information, vendor information, medical, financial, or other business-related or company confidential information. Any information created, stored or processed on BMCHS systems, or systems maintained on BMCHS's behalf by a vendor or other individual or entity, is the property of BMCHS, as is any information created by or on behalf of BMCHS, whether written, oral or electronic. BMCHS reserves the right to monitor and/or inspect all systems that store or transmit BMCHS data, the data stored therein, as well as all documents created by or on behalf of BMCHS.

Definitions:

Agreement means this *BMCHS Information Security and Privacy Agreement*.

Confidential Information means confidential information that is created, maintained, transmitted or received by BMCHS and includes, but is not limited to, Protected Health Information ("PHI"), Electronic Protected Health Information ("ePHI"), other patient information, Workforce member information, employee, physician, medical, financial and other business-related or company private information in any form (e.g., electronic, verbal, imaged or written).

Protected Health Information ("PHI") means individually identifiable health information that relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual. PHI can be oral, written, electronic, or recorded in any other form.

Electronic Protected Health Information ("ePHI") means Protected Health Information in electronic form.

User means a person or entity with authorized access to any BMCHS network and/or other information systems, including computer systems.

Workforce means employees, volunteers, trainees, and persons whose conduct, in the performance of work for BMCHS, are under the direct control of BMCHS, whether or not they are paid by BMCHS. Workforce also include management and employed medical staff.

I HAVE READ AND UNDERSTAND THIS ENTIRE AGREEMENT, AND I AGREE TO THE FOLLOWING:

(Note: Please acknowledge your review and understanding at the end of your Compliance training.)
1. I understand it is my personal responsibility to read, understand and comply with all applicable BMCHS company policies and procedures, including Security policies. I understand that these policies provide important information about the acceptable use of information systems, protection from malicious software, Mobile device usage, and data encryption, and other important information. If I am provided access to PHI or ePHI, I also agree to comply with the Privacy policies.
2. I have been provided access to the Security (and Privacy policies as applicable).
3. I agree not to disclose any PHI, ePHI or any other Confidential Information obtained by accessing the BMCHS network and/or other information systems, including computer systems, or otherwise to any unauthorized party. I agree not to access or use any PHI, ePHI or any other Confidential Information unless I am authorized to do so. I agree that all patient-related information shall be held to the highest level of confidentiality.

4.	I agree to access the BMCHS network and/or other information systems, including computer systems, only for purposes related to the scope of the access granted to me.
5.	I understand that BMCHS regularly audits access to information systems and the data contained in these systems. I agree to cooperate with BMCHS regarding these audits or other inspections of data and equipment, including BMCHS inquiries that arise as a result of such audits.
6.	I agree that I will not share or disclose User IDs, passwords or other methods that allow access to BMCHS network and/or other information systems, including computer systems, to anyone, at any time, nor will I share my account(s). I also agree to store all BMCHS company-related data onto the system servers rather than on hard drives of individual workstations, personal computers, or other devices.
7.	I agree to contact my supervisor (or for non-employees, the applicable BMCHS Department Director or Business Contact) and IS Security Officer immediately if I have knowledge that any password is inappropriately revealed or any inappropriate data access or access to Confidential Information has occurred.
8.	I understand that Confidential Information includes, but is not limited to PHI, ePHI, other patient information, employee, physician, medical, financial and all other business-related or company private information (electronic, verbal or written).
9.	I agree that I will not install or use software that is not licensed by BMCHS (or that is otherwise unlawful to use) on any BMCHS information systems, equipment, devices, or networks. I understand that unauthorized software may pose security risks and will be removed by BMCHS.
10.	I agree to report any and all activity that is contrary to this Agreement or the BMCHS Security or Privacy policies to my supervisor, Department Director, IS Security Officer or Privacy Officer.
11.	I understand that for employees this form will be part of the employee file at BMCHS and that failure to comply with this Agreement and the BMCHS Security and Privacy policies may result in formal disciplinary action, up to and including termination. I understand that for non-employees, failure to comply with this Agreement and the BMCHS Security and Privacy policies may result in revocation of access and the termination of any agreements or relationships with BMCHS.
12.	I understand that all information and/or data transmitted by or through or stored on any BMCHS device, or system maintained on any BMCHS company's behalf by a vendor or other individual or entity, will be accessible by BMCHS and considered the property of BMCHS, subject to applicable law. I understand this includes, without limitation, any personal, non-work related information. I do not have any expectation of privacy with regard to information on any BMCHS network and/or other information systems, including computer systems, and understand that BMCHS has no obligation to maintain the privacy and security of the information. I understand that BMCHS reserves the right to monitor and/or inspect all systems that store or transmit BMCHS data, the data stored therein, as well as all documents created by or on behalf of BMCHS.
13.	I agree that all devices used by me that are connected to a BMCHS network and/or other information systems, including computer systems, whether owned by me or not, will be continually running approved and updated anti-virus software.
14.	I will follow the requirements for Users described in all BMCHS Security policies, including but not limited to the BMCHS Security policy *Appropriate Use of Technology Policy.*

The BMCHS Information Security and Privacy Policies are available through my supervisor, manager, BMCHS business contact or the BMCHS Corporate Compliance Office, and on the intranet located in Policy Tech. I can use my BMCHS email and password to access these policies.

By clicking on the green checkmark located at the end of the orientation and/or annual Compliance training you confirm that you understand and agree to abide by the conditions imposed above.

[i] BMCHS Confidential" – Refer to Information Classification and Handling Policy for definition and handling requirements.

Policy #:	07.30.000
Issued:	December 1, 1999
Reviewed/ Revised:	9/2006, 11/2010, 2/2014, 11/2018, 7/2019, 3/2022
Section:	Human Resources

Resources Acceptable Use

Purpose:
To establish the acceptable and appropriate behavior for employees, medical staff, and others authorized to access and use BMC resources, including, the internet from a Boston Medical Center ("BMC") computer or BMC-provided mobile device, access/use of the internet while working at or for BMC, electronic mail ("email"), and voicemail

Policy Statement:
BMC provides resources, including but not limited to the computer network, internet, email and voicemail, at its expense to support and enhance patient care and to support and enhance its business, academic, and research pursuits. Use of these resources is for legitimate job-related purposes and must never breach the confidentiality of BMC patient and proprietary information. **Violations of any of the terms of this Policy may result in discipline, up to and including termination from employment or services.**

Application:
All employees, medical staff and authorized third parties with access to BMC electronic resources.

Exceptions:
None

Definitions:
Business Records: Some forms of electronic communications that are sent, received, or stored within BMC's computing environment are considered a business record subject to *Policy #02.06.000 - Medical Record and Document Retention*.

Electronic Communications: Collectively, BMC email and voicemail.

Social Media: Forms of electronic communication (such as websites for social networking and blogging) through which users create online communities to share information, ideas, personal messages, and other content (such as photographs and videos). Social media sites may include but are not limited to Facebook, Twitter, LinkedIn, Instagram, and YouTube.

BMC Policies and their language are not intended to create or constitute a contract between BMC and any of its employees. BMC reserves the right to unilaterally modify, revoke, suspend, terminate or change any and all policies, procedures and benefits it may have with or without notice, at any time. BMC reserves the right to decide not to apply any particular policy in a given situation if, in its sole discretion, it determines that to do so should better serve its interest.

Procedure:

1. BMC Network and Internet

1.1. No Expectation of Privacy: Employees, medical staff and authorized third parties have no expectation of privacy with respect to BMC network and internet use.

1.2. BMC may monitor any and all employee network use and internet access at any time and without notice.

1.3. Internet use is a privilege, and BMC reserves the right to restrict or deny this privilege at any time.

2. Social Media Use

2.1. Access: Some BMC employees and users may have access to social media sites through the BMC network or devices. BMC provides access to these sites solely to support and enhance patient care or BMC's business, academic, and research pursuits.

2.1.1. No Personal Use: Those who are permitted to access/use social media and social networking sites may only do so for legitimate, job-related purposes, and not for personal use.

2.1.2. No Representations on Behalf of BMC: No employee may utilize social media on behalf of or representing BMC without the express authorization of the Communications Department.

2.1.3. Responsible for Content: An individual with access to social media and networking sites is responsible for the content accessed or added to these sites under his/her username and password, and he/she may not permit another employee or third party to use his/her login and password to access these sites.

2.1.4. No Confidentiality Breach: Communications in online communities must never contain information that identifies a patient in any way, including by words, description or photograph, or discloses information regarding a patient's medical care or condition.

2.1.5. Access/use of social media and networking sites is subject to the same rules, restrictions and discipline as general internet access and use described above.

3. Email Use:

The BMC email system is a BMC resource that is to be used for legitimate business purposes.

3.1. An email message must be treated as if it is being sent on BMC letterhead and with the understanding that it may be printed, forwarded or duplicated, or subpoenaed in legal proceedings.

BMC Policies and their language are not intended to create or constitute a contract between BMC and any of its employees. BMC reserves the right to unilaterally modify, revoke, suspend, terminate or change any and all policies, procedures and benefits it may have with or without notice, at any time. BMC reserves the right to decide not to apply any particular policy in a given situation if, in its sole discretion, it determines that to do so should better serve its interest.

3.2. Encryption: The internet is not a secure method of communication, so any emails containing sensitive or confidential information or Protected Health Information (PHI) must be encrypted prior to transmission.

3.2.1. This includes, but is not limited to, all emails that contain any information that may be used to identify patients.

3.3. No Privacy Expectation: BMC may monitor the electronic communications of an employee, medical staff or third party at any time without notice and may do so in the following non-exhaustive examples:

3.3.1. To prevent system abuse or misuse and/or to investigate allegations of system abuse or misuse;

3.3.2. To prevent or investigate violations of BMC's policies and procedures;

3.3.3. To assure compliance with software copyrights or any other laws;

3.3.4. To comply with legal and regulatory requests for information;

3.3.5. To maintain continuity of operations during an employee's absence; or

3.3.6. Any other business reasons.

4. Violations:

The following are non-exhaustive examples of prohibited resources access/use that will subject an employee to an investigation for a potential violation of *Policy #07.13.000 - Employee Conduct* as well as this Policy:

4.1. Transmitting, creating, distributing, reviewing, downloading or storing files/documents/messages containing profanity, vulgarity, material with a sexual content or any other material that is offensive in violation of *Policy #07.00.000 - Anti-Discrimination and Harassment*;

4.2. Revealing or publicizing (except as directly related to a legitimate business purpose and as permitted by law) any BMC proprietary or confidential information including, but not limited to, HIPAA-protected data, patient information, financial information, or system or network access codes.

4.2.1. If an employee has any question regarding whether or not disclosure of information is related to a legitimate business purpose or legal, he/she should not disclose the information unless and until he/she has contacted BMC's Office of the General Counsel and been given specific permission to disclose it;

4.3. Using the internet to harm or attempt to harm others in any way, including minors;

4.4. Using the internet to disparage or defame BMC, a BMC affiliate or a BMC coworker, supervisor or any other person affiliated with BMC;

BMC Policies and their language are not intended to create or constitute a contract between BMC and any of its employees. BMC reserves the right to unilaterally modify, revoke, suspend, terminate or change any and all policies, procedures and benefits it may have with or without notice, at any time. BMC reserves the right to decide not to apply any particular policy in a given situation if, in its sole discretion, it determines that to do so should better serve its interest.

4.5. Using the internet to engage in illegal activities, including publishing pictures or other information about participation in illegal activities, or accessing/using a web site that encourages illegal activity;

4.6. Impersonating another person, using another person's BMC identification or passwords, allowing another person to use your BMC identification or password, or attempting to modify or access files, passwords, data or internet access rights belonging to others, or attempting to modify or access another person's email;

4.7. Using the internet or email to solicit or foster non-BMC business for personal gain;

4.8. Storing BMC data (including grant information) on non-BMC servers and networks;

4.9. Using the internet or email in a manner that interferes with or negatively affects an employee's performance of his/her job duties;

4.10. Transmitting BMC confidential information without encryption (failure to send secure message);

4.11. Creating or distributing emails with harassing, threatening, intimidating, and/or disparaging content regarding or directed at a BMC coworker, supervisor, or other person affiliated with BMC;

4.12. Using email or the network to intentionally or recklessly distribute viruses and/or other destructive software; and/or

4.13. For non-exempt employees: accessing BMC email outside of regular work hours without prior authorization from a manager/supervisor.

5. Virus/Malware Infection Concerns

5.1. Internet and email use also creates the risk of infecting BMC's computing resources with viruses or malware.

5.1.1. Users should not open an attachment to an email from an unknown sender.

5.1.2. Emails believed to be "spam" should be forwarded to Information Security via spam@bmc.org, and then deleted.

5.2. All employees, medical staff and authorized third parties are required to be mindful of these risks when using BMC electronic resources, and must notify the IT Service Desk (x4-4500) immediately if they have reason to believe that one these risks has or may have occurred.

Responsibility:
All staff

BMC Policies and their language are not intended to create or constitute a contract between BMC and any of its employees. BMC reserves the right to unilaterally modify, revoke, suspend, terminate or change any and all policies, procedures and benefits it may have with or without notice, at any time. BMC reserves the right to decide not to apply any particular policy in a given situation if, in its sole discretion, it determines that to do so should better serve its interest.

Forms:
None

Other Related Policies:
02.06.000 Medical Record and Document Retention
02.09.000 HIPAA Disclosure of Protected Health Information
02.37.000 Electronic Device
07.00.000 Anti-Discrimination and Harassment
07.13.000 Employee Conduct
38.02.001 Privacy and Confidentiality on Social Media
40.01.002 Acceptable Use

Initiated by: Human Resources
Contributing Departments:
1. Compliance
2. Communications
3. Office of the General Counsel

BMC Policies and their language are not intended to create or constitute a contract between BMC and any of its employees. BMC reserves the right to unilaterally modify, revoke, suspend, terminate or change any and all policies, procedures and benefits it may have with or without notice, at any time. BMC reserves the right to decide not to apply any particular policy in a given situation if, in its sole discretion, it determines that to do so should better serve its interest.

Boston Medical Center
HEALTH SYSTEM

Policy #:	40.01.025
Issued:	4/2025
Reviewed/ Revised:	
Section:	Information Technology Systems (ITS)

Workforce Artificial Intelligence Acceptable Use Policy

Purpose:

The Boston Medical Center Health System (BMCHS) Workforce Artificial Intelligence (AI) Acceptable Use Policy (Policy) outlines the guidelines and expectations for workforce members using AI technologies in the workplace and applies to the BMCHS workforce. The policy is designed to ensure responsible and ethical use of AI tools, promoting a safe, secure, fair, and robust system while safeguarding member, provider, and BMCHS information.

Scope:

This policy applies to BMCHS workforce members and affiliated subsidiaries.

Overview Statement:

This Policy is designed to ensure that approved AI technology is used in a responsible, ethical, and secure manner. The use of AI Solutions is solely for tasks that contribute directly to BMCHS business objectives and duties in alignment with the Code of Conduct, applicable policies, procedures, and law. Employees are only allowed to use AI Solutions and tools approved by the organization, Responsible AI program, and their supervisor. By abiding with this Policy, BMCHS can harness the benefits of AI technology while minimizing the risks ensuring that our practices align with our policies, values and ethical standards.

Applications:

This policy applies to all employees, contractors, volunteers, and any other individuals granted access to BMCHS's technology resources including the workforce members of the BMCHS hospitals, Clearway Health, Boston University Medical Group (BUMG), Inc. and members of the BMC Medical Dental Staff. This policy is not applicable to Wellsense Employees.

Definitions:

Artificial Intelligence (AI): means a branch of computer science that uses data processing systems that perform functions normally associated with human intelligence, such as reasoning, learning, and self-improvement, or the capability of a device to perform functions that are normally associated with human intelligence such as reasoning, learning, and self-improvement.

Accrediting Body: means an organization that grants accreditation to programs or institutions ensuring that they meet certain standards, such as Joint Commission on Accreditation of Healthcare Organizations (JCAHO) and National Committee for Quality Assurance (NCQA).

Bias: means effects that deprive a statistical result of representativeness by systematically distorting it and includes without limitation, systemic bias, (historical, societal, institutional); statistical and computational biases (errors that result when a sample is not representative of the population); and human bias.

Black Box: means the functioning of an AI system where the step-by-step logical processes are not

known such that it may not be possible to explain how an output was derived from known input data.

Chatbot: means AI which responds in real time to human-generated text prompts in a text interface and simulates human language responses.

Data Set: means a collection of related data used within machine learning, which is typically structured, covers one topic, and can be treated as a single unit of data for analysis and training.

Downstream Entity: means any party that enters into a written arrangement, acceptable to Centers for Medicare & Medicaid Services (CMS), with persons or entities involved with the Medicare Advantage benefit or Medicare Part D benefit, below the level of the arrangement between a Managed Care Organization or applicant or a Part D plan sponsor or applicant and a first-tier entity. These written agreements continue down to the level of the ultimate provider of both health and administrative services.

First Tier Entity: means any party that enters into a written arrangement, acceptable to CMS, with a Managed Care Organization or Part D plan sponsor or applicant to provide administrative services or health care services to a Medicare eligible individual under the MA program or Part D program.

Generative Artificial Intelligence (Generative AI): means technology that can be used to produce or create new content (such as audio, code, images, text, simulations, videos, synthetic data, etc.) that reflects the general characteristics of training data without necessarily duplicating such training data, for example text generation using a large language model.

Hallucinations: refers to a feature of large language models (LLM) used to describe an output which may initially appear to be believable, but which is factually or grammatically incorrect or in which words are jumbled or do not make sense.

Large Language Model (LLM): means artificial intelligence systems trained on vast amounts of data that can appear to understand and generate human language in tools such as Chatbots.

Machine Learning: means the "field of study that gives computers the ability to learn without being explicitly programmed," or computer programs that utilize data to learn and apply patterns or discern statistical relationships. Machine learning includes reinforcement learning, supervised learning, and unsupervised learning.

Output(s): means any outcome, output, or other result, action, or decision obtained from or otherwise performed by or with the assistance of, an AI Technology.

Predictive Artificial Intelligence (Predictive AI): refers to the mining of historic data using algorithms and/or machine learning to identify patterns and predict outcomes that can be used to make or support the making of decisions.

Related Entity: means any entity that is related to a Managed Care Organization or Part D sponsor by common ownership or control and:

1. Performs some of the Managed Care Organization or Part D plan sponsor's management functions under contract or delegation;
2. Furnishes services to Medicare enrollees under an oral or written agreement; or
3. Leases real property or sells materials to the Managed Care Organization or Part D plan sponsor at a cost of more than $2,500 during a contract period. (See, 42 C.F.R.

§423.501).

Responsible AI Program: BMCHS program that oversees and administers Responsible AI and is designed to harmonize ethical considerations, technical advancements, regulatory adherence, and innovation.

Supplier: An external entity or individual in which BMCHS contracts to provide products and services.

Workforce: means an employee, volunteer, trainee, or other person whose conduct, in the performance of work or research for BMCHS, is under the direct control of BMCHS, whether or not they are paid by BMCHS.

Procedure:

I. Authorized Use: Employees may use AI technologies provided or approved by the organization for work-related tasks, as outlined by their job responsibilities and tasks designated by their supervisors such as to retrieve data, generate drafts, provide decision predictions, and rational and similar capabilities. AI use must comply with all applicable laws, regulations, Accrediting Body standards, and BMCHS policies and procedures as well as those of affiliated subsidiaries.

II. Prohibited Use: a) AI shall not be used to make clinical decisions or benefit and eligibility determinations. Clinical decisions are to be made by appropriately licensed professionals. b) The use of AI for fraudulent, malicious, or deceptive activities is strictly prohibited. c) Blackbox technologies are prohibited, unless reviewed and expressly approved by the Responsible AI Committee. Prohibited use also applies to all contracted third-party entities.

III. Data Privacy and Security: All AI activities involving sensitive data, confidential/proprietary data, protected health information (PHI), personally identifiable information (PII), 42 CFR Part 2 Substance Use Disorder Program data, must be carried out following each BMCHS affiliated subsidiary's data protection and privacy policies.

IV. Responsible AI Usage: To perform work, workforce members may only use AI tools that have been reviewed and approved for use by the Responsible AI Committees. Workforce members must ensure that any AI tools used for BMCHS work are approved prior to use.

V. Compliance with Laws and Regulations: Workforce members use of AI must comply with all applicable federal and state laws and regulations, federal and state contract requirements, and accreditation agency standards related to AI use, data protection, data security and privacy, and intellectual property.

VI. Intellectual Property: When utilizing AI tools to develop new software, applications, algorithms, or processes, the Workforce member must follow intellectual property policies.

VII. Accountability: If a Workforce member's role provides AI-generated content or interactions with patients, members, or stakeholders, they must follow BMCHS and affiliated subsidiary policies and procedures to ensure they are complying with appropriate use and disclosures requirements when AI is being used.

VIII. Avoiding Bias: a. Workforce members who develop AI technologies for business or research purposes must make efforts to identify and mitigate Bias. b. If any workforce member

suspects Bias in AI-generated outputs, they should promptly report the issue to their supervisor *and* the compliance department.

IX. Monitoring: Ensure thorough periodic review that the use and application of AI technology continues to comply with the Code of Conduct and applicable policies and procedures. Require delegated entities and suppliers to attest or confirm that AI solutions continue to align with BMCHS policies & procedures.

X. Reporting Misuse or Concerns: a. Workforce is responsible to promptly report any misuse or concerns related to approved AI technologies, including misuse by delegated entities and suppliers to their supervisor *and* the compliance department. Examples of concerns could be if any of the following are observed: anomalies, a decline or material deviation in accuracy of Outputs, biased, discriminatory, or illegal Outputs, Hallucinations, or Outputs that divert from expectations as originally expected when deployed and/or outlined in the Code of Conduct or applicable policies and procedures or the AI Solutions documentation. b. Reports of possible AI-related security breaches or vulnerabilities must be submitted as per privacy & security incident reporting policies and procedures.

XI. Consequences of Violations: Failure to adhere to this policy may result in disciplinary action, up to and including termination of employment, revocation of delegation or supplier agreement, or legal action.

XII. Responsible AI (RAI) Governance Committee Role & Responsibility: Notwithstanding the foregoing policy, the RAI Governance Committee reserves the right to reassess, reevaluate, and/or redetermine AI Solutions and tools previously approved by the organization and/or Responsible AI program. Determinations for existing and proposed AI Solutions and tools are made on an ongoing basis, including but not limited to, vendor solutions and/or services contracted for prior to the effective date of this policy.

Exceptions:

Exceptions may be requested and approved by the RAI Governance Committee on a case-by-case basis.

Related Policies & Procedures:

40.01.024 Appropriate Use of Technology
09.18.000 Code of Conduct and Compliance Training
Workforce Acceptable Use Tip Sheet

References:

American Medical Association (AMA) AI Policy
Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA)
Health AI Standards from HL7 (FHIR)
M.G.L. c. 93H, Massachusetts Data Privacy Law
M.G.L. c. 176D, Unfair Methods of Competition and Unfair and Deceptive Acts and Practices in the Business of Insurance
M.G.L. c. 176W, Corporate Governance Annual Disclosure, (CGAD)
201 C.M.R. 17.00, et seq., Massachusetts Office of Consumer Affairs and Business Regulations, standards for the protection of personal information of residents of the Commonwealth
211 C.M.R. 52.00, et seq., Massachusetts Division of Insurance, managed care consumer protections and accreditation of carrier's consumer protection regulations
Bulletin 2024-10, The Use of Artificial Intelligence Systems in Insurance, Massachusetts Division of

Insurance
RSA 507-H, New Hampshire Data Privacy Act
Food and Drug Administration (FDA) AI/ML Regulatory Framework
International Organization for Standardization (ISO): ISO/IEC 42001, 22989, 23053, 23894
National Academy of Medicine (NAM) AI Framework
National Committee for Quality Assurance (NCQA) 2025 Standards
NIST Artificial Intelligence Risk Management Framework 1.0
NIST Cybersecurity Framework
Principles of Artificial Intelligence, National Association of Insurance Commissioners (NAIC) 2020

Initiated by:
External/Internal Policy Committee

Boston Medical Center
HEALTH SYSTEM

Policy #:	09.12.010
Issued:	September, 2024
Reviewed/ Revised:	2/2025
Section:	Compliance

ACA Section 1557 Policies and Procedures Requirements (45 C.F.R. § 92.8)

Purpose:
To show BMC Health System's (BMCHS) compliance with the Affordable Care Act's Section 1557 policy and procedure requirements as noted in 45 C.F.R. § 92.8.

Policy Statement:
BMCHS is committed to nondiscrimination, supporting the rights of all patients, and providing accessible healthcare services to every patient, including individuals with disabilities and individuals with limited English proficiency. In collaboration with BMCHS hospitals' departments and staff, the Section 1557 Coordinator strives to ensure equitable health services regardless of race, color, national origin, sex (including sexual orientation and gender identity), age, or disability.

Application:
All employees and all organizational levels of the hospitals within BMC Health System.

Exceptions:
None

Procedure:

- In order to comply with 45 C.F.R. § 92.8(b) *Nondiscrimination policy*, see BMC Policy #07.00.000 *Anti-Discrimination and Harassment* and BMC Policy #03.12.000 *Interpreter Services Department and Communication Assistance*.

- In order to comply with § 92.8(c) *Grievance procedures*, see BMC Policy #03.08.000 *Patient Advocacy Program*.

- In order to comply with § 92.8(d) *Language access procedures*, see BMC Policy #03.12.000 *Interpreter Services Department and Communication Assistance*.

- In order to comply with § 92.8(e) *Effective communication procedures*, see BMC Policy #03.12.000 *Interpreter Services Department and Communication Assistance*.

- In order to comply with § 92.8(f) *Reasonable modification procedures*, see BMC Policy #03.12.000 *Interpreter Services Department and Communication Assistance*. Should a patient with a disability seek an adjustment to a rule or policy, they can address it by reaching out to the 1557 policy coordinator.

Responsibility:
The Section 1557 Coordinator is the Director of Patient Advocacy, who can be contacted at DG-Patient-Advocacy@bmc.org and the Director of Hospital Compliance, who can be contacted at Privacyofficer@bmc.org.

Forms:
None

Other Related Policies:
07.00.000 - Anti-Discrimination and Harassment
03.12.000 - Interpreter Services Department
03.08.000 - Patient Advocacy Program
09.18.000 – Code of Conduct and Compliance Training
02.28.010 – Code of Conduct for Patients, Staff and Visitors

Initiated by:
Compliance

Contributing Departments:
Interpreter Services Department
Patient Advocacy
Office of General Counsel

Annual Compliance Training



Boston Medical Center
HEALTH SYSTEM

Agenda

Introduction
Avoid Conflicts of Interest
Anti Kickback and False Claims
Protect our Patients' Privacy
Information Security and Digital Communications
Prevent Fraud Waste and Abuse
Exclusion from Payers
Accountable Care Organizations
How to Report
How to Make the Right Decision



Boston Medical Center
HEALTH SYSTEM

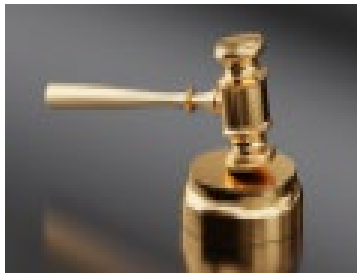
What is Compliance?



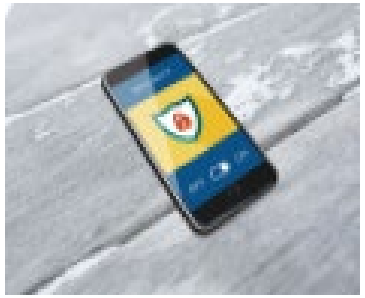
The process of making sure we all follow the laws, regulations, standards, and ethical practices that apply to Boston Medical Center Health System and the work we do here



Compliance Department



Ensures we follow the rules that govern health care



Protects patient privacy



Audits Medicare and Medicaid claims



Ensures outside interests do not influence job performance



Provides information and education on Compliance and Privacy issues



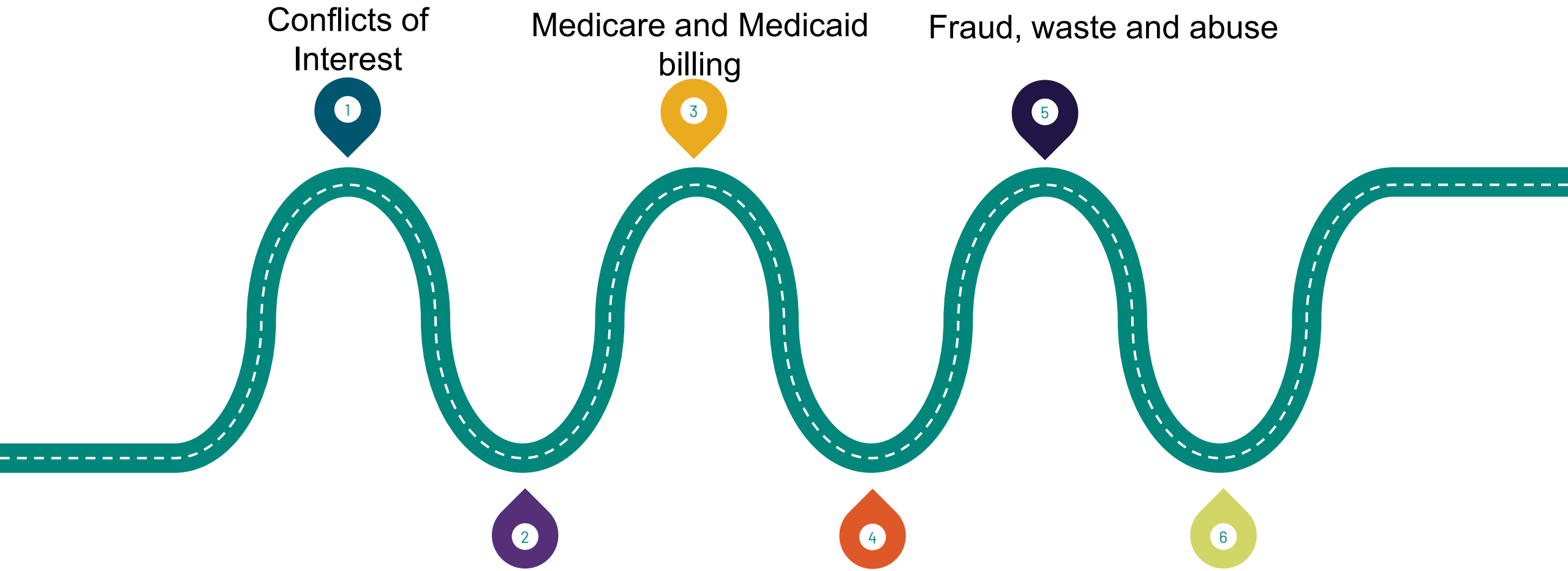
Monitors access to electronic medical records

Compliance Hotline



- Use it 24/7 to report privacy, ethics, or compliance concerns anonymously
- You cannot be retaliated against for making a good faith report
- You can also ask questions and get assistance

Common Compliance Areas of Focus



1

Avoid Conflicts of Interest



Boston Medical Center
HEALTH SYSTEM

Conflict of Interest

When you are in a position to receive a personal benefit for a work decision



Conflicts of Interest and How to Avoid Them

When you are in a position to receive a personal benefit for a work decision



Always put the best interests of BMCHS first



Never let outside personal or financial interests influence (or appear to influence)



Never accept gifts or items for personal benefit from outside companies or vendors

Disclosing Conflicts

If you have any personal interests (income, stock, grants, positions) in a company or organization that are related to your work at BMCHS, you have a potential conflict of interest



If this happens, you must disclose to the Compliance Department



The Compliance Department will let you know how to manage the situation



Keep your disclosure data up to date, report all outside interests as they occur

2

Anti Kickback and False Claims Act



Boston Medical Center
HEALTH SYSTEM

Anti-Kickback Statute



Never give or receive anything of value





Referrals of patients, products, or services
that are reimbursed by any state or federal healthcare program

BMCHS accepts patient referrals and admissions based solely on the patient's medical needs and on our ability to render medically necessary services

These vendor activities can violate the Anti-Kickback Statute



Payments to physicians for sham educational sessions



Gifts or no-cost loans of equipment



Non-business-related entertainment and meals



Consulting that does not require any real work or pay more than fair market value for work



Financial grants to institutions and individuals that are tied to sales activities

Boston Medical Center
HEALTH SYSTEM



The False Claims Act makes it illegal to submit a false claim for payment to the federal or state government

Boston Medical Center
HEALTH SYSTEM



Anyone who has direct and independent knowledge of a violation can file a complaint

False Claims Act violations include



Billing for a higher level of service than actually provided or over-representing a patient's complexity



Billing for medical services not provided



Submitting claims when the billing requirements are not met



Knowingly submitting inaccurate quality data



Failing to report and return an identified overpayment

Boston Medical Center
HEALTH SYSTEM

To avoid false claims, all medical record documentation must be



Accurate



Timely



Complete

"If it's not documented in the medical record, it wasn't done."

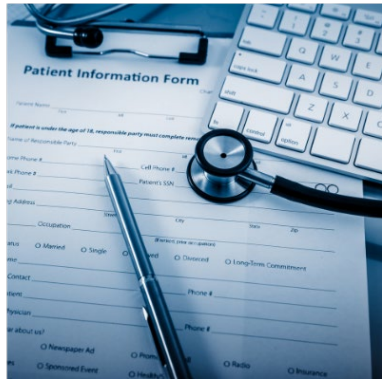
Our Billing Compliance team helps BMCHS avoid false claims by providing training and auditing



Compliance provides education on coding and billing to our clinicians to help avoid mistakes



If billing or coding is inaccurate, BMCHS may be required to refund the government or other payer



Compliance responds to government audit requests

Boston Medical Center
HEALTH SYSTEM

3

Protect Our Patients' Privacy and Rights



Boston Medical Center
HEALTH SYSTEM

Protected Health Information (PHI)

What is PHI?

- Information that might allow someone to identify the patient, together with any information about their health care

What is ePHI?

- PHI that is transmitted over the internet, stored on a computer or transmitted electronically



There are at least 18 potential identifiers for ePHI and PHI

Why Protect Our Patients' Privacy?

- Our patients- and those participating in research- have a **right to privacy about their health**

- Patients and research subjects trust us with their most sensitive information, so it is your duty to protect that information

- **The threat is real.** Inappropriate use or release of this information can cause serious harm

- There are a lot of rules to follow, such as, HIPAA, Massachusetts data breach laws, and other state and federal regulations

Under HIPAA, you may only access PHI when:



There is a business-related reason

+



You only have access to or disclose the minimum amount of information necessary for treatment, payment, or other hospital operations

Boston Medical Center
HEALTH SYSTEM

You cannot have access to PHI for personal reasons, including



Checking on a family member



Making an appointment



Searching for someone's address or birth date



BMCHS monitors access to medical records

The Privacy Office conducts routine audits and investigates complaints to ensure the security of PHI

Boston Medical Center
HEALTH SYSTEM



Disciplinary action, up to and including termination, against any employee who gains access to or discloses PHI without a business need

Knowledge Check Question

Multiple Choice

You work in the Cancer Care Center and have access to our electronic medical record system (EPIC, etc.) for your job. Your family member texts you and asks you to look up the time of their appointment in Ophthalmology. Which is the correct response?

- A. Look up your family member's appointment information and tell them the time and date.
- B. Ask a colleague to look up your family member's appointment because they have no personal relationship with the patient.
- C. Tell your family member you cannot look up their chart in the medical records system and ask them to call their provider's office or check their patient portal, i.e. MyChart, etc.

Safe Storage of PHI



- Use only approved, encrypted removable hardware (thumb drives, hard drives, flash drives or other electronic storage)
- Use BMCHS network drives for all confidential data including PHI and research subject data
- When approved, use OneDrive to send and share large datasets outside BMCHS network



Transmitting PHI Outside of BMCHS and Emails

Secure Email

- Ensure your recipients are authorized to receive the information
- Double check email addresses
- Send secure by typing the word “SECURE” in the subject line or by using OneDrive

IT Service Desk: (617) 414-4500
Compliance: (617) 638-7919

Phishing and Malware

- Do not click on links or download attachments contained in emails when you do not know or trust the sender
- Click the “report message” function located on the top banner of your email or right click on the email and select “report message”
- If you believe you fell victim to a phishing or malware attempt, please contact the IT service desk and Compliance immediately

Recognizing Phishing

****Please click on the e-mail below to learn about spotting phishing red flags before moving forward with the training****

From: CEO@boston.medical.center.com

To: john.smith@bmc.org

Date: Sunday, October 1 at 3:06AM

Subject: Information Needed Immediately

Hello,

The Finance Department has reported to me that over the weekend there has been an unexpected issue with your direct deposit account that needs immediate attention. In order to correct the issue and avoid payment delay, please update your banking account information through this portal: www.boston.medical.finance.portal.com.

Thank you,
Alastar, CEO

Recognizing Phishing

****Please click on the e-mail below to learn about spotting phishing red flags before moving forward with the training****

From: CEO@boston.medical.center.com

Sender's email address has a strange domain name. Sender's domain was @boston.medical.center.com, instead of @bmc.org

To: john.smith@bmc.org

I was cc'ed on an email to other people I do not personally know, or who are not in my organization I received an email that was sent to an unusual mix of individuals.

Date: Sunday, October 1 at 3:06AM

Was the email was sent outside of sender's working hours? Email was sent on a Sunday at 3:06AM, which is an unexpected time to receive an email from the CEO.

Subject: Information Needed Immediately

Is the subject line very vague, urgent, or threatening? Information Needed Immediately is not a typical subject line.

Hello,

The Finance Department has reported to me that over the weekend there has been an unexpected issue with your direct deposit account that needs immediate attention. In order to correct the issue and avoid payment delay, please update your banking account information through this portal: www.boston.medical.finance.portal.com.

The hyperlink is not one I recognize or contains a misspelling of a known website

Thank you,
Alastar, CEO

Is the sender asking me to click a link that seems odd, or not the standard way of doing things?
Do I have an uncomfortable gut feeling about the sender's request?
Does the content of the message seem like something that the sender would not ordinarily contact me about? The CEO will not email an employee personally about an issue with their direct deposit.
Does the email have spelling errors and contain bad grammar?
The spelling of our CEO's first name is incorrect.

Boston Medical Center
HEALTH SYSTEM

Knowledge Check Question

Multiple Choice

You see an email with a $50.00 gift card to Amazon awarding you for title of “Best Employee”. To claim your gift card you must click a link but you notice that the sender’s email is an odd external address. What is the best response?

- A. Do not click on the link or reply to the sender. Immediately report the suspicious email by clicking on the Mimecast function and selecting “report email”, or by right clicking on the email and selecting “report email”.
- B. You are pretty awesome. Click on the link and claim your prize!
- C. Email the sender and ask them if it’s real.

Social Media, Photography and Patient Data

General guidelines:

- Don’t share anything about BMCHS’ patients or confidential information on social media
- Filming or photography on campus is prohibited.

Patient Care Photos:

- Use Haiku when taking photos for care purposes
- Photos for research, peer education, or fundraising - obtain written consent before filming or photographing the patient



Knowledge Check Question

Multiple Choice

You've realized you have a really interesting job at BMCHS and decide to make a social media video, documenting a day in your life at work. How can you do this properly?

- A. Just go for it! Your work is interesting. You want to share all the great work we are doing and you don't need permission.
- B. Only with special written permissions in collaboration with the Communications Department and before any filming can occur on campus, per BMCHS policies.
- C. It's fine, so long as you don't record any patient faces in your video.

Protect Patient Information

Boston Medical Center
HEALTH SYSTEM

Protect It

- Don’t leave protected health information (PHI) unattended in rooms, hallways, desks, cars etc.
- Only discuss patient information privately

Shred It

- Discard PHI the right way- only in locked containers or shredders

Report It

Report the loss of protected health information to:

- your supervisor
- Compliance Office (617-638-7919)
- Compliance Hotline (800-586-2627)
- Compliancehelp@bmc.org

Lost devices containing PHI:

- To Compliance Office *and*
- ITS (617-414-4500)

Knowledge Check Question

Multiple Choice

You are working with a paper chart containing patient or research participant information when you get called away to attend to an urgent issue. Before walking away you should:

- A. Leave the chart out in the open in case your colleagues want to see it.
- B. Return the chart to a safe secure location until you can resume your work on it.
- C. Put the chart in your personal backpack; you'll be sure to take it out once you get back to your station.

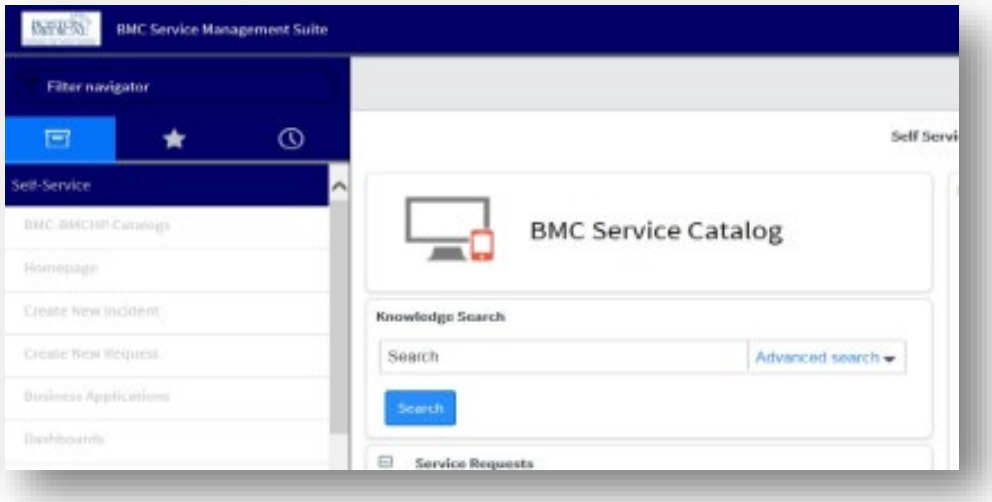
Stop Information Leaks

Non- BMCHS Managed Systems, Services, and Websites

- If a website or service is free, the real cost is the information you enter
- If you want to install non-BMCHS-managed software on a BMCHS system, put in a Service Now ticket
- If you want to use a non-BMCHS-managed device with BMCHS data, put in a Service Now ticket

SERVICE DESK
617- 414 - 4500 or **4 - 4500**
Service Now ticketing system

For questions, issues, or concerns.



Boston Medical Center
HEALTH SYSTEM

👉Go to the **Information Security** HUB page for more information
Topics: email, encryption, secure access, etc.

Protecting Our Patients From Discrimination



Boston Medical Center
HEALTH SYSTEM

Section 1557 of the Affordable Care Act (ACA) prohibits discrimination, in healthcare programs or activities, based on:

- Race
- Color
- National origin
- Age
- Disability
- Sex (including pregnancy, sexual orientation, gender identity, and sex characteristics), in covered health programs or activities

BMCHS must ensure that our patients have equal access to quality healthcare. This includes:

- Providing patients with free language assistance services and auxiliary aids to help individuals with limited English proficiency and individuals with disabilities

Keep BMCHS Discrimination Free

Do Your Part

As a BMCHS employee you must act in a manner that supports our mission to provide exceptional care for all

You can do this by behaving ethically, treating everyone, regardless of background, with kindness, respect, and empathy and by becoming familiar with compliance standards around discrimination

- *See* Anti-Discrimination and Harassment, and BMC Interpreter Services Department and Communication Assistance policies
- *See* Patient Advocacy Program policy for grievance procedure surrounding concerns of discrimination
- *See* ACA Section 1557 Policies and Procedures Requirements (45 C.F.R. § 92.8) which addresses all the policies we have in place to comply with Section 1557 of the ACA

Speak up when you've observed instances of discrimination

Report any instances of discrimination to BMCHS' 1557 Coordinators:

- Director of Compliance at privacyofficer@bmc.org
- Director of Patient Advocacy at DG-Patient-Advocacy@bmc.org

Our patient's can also file a report with U.S. Department of Health and Human Service's Office for Civil Rights at:

- https://ocrportal.hhs.gov/ocr/smartscreen/main.jsf

When patients require language assistance services, contact the interpreter services department. The contact information can be located on the HUB, or call 617-414-5549

Knowledge Check Question

Multiple Choice

A patient comes to you following an appointment reporting that they feel like they were treated differently due to their nationality. What should you do?

- A. Do nothing.
- B. Apologize.
- C. Speak Up- Report any instances of discrimination to BMCHS' 1557 Coordinators:
  Director of Compliance at privacyofficer@bmc.org
  Director of Patient Advocacy at DG-Patient-Advocacy@bmc.org

4

Information Security and Digital Communications



Boston Medical Center
HEALTH SYSTEM

Appropriate Use of BMCHS Email



Email communication reflects our collective commitment to excellence in healthcare and research

Boston Medical Center
HEALTH SYSTEM

Use BMCHS Email and Computer Resources Only for BMCHS Tasks and Communications

Email / Internet /Computer Network

- BMCHS provides email, internet and a computer network to support and enhance patient care and to support and enhance its business, academic, and research pursuits
- You should use BMCHS Distribution Groups (Email) responsibly and for work-related purposes only
- Only use these resources for legitimate job-related purposes

Before you click send please make sure you, above all, ask yourself these two questions:

- Could the reader misinterpret my message?
- If the recipient forwards my message, will it come across as clear, patient-caring, and respectful to any audience?

Violations of BMCHS Email Policy

<u>Examples</u> of violations include but are not limited to the following:

- Creating or distributing emails with **bullying and unlawful harassing, threatening, intimidating, or disparaging** content
- Using the internet or email to solicit or foster **non-BMCHS business**
- Using work email to **support or oppose a political candidate**
- Engaging in **political activities or commentary with BMCHS email** or resources
- Using your work email address **to register on social networks, blogs, or other online tools** used for personal use
- Sending messages related to **personal non-work related** views to individuals or groups

<u>Violations of this Policy may result in discipline, up to and including termination</u>

Personal Activism at Work

We respect every employee's right to advocate for their passions

Personal political activities and personal activism should take place outside of the workplace. When engaging in such activities outside of the workplace, it is important that you do not present yourself and your views as a BMCHS employee, without prior coordination with the Government Affairs office

Boston Medical Center
HEALTH SYSTEM



Our policies on personal activism at work:

- Respect your colleagues' differing viewpoints
- Avoid disruptions to work activities
- Using work email to support or oppose a political candidate is prohibited
- Do not use BMCHS resources or equipment for personal activism
- Maintain professionalism in all communications
- These policies apply to unprotected activity

Posting on social media

Our engagements on social media should reaffirm to patients and members our commitment to providing equitable care and thoughtful public exchange.

Please review our social media policy and Employee Code of Conduct, and before you post on social media, pause to consider the content with these two questions in mind:

- Does my post, or the content that I like or share, show empathy across communities and reaffirm our shared commitment to our mission?
- Have I made it clear that my social interactions are my own and do not represent a collective perspective from BMCHS?
- Could my content be perceived as unkind, disrespectful, or harmful to individuals or groups?
- Could this action discourage or dissuade patients from seeking care or services at BMCHS?



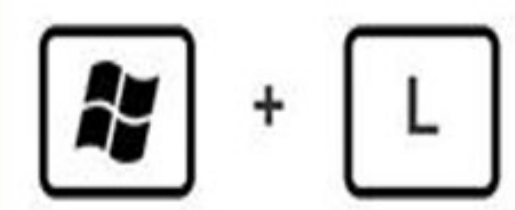
Do not share anything about BMCHS' patients or confidential information on social media

Safe Devices and Computing



- Devices must be password protected and encrypted
- Keep your passwords unique, and don't reuse personal passwords for work
- Never share your password or post your password on a sticky note
- Lock your computer before walking away
- Please review the ***IT Information Security and Privacy Agreement***

To lock your workstation



OR

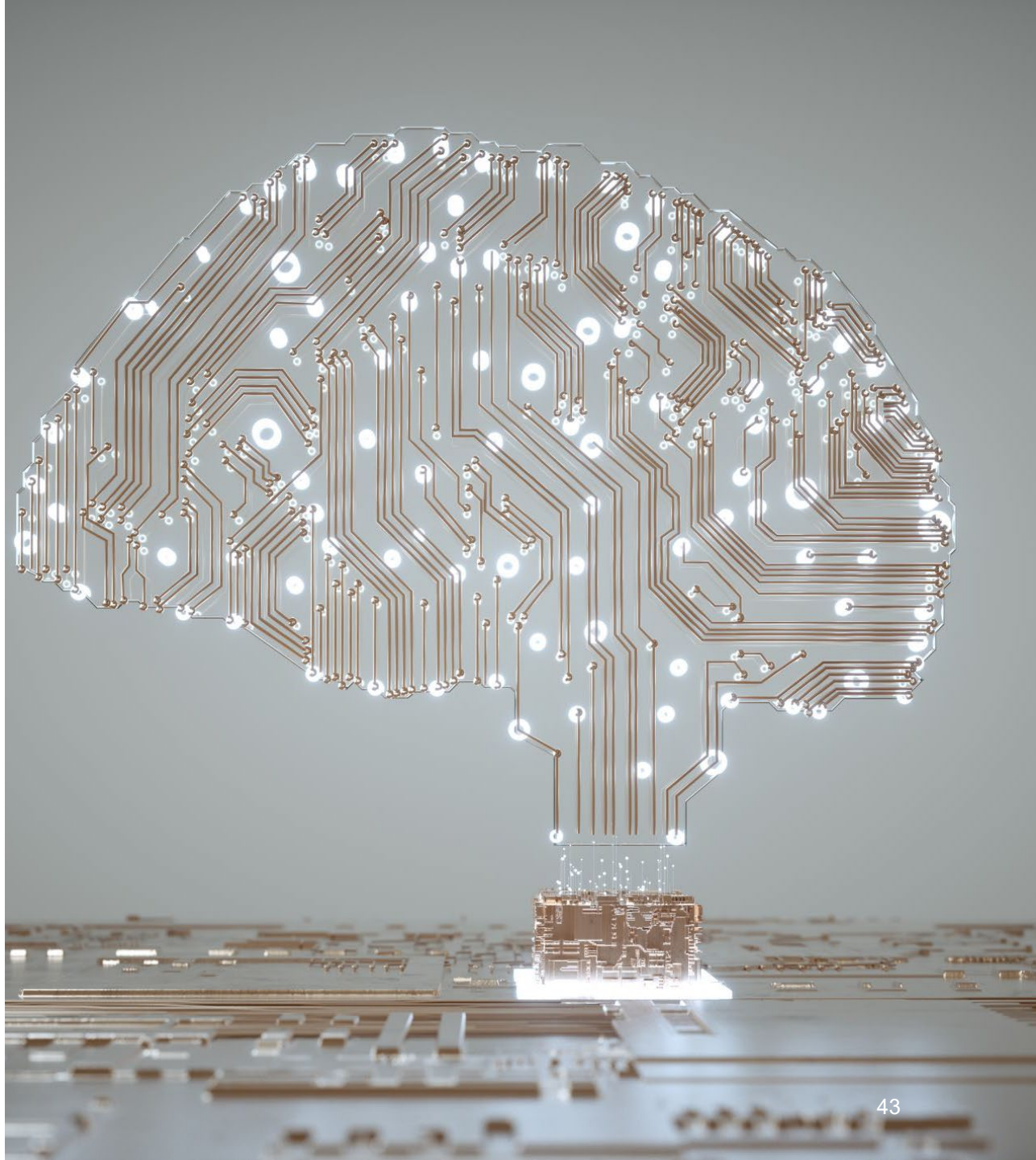


Click "Lock Computer"

Acceptable Use of Artificial Intelligence (AI)

BMCHS is committed to using AI the right way, minimizing the risk of legal and ethical violations. Following BMCHS policy and guidelines can help reduce the risk of using AI in the workplace:

- Only use AI in professional and appropriate manner. Avoid creating harassing, bullying and other unprofessional text and images.
- Only use BMCHS approved AI solutions.
- Never upload information, including patient, member, and organizational information, to an AI tool without permission.
- Respect Privacy: only utilize AI to collect, store and use authorized information, and only use that information to the extent you have permission. Consult with the Compliance Department before uploading patient or member PHI, personal or sensitive data, or proprietary information into an AI tool.
- Check AI output for bias and accuracy every time it is used to make work decisions or forecasts.
- Review the Acceptable Use of AI Policy and Tip Sheet for more helpful information.



5

Prevent Fraud, Waste, and Abuse



Boston Medical Center
HEALTH SYSTEM

Waste and abuse are about causing inappropriate costs to the government



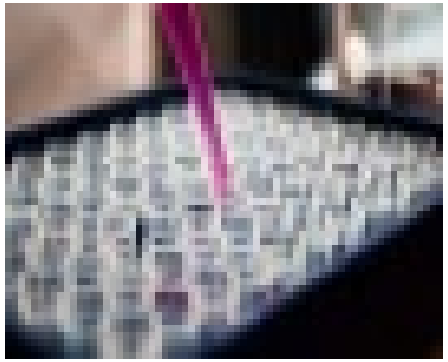
Waste is misusing resources that cause unnecessary Medicare costs



Conducting unnecessary office visits



Writing unneeded prescriptions



Ordering excessive laboratory tests

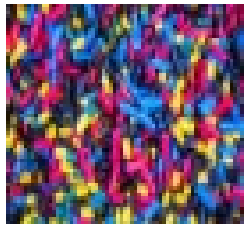
Abuse is receiving payments for items or services BMCHS is not legally entitled to receive, even if we weren't trying to misrepresent the facts

Boston Medical Center
HEALTH SYSTEM

Examples include:



Billing for unnecessary medical services



Billing for brand name drugs when generics are dispensed



Charging excessively for services or supplies



Misusing codes on a claim, such as upcoding or unbundling codes

Depending on the situation, penalties for waste and abuse can include



Fines and prosecution



Exclusion from federal healthcare programs



Loss of provider license

6

Exclusion from Medicare/ Medicaid



Boston Medical Center
HEALTH SYSTEM

The US Office of the Inspector General has the authority to exclude any individual or entity from Medicare and Medicaid

Mandatory exclusion: if you are convicted of a felony involving health care
Permissive exclusion: if you are convicted of a misdemeanor involving fraud in a federal health care program or kickbacks

The government will not pay for any items or services furnished, ordered, or prescribed by an excluded person or entity

Boston Medical Center
HEALTH SYSTEM

If you are excluded



You will be notified in writing by the Office of Inspector General or MassHealth



You must call the Compliance Office at **617-638-7919** and report it immediately

7

Accountable Care Organizations

Boston Medical Center
HEALTH SYSTEM

BMCHS Participates in both a MassHealth and a Medicare ACO

Boston Medical Center
HEALTH SYSTEM



ACOs

Groups of health care providers who come together to coordinate – and become *accountable* for - high-quality care for their patients

Payments for services we provide in these arrangements depend on our ability to keep our patients healthy

To succeed in an ACO, BMCHS must navigate many new Compliance risks



Sharing patient information with our ACO partners to provide coordinated care while also complying with privacy laws



Operating in a value-based system while avoiding inappropriate inducements



Submitting accurate quality data



Ensuring we are paid appropriately for the complexity of our patient population

Boston Medical Center
HEALTH SYSTEM



You Have a Duty to Report Compliance and Privacy Violations

Boston Medical Center
HEALTH SYSTEM

Help us protect BMCHS by reporting any known or suspected violations of

- Federal, state, or local laws or regulations
- The BMCHS Code of Conduct and BMCHS policies
- Instances of suspected or actual fraud, waste, or abuse

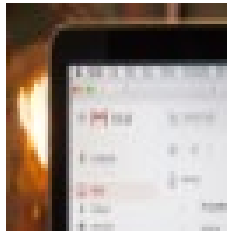
Boston Medical Center
HEALTH SYSTEM

To report an issue



Speak with your supervisor or the Compliance Office at **617-638-7919**

or



Send an email to **compliancehelp@bmc.org**

or



Call the Compliance Hotline at **800-586-2627**

Knowledge Check Question

Multiple Choice

Which are ways to report an actual or suspected Compliance or Privacy violation?

- A. Speak with your supervisor, manager or HR, call or email the Compliance Office at **617-638-7919** or compliancehelp@bmc.org or call the 24 hour, confidential and anonymous hotline at **800-586-2627**.
- B. Post your concern on your social media accounts tagging BMCHS.
- C. Do nothing.

You can also report Medicare fraud, waste and abuse to the federal government

Include this information in a report:

- Contact information for yourself, the suspects, and witnesses
- Details of what you think happened
- Specific Medicare rules you think were violated
- The suspected violator's history of compliance, education, training, and communication with BMCHS or other entities

Boston Medical Center
HEALTH SYSTEM

Where to report an issue

HHS Office of Inspector General
1-800-HHS-TIPS (1-800-447-8477) or
TTY 1-800-377-4950
Fax: 1-800-223-8164
https://oig.hhs.gov/fraud/report-fraud/

For Medicare Parts C and D
National Benefit Integrity Medicare Drug Integrity Contractor (NBI MEDIC) at 1-877-7SafeRx | (1-877-772-3379)

For all other Federal health care programs
CMS Hotline at 1-800-MEDICARE (1-800-633-4227)

HHS and U.S. Department of Justice (DOJ)
justice.gov/criminal-fraud/health-care-fraud-unit

You cannot be retaliated against

- For reporting a suspected or actual compliance or privacy violation
- For becoming a whistleblower and filing a False Claims Act lawsuit

If you engage in retaliation

You will be subject to discipline, up to and including termination of employment

Boston Medical Center
HEALTH SYSTEM



If you believe you have been subject to retaliation

contact the Compliance Office or call the Compliance Hotline (800-586-2627)

8

How to Make The Right Decisions

If the answer to all these questions is “YES” then it’s the right thing to do



Is it legal?



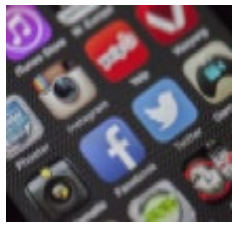
Does it comply with our Code of Conduct and policies?



Is it the fair and honest thing to do?



Is it in the best interests of our patients and our hospital?



Would you be comfortable if the decision went viral on social media?

Boston Medical Center
HEALTH SYSTEM

Compliance Is Everyone's Responsibility

Click all 6 of the documents and policies in the Resources tab, to review

I read, understand and agree with BMCHS' Compliance Policies, including Appropriate Use of Technology, Workforce Artificial Intelligence Acceptable Use Policy, AI Tipsheet, Resources Acceptable Use, Code of Conduct and the Information Security and Privacy Agreement- click on the **Green check**



I don't understand BMCHS' Compliance *and Information Technology Services* Policies, click on the **Red "X"** to review the course



*A copy of all BMCHS Compliance and Information Technology Services Policies are on the **HUB** located in **Policy Tech**. You can use your BMCHS email and password to access.*

CONGRATS!

You have completed Compliance is Everyone's Responsibility training

Boston Medical Center
HEALTH SYSTEM

The Compliance team is here to protect you and our hospitals

Report a concern, get advice, find resources, or just talk over an issue



Call: Compliance Hotline 800-586-2627 (24/7) or 617-638-7919 during business hours



E-Mail: DG-Compliancehelp@bmc.org

Exit

BMC Emergency Management FY26

What You Need to Know

Boston Medical Center
HEALTH SYSTEM

What is Emergency Management

Managerial function tasked with creating the framework which reduces vulnerability to threats/hazards and cope with disasters

- **Biological**
- **Technological**
- **Natural**
- **Human Caused**

The Department of Emergency Management leads the Emergency Preparedness Program across the BMC enterprise, with a focus on:

- **Safeguarding Human Resources**
- **Maintaining Business Continuity**
- **Protecting Physical Resources**



Boston Medical Center
HEALTH SYSTEM

https://emilms.fema.gov/is_0230e/groups/999.html

Emergency Management at BMC

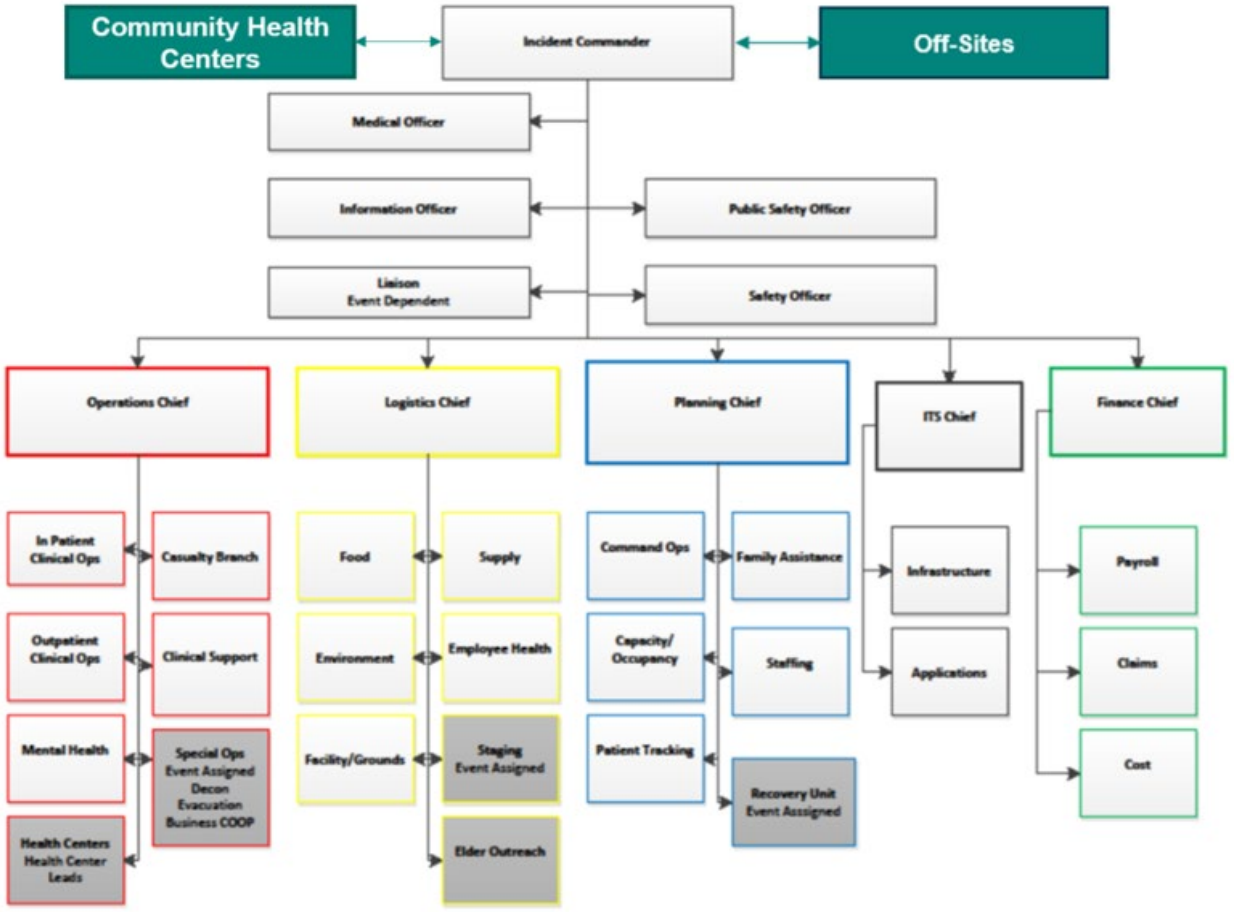
BMC utilizes the ***Hospital Incident Command System (HICS)***

A standardized approach to response activities for emergencies and disasters of any kind

- **Led by a hospital Incident Commander who is responsible for the management of the emergency**
- **Each position is staffed by trained personnel that make up BMC's Incident Management Team**

Incident Command ensures:

- **Event response is based on objectives & priorities**
- **Ensures oversight & control of the response**
- **Ensures accurate & timely information**
- **Response if efficient & effective**



Emergency Response Activation

The ***Emergency Operations Plan (EOP)*** defines critical roles, responsibilities and provides authority to rapidly mobilize material and personnel resources in response to the needs of an emergency event

- **BMC has four phases of emergency response: A-D**
- **Phases communicates the scope and impact of an event**
- **Ensure appropriate and sufficient mobilization of hospital resources to manage the event**

Phases must be:

Declared by the appropriate authority based on incident type, location, scope and impact to facility and/or clinical operations

- **The declaring authority will contact the Control Center to initiate the activation of the Emergency Operations Plan (EOP)**



Knowledge Check

Multiple Choice

BMC has _____ Emergency Response Phases

- 2
- 3
- 4
- 1

Emergency Response - Phase A

Administrative Advisory

An event or impending event that can be managed under normal operations but is being monitored

- Hospital / Site remains at normal operations
- Event is being monitored by Emergency Management, hospital administration, or the department resolving the issue
- Typically no actions are needed

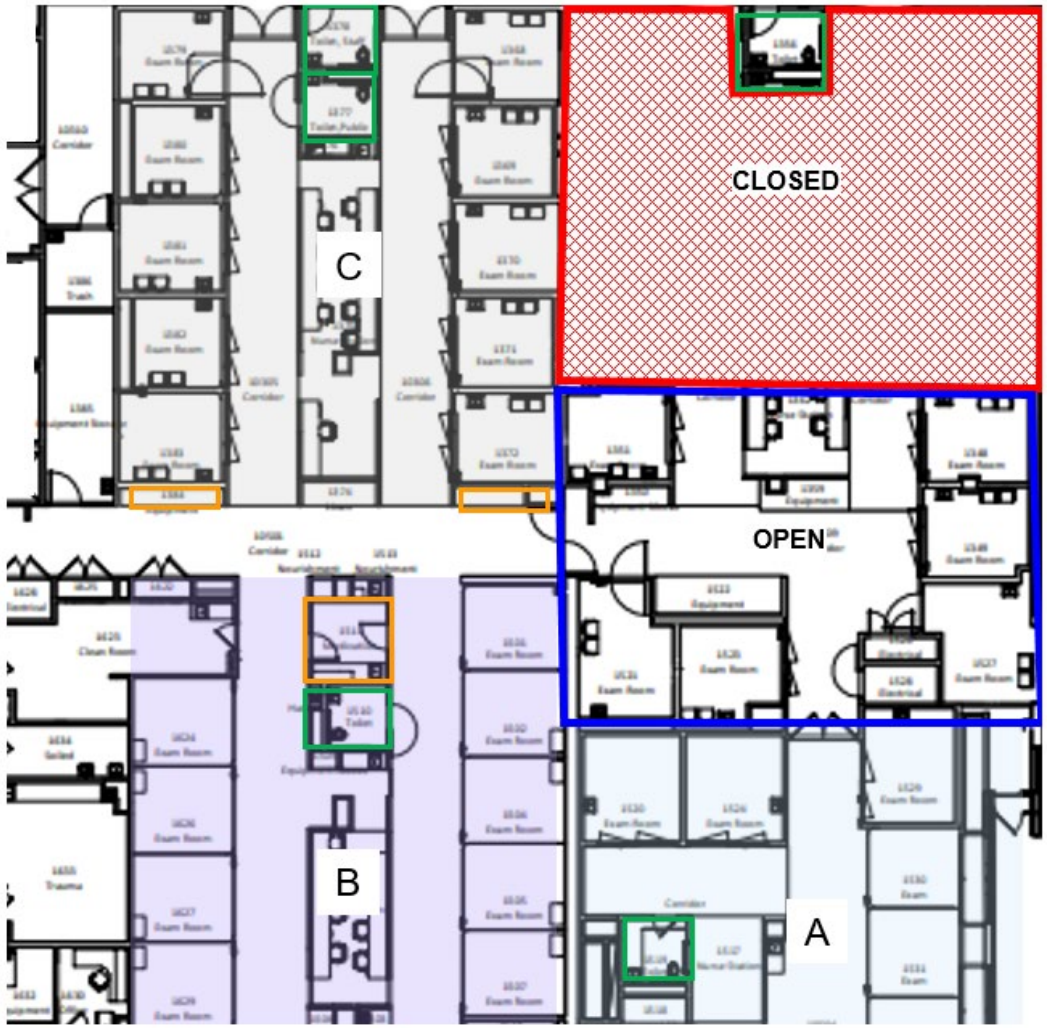
Sun 10/8/2023 5:04 PM

Lord, Shaun

D Pod Floor Repair Phase A

To DG-ED Residents; DG-ED PGY 4 Residents; DG-ED PGY 3 Residents; DG-ED PGY 2 Residents; DG-ED PGY 1 Resident; DG-Nursing ED Unit Coordinator; DG-ED Attendings; DG-ED APP; 'DG-UCC NP'; DG-PEM-Faculty; DG-PEM-Fellows;

This message was sent with High importance.



Boston Medical Center
HEALTH SYSTEM

Emergency Response - Phase B

Localized Response

Event impacts some of the hospital / site operations and requires the response and mobilization of hospital resources beyond normal operations

- All staff remain on duty for a short duration until the extent and impact of the incident is determined.
- The Incident Commander will active *some* Incident Management Team members and their services to manage the incident
- Departments with Phase B tasks will deploy their equipment, supplies, and personnel



Eversource Manhole explosion 5/2023

Emergency Response - Phase C

Hospital-Wide Response

Event impacts normal hospital / site operations and requires the response and mobilization of all hospital resources

- All staff remain on duty
- The BMC Command Center is activated & opened
- The Incident Commander On-Call activates all Incident Management Team members and their services
- Additional staff may be called in and should report to departmental leadership for further instruction
- Some elective clinical operations may need to be cancelled and rescheduled



ED Flood 2/2023

Knowledge Check

Multiple Choice

The Incident Commander may activate *some* members of the Incident Management Team during which Phase

- **B**
- **A and B**
- **D only**
- **A, B, C**

Emergency Response - Phase D

City-Wide Response

Event impacts normal hospital / site operations and further disrupts city infrastructure and services



- All staff remain on duty
- The BMC Command Center is activated & opened
- The Incident Commander On-Call activates all Incident Management Team members and their services
- All hospital resources will be needed to manage incident response
- Elective clinical operations will be cancelled and rescheduled
- Hospital census may be reduced
- Hospital resources will be reassigned/redistributed to maintain critical operations

Knowledge Check

Multiple Choice

The Command Center will normally be opened and activated during phases

- **A, B, C, D – All Phases**
- **C and D**
- **D only**
- **C only**

Workplace Safety

Boston Medical Center
HEALTH SYSTEM

Workplace Safety – General Rules

- Plan ahead and be prepared
- Always be aware of your surroundings
- Use commonly travelled pathways
- Know what safety tools are available to you
- Know where to get help

If you see something – SAY SOMETHING – Call Public Safety at 617-414-4444

Workplace Safety at BMC – Code Green

Code Green **is the hospital / site assessment or response to act(s) of significant and major violence that compromises patient, staff and visitor safety and disrupts the standard of care.**

- Staff should notify Public Safety immediately if witnessing or experiencing any act of violence
- Public Safety leadership has authority to declare a hospital-wide Code Green
  - A hospital-wide Code Green alert will be sent by text, call, or email via the Send Word Now Emergency notification system or at the location of the incident via overhead announcement
  - All staff must follow the directions provided by Public Safety in the announcement(s)

Incident Severity	Impact characteristics
Major	• Threat to life for patients, visitors, staff, or students • Widespread impacts to physical resources • Extended disruption to operations • Significant external resources or support required • International or national media attention • Violation of firearm policy
Significant	• Potential threat to life for patients, visitors, staff, or students • Potential impacts to physical resources • Disruption to operations • Some external resources or support required • Local media attention

Code Green Example – Shelter in Place

S	A	F	E
Secure	**Alert**	**Follow**	**Emerge**
Secure your location. Close/lock doors	Call Public Safety internally at x4-4444 or externally at 617-414-4444 and report conditions *If you are in immediate danger, leave the area and then make the call.*	Follow directions of Public Safety and Police Officers	Emerge when you hear the "all clear" announced or are instructed by police or public safety officers

Code Green Example – Active Shooter

Run

If you can: RUN

Do not take personal belongings

Run in the direction from which the police are coming

Follow all police and public safety directions

Hide

Close and lock doors

Barricade doors with heavy objects

Hide behind desks and furniture

Turn off lights, silence cell phones and pagers

Fight

Use anything as a weapon

Act as a group if you are with others

Commit to your actions

Notify

Call 911 and Public Safety immediately

If you cannot speak, stay on the phone and do not hang up

If you can speak, provide as much information as you can

Run, Hide, Fight does not need to happen in this order
Make the decision that's best when presented

Infant/Pediatric Abduction - Code Pink

Code Pink **is the hospital response to a missing or abducted infant or child**

- **Look for and report any suspicious persons or activities**
- **Search your area including bathrooms, storage, and break rooms**
- **General Services personnel will search common areas and grounds**
- **Cooperate with Public Safety and Police**
  - **The building will be under controlled access**
  - **Public Safety Officers may question and search all individuals (including staff) leaving the facility**

Code Red – Smoke or Fire Condition

R

RESCUE

Move people away from immediate harm

Go to your lateral receiving location

Use your departmental Evacuation Check Sheets

A

ALERT

Pull the fire alarm

Fire alarm pull stations are located at the exit stairwell doors

Call out "Code Red"

Call the Control Center at 4-6666 to report the location and conditions.

C

CONFINE

Close all doors to rooms and areas.

E

EXTINGUISH

If safe - use fire extinguisher to extinguish small fires or escape larger fires

EVACUATE

If smoke or fire are in your immediate area, begin relocating patients, visitors, and staff.

Code Red **is the hospital's fire response plan to a fire or smoke condition**

- **All staff should follow the race plan**
- **Patient care units should follow their unit specific fire response plan**
- **Always keep hallways and exit doors clear**

Code Red – Fire Alarm Activation

What Does the Fire Alarm Mean?

The Fire Alarms can be activated by:

1. Smoke/heat detectors
2. Manually pulling the fire alarm box
3. Activation of the hospitals fire suppression system

What to Expect when the fire alarm system is activated (STOP-LOOK-LISTEN)

First - A loud audible tone sounds to get your attention
Second – Verbal Instructions
Third – One of two things will happen:

The strobe lights will flash but there will be <u>no sound</u>
The emergency is in your building
OR
The strobe lights will flash <u>and</u> a loud <u>audible tone</u> will sound
The emergency is on your floor, the floor above you, or the floor below you



Evacuation

The movement of patients, staff, and visitors from an area when the environment cannot support clinical operations

- The declaring authority will activate the EOP and declare the appropriate Phase
- All personnel will remain available for reassignment and may be asked to perform functions outside of normal responsibilities
- Evacuation operations will depend on the location and evacuation type

BMC executes two types of evacuation: *Emergent and Controlled*

Emergent Evacuation – Immediate risk to life safety for patients and staff

- *In-patient areas will proceed horizontally through a smoke barrier to an adjacent safety zone*
- *Ambulatory areas will begin a vertical evacuation (exit via stairs or safest route)*

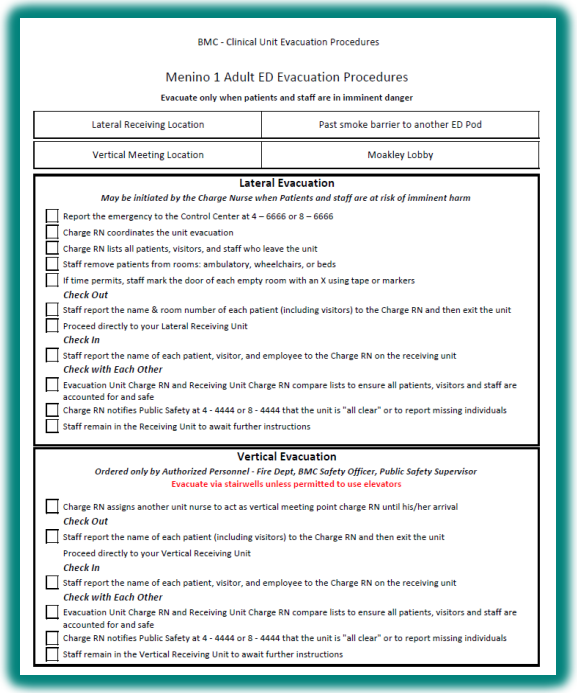
Controlled Evacuation - Planned urgent or non-urgent movement of patients and staff

- *Authority to order a controlled evacuation of an in-patient area is subject to incident type and on-scene resources*

Evacuation Resources

Unit Specific Evacuation Check Sheet

- *Departments should have a unit specific evacuation check sheet posted near emergency flipcharts*



BMC - Clinical Unit Evacuation Procedures

Menino 1 Adult ED Evacuation Procedures

Evacuate only when patients and staff are in imminent danger

Lateral Receiving Location	Past smoke barrier to another ED Pod
Vertical Meeting Location	Moakley Lobby

Lateral Evacuation

May be initiated by the Charge Nurse when Patients and staff are at risk of imminent harm

- ☐ Report the emergency to the Control Center at 4 – 6666 or 8 – 6666
- ☐ Charge RN coordinates the unit evacuation
- ☐ Charge RN lists all patients, visitors, and staff who leave the unit
- ☐ Staff remove patients from rooms: ambulatory, wheelchairs, or beds
- ☐ If time permits, staff mark the door of each empty room with an X using tape or markers

Check Out

- ☐ Staff report the name & room number of each patient (including visitors) to the Charge RN and then exit the unit
- ☐ Proceed directly to your Lateral Receiving Unit

Check In

- ☐ Staff report the name of each patient, visitor, and employee to the Charge RN on the receiving unit

Check with Each Other

- ☐ Evacuation Unit Charge RN and Receiving Unit Charge RN compare lists to ensure all patients, visitors and staff are accounted for and safe
- ☐ Charge RN notifies Public Safety at 4 - 4444 or 8 - 4444 that the unit is "all clear" or to report missing individuals
- ☐ Staff remain in the Receiving Unit to await further instructions

Vertical Evacuation

Ordered only by Authorized Personnel - Fire Dept, BMC Safety Officer, Public Safety Supervisor

Evacuate via stairwells unless permitted to use elevators

- ☐ Charge RN assigns another unit nurse to act as vertical meeting point charge RN until his/her arrival

Check Out

- ☐ Staff report the name of each patient (including visitors) to the Charge RN and then exit the unit

Proceed directly to your Vertical Receiving Unit

Check In

- ☐ Staff report the name of each patient, visitor, and employee to the Charge RN on the receiving unit

Check with Each Other

- ☐ Evacuation Unit Charge RN and Receiving Unit Charge RN compare lists to ensure all patients, visitors and staff are accounted for and safe
- ☐ Charge RN notifies Public Safety at 4 - 4444 or 8 - 4444 that the unit is "all clear" or to report missing individuals
- ☐ Staff remain in the Vertical Receiving Unit to await further instructions

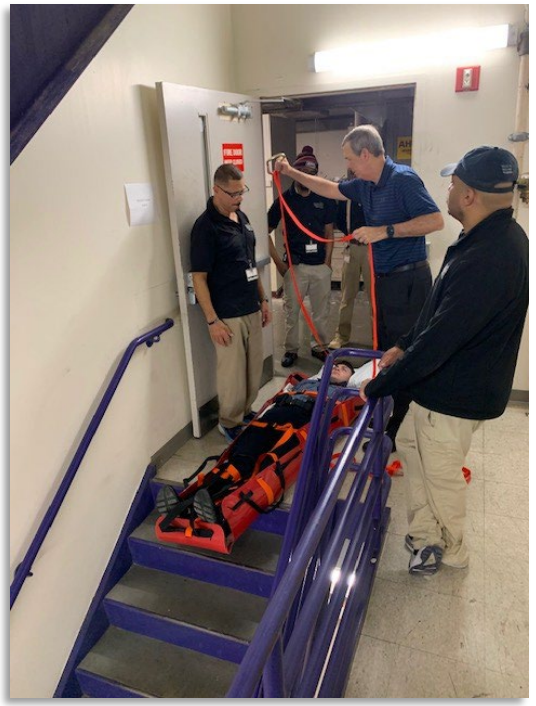
Evacuation Equipment

Stair Chairs are available at each stairwell in ambulatory care buildings

- *Used to move non-ambulatory patients to hallways or nearest exit stairwell*
- *Notify Public Safety and report the location of patients needing assistance*

MedSleds are transport sleds used to quickly move non-ambulatory patients

- Can be used to safely vertically evacuate non-ambulatory patients downstairs



Boston Medical Center
HEALTH SYSTEM

Public Safety will direct emergency response agencies to locations to assist with evacuation

Emergency Notification

BMC uses *AlertMedia* emergency notification system to rapidly disseminate messages via phones, pagers, text messages, and emails

- All staff will receive a BMC ALERTS for major emergencies
- Designated departments/groups and departmental leadership will receive Phase A-D notifications

You may also be notified by:

- Overhead announcements
- Direct call from your supervisor
- Department huddles
- All staff emails and postings on the HUB

Tools for Employees

MY-EOP App

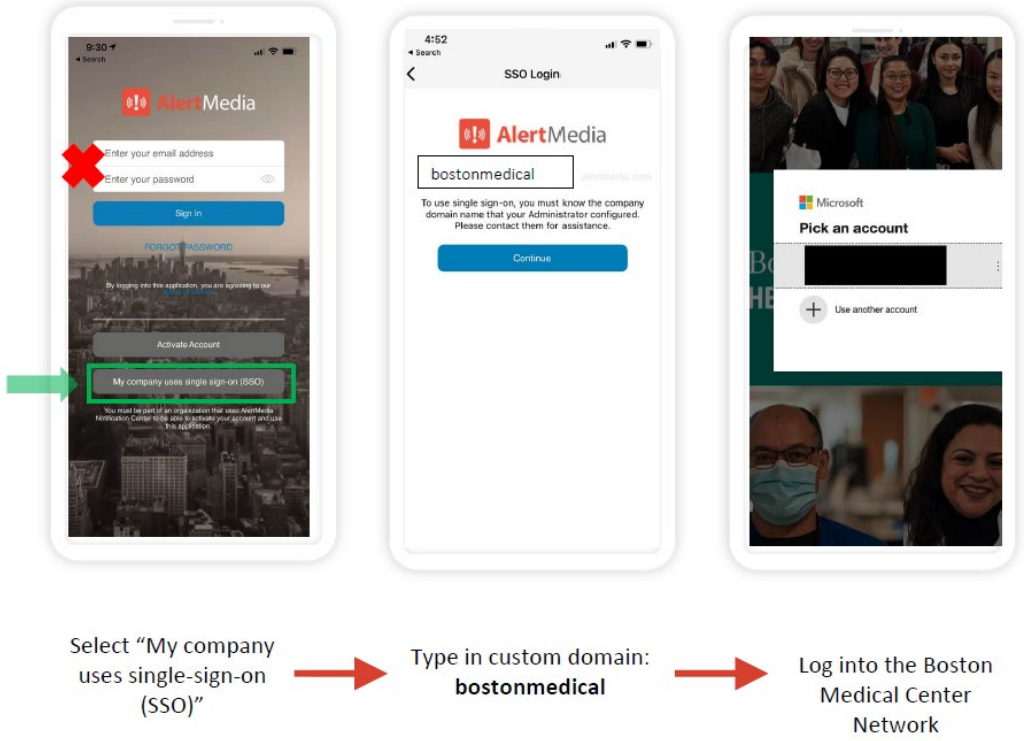
- Direct links to emergency numbers and plans
  - ***Enter Code: BMC | Password: BePrepared***

BMC Alerts – Alertmedia

- Notification via text, email and phone call for major emergencies
- Available to all employees and physician staff

Sign up for major emergency notifications by:

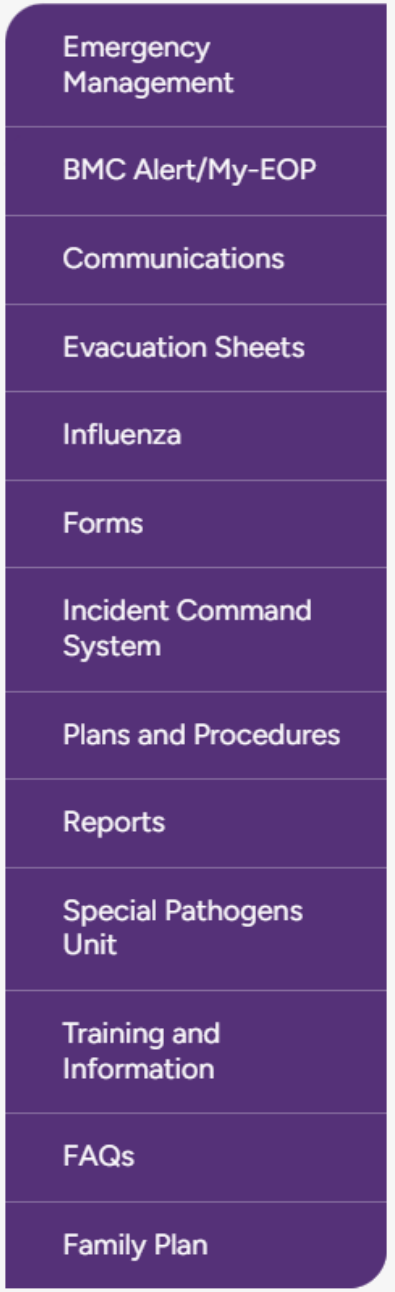
- Scan the barcode
- Select SSO – enter ***bostonmedical***
- ***Log into the BMC network using your BMC credentials (username and password)***



Tools for Employees

- Visit BMC's Emergency Response Webpage for plans and information
- A red banner will appear on the BMC Intranet home page with information and instructions
- Event specific links will be posted on the BMC Intranet home page
- Safety Flip Charts
- BMC Emergency Management APP – MyEOP
- Red Badges





Boston Medical Center
HEALTH SYSTEM

Emergency Management

The Office of Emergency Management is responsible for all aspects of institutional response to external and institutional emergencies that may affect hospital operations.

Primary Contact Information

Zania Campos

Director of Emergency Management

Phone: 617-835-9129

Email: zania.campos@bmc.org

Location: Solomon Carter Fuller 4th floor RM 405

Thank you for participating and completing
Emergency Management & Preparedness
Annual Training

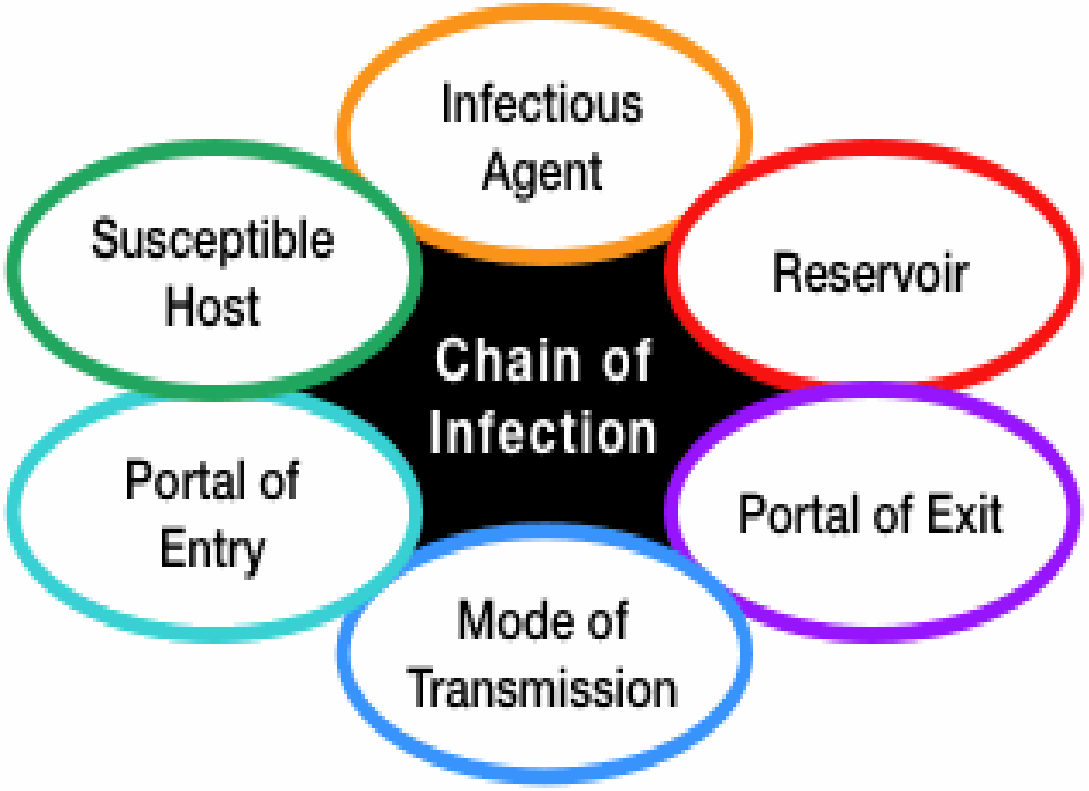
Boston Medical Center
HEALTH SYSTEM



Boston Medical Center
HEALTH SYSTEM

Break the Chain of Infection!

- Wash hands
- Cough etiquette
- Get Vaccinated – Influenza and Hepatitis B
- Don’t work if you are ill
- Disinfect shared office equipment (i.e., Computers, Phones, shared workstations).
- Disinfect patient care equipment and environment
- Appropriate use of PPE
- Proper Handling of needles and Sharps



First Line of Defense – Hand Hygiene

- Whether you work in an office or operating room...



...hand washing is key!

Hand Hygiene : The Key to Preventing Infections

WHAT? Hand hygiene applies to the use of either alcohol-based hand rub or the use of soap and water
WHEN? When entering and exiting patient environment; before using and after removing gloves
HOW? Rub hands vigorously for at least 15 seconds
WHICH? Hand Sanitizer, soap and water if hands are visibly soiled
WHO? All healthcare providers, patients, family



Remember! The use of gloves is NOT a substitute for hand hygiene



Handwashing Sinks

- Designated **Clean** Sinks are for **Handwashing only**
- Handwashing sinks are separate from patient-use sinks and are not used for waste disposal.
- Designated **Dirty** Sinks are NOT to be used for Handwashing.

Clean Sink

Handwashing Only



Dirty Sink

Do Not Use For Handwashing



Accidental Exposures

Boston Medical Center
HEALTH SYSTEM

Standard Precautions

Personal protective equipment (PPE)

- Gloves
- Mask and **eye protection** (***exposure to the eyes is the most common splash-type blood exposure at BMC***)
- Gown if contamination is likely

When working with Personal Protective Equipment (PPE), it is important to:

- Wear the **appropriate** equipment
- Wear **adequate sized** equipment
- Keep this equipment **readily available**
- **Dispose** of the used equipment properly

Standard precautions are the **minimum** infection prevention practices that should be used in the care of **all patients all of the time regardless of the infection status.**







Transmission-based Precautions

When to use these?

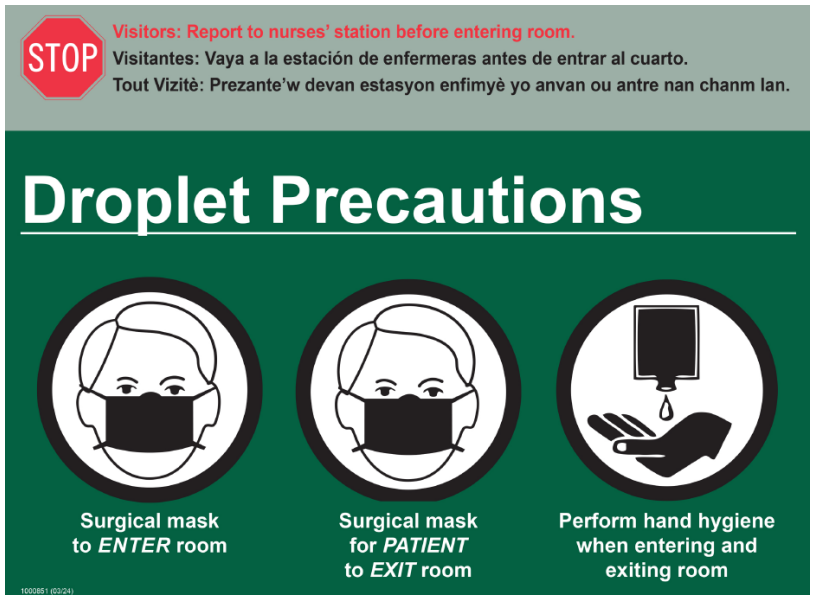
- Patients ***known*** or ***suspected*** to have any infections for which additional precautions are needed to prevent transmission
  - Contact (MRSA, VRE, MDROs)
  - Contact Plus (C Diff, Norovirus, Candida Auris)
  - Droplet (Influenza, Pertussis, Meningococcemia, Mumps, Rubella)
  - Airborne (M. tuberculosis, Varicella, Measles)
  - Enhanced (COVID-19, M-Pox)

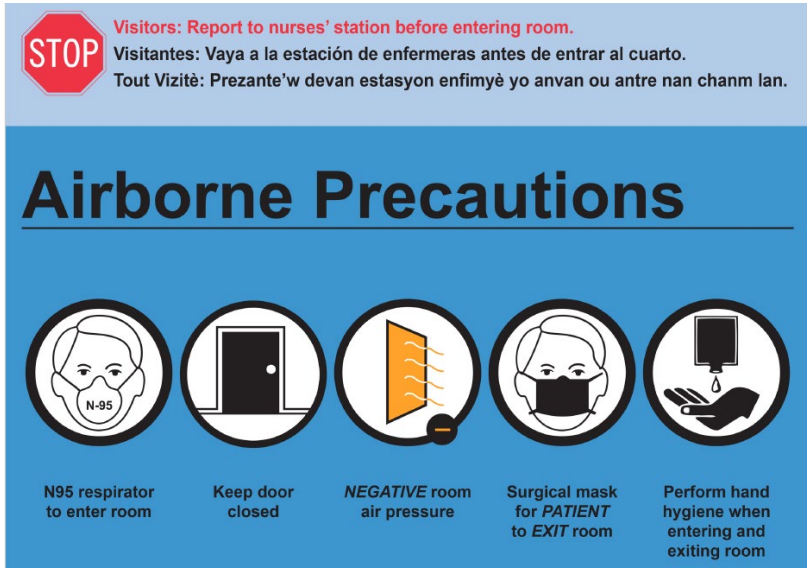
- Use appropriate PPE based on mode of Transmission

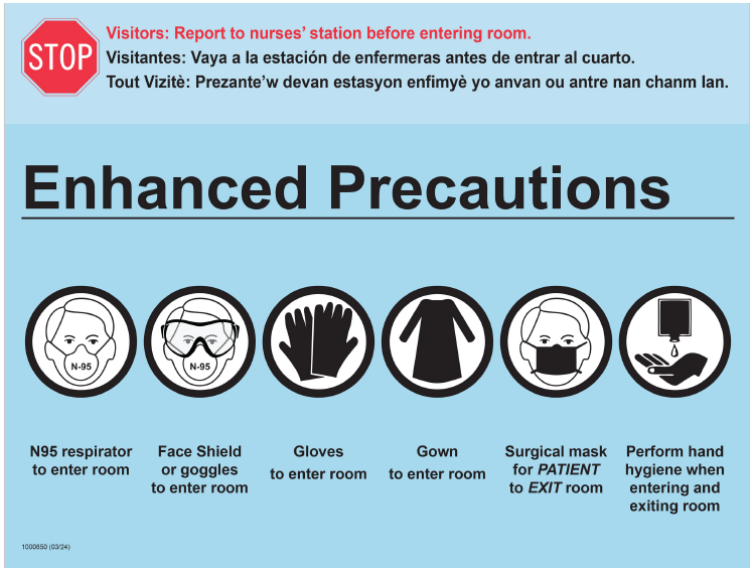
Preventing the Spread of Infection: Communication and Signage











Blood And Body Fluid Exposure

Does your job include potential exposure to blood or other body fluids?

Boston Medical Center
HEALTH SYSTEM

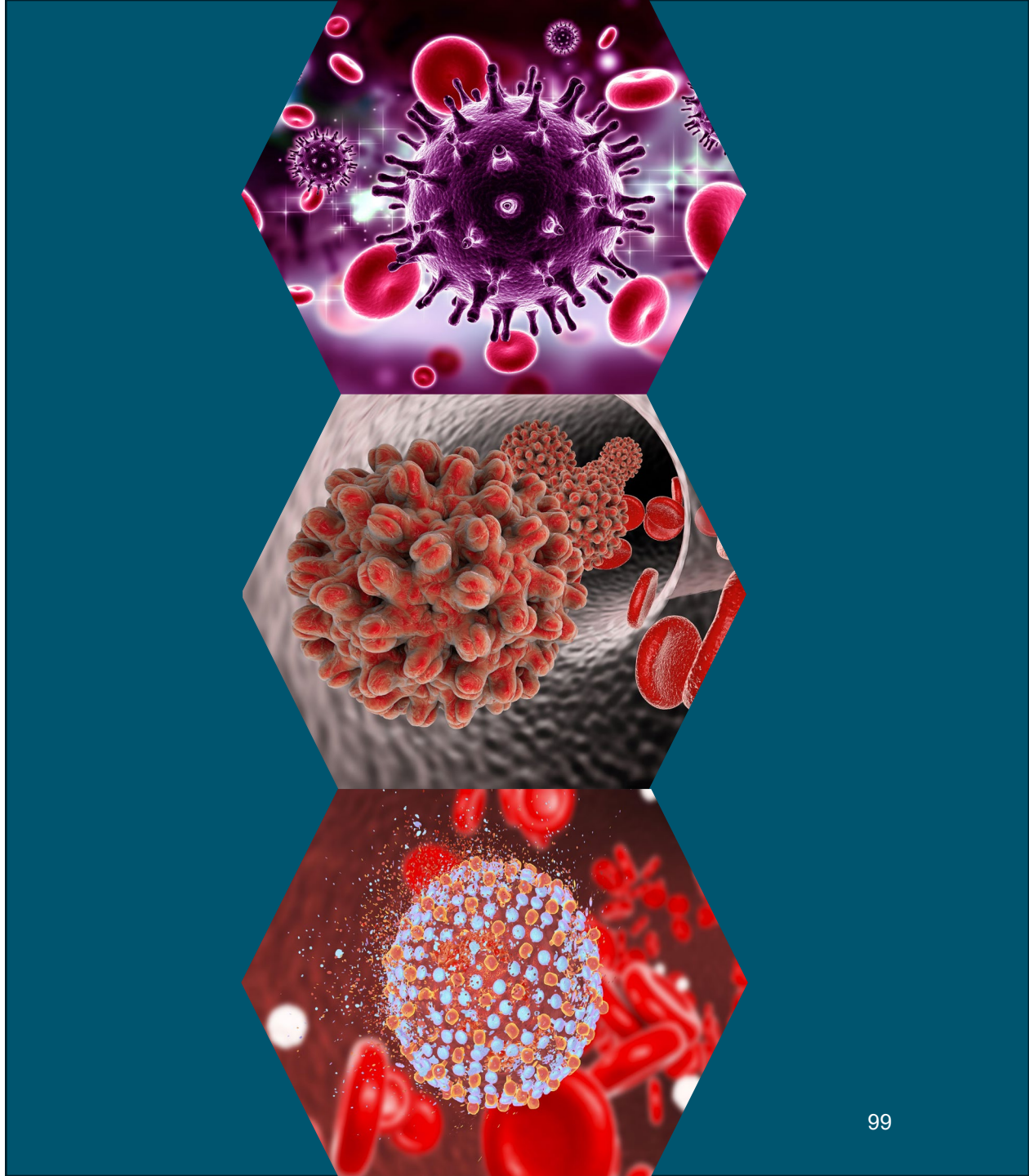
Bloodborne Pathogens (BBPs)

3 BBPs of concern:

- Human Immunodeficiency Virus (HIV)
- Hepatitis B virus (HBV)
- Hepatitis C virus (HCV)

Risk of infection if exposed to blood with the virus is approximately:

- HIV: 0.2%
- HBV: 20%
- HCV: 2%



How do I know if I've been potentially exposed to a bloodborne pathogen?



Bloodborne Pathogen Exposure (BBPE)

An **exposure** means the contaminated fluid reaches your blood stream, either through:

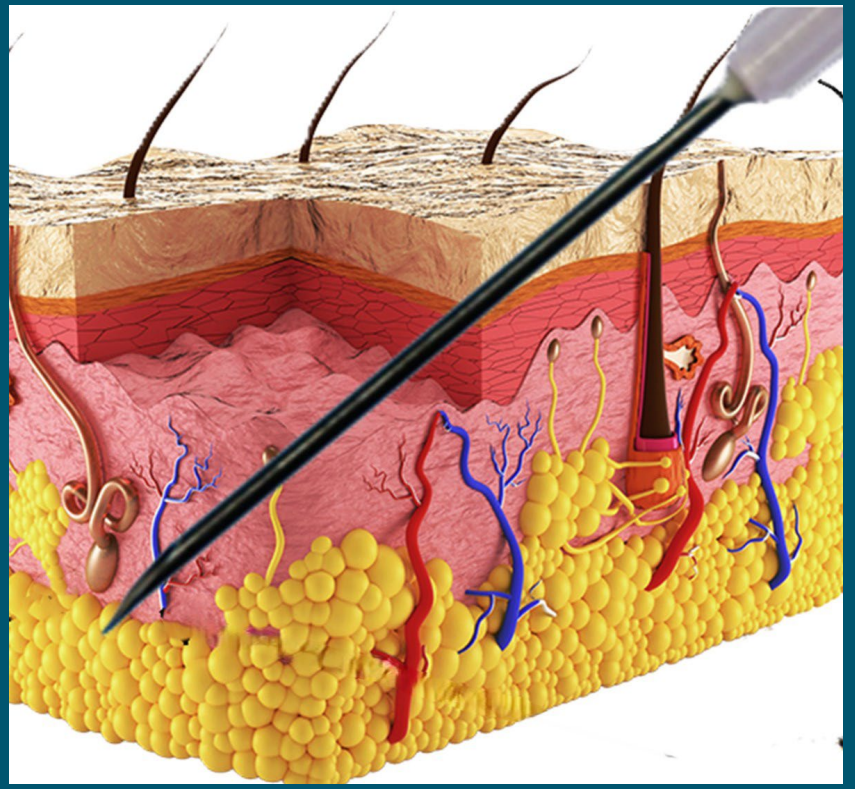
1. A contaminated instrument such as a scalpel or needle piercing completely through your skin to underlying tissue

or

2. Contaminated fluid being absorbed through mucous membranes (eyes, mouth, etc.)

*** Blood contacting intact skin is **not** an exposure***

*** Spit, vomit, urine and feces are **not** contaminated with BBPs and contact with these are **not** a BBP exposure, unless they are contaminated with blood ***



What to do if you experience a BBPE?

- **Wash**/rinse wound or exposed area or flush eyes immediately, as applicable.
- **Report** the incident to your supervisor and complete an **RL Employee Safety Event**
- Have a member from the source patient's treating team **consent** and draw the patient for BBP testing (do not do this yourself, as the exposed worker)
- Call or go to the **BMC-Main Occupational Health** clinic on the ground floor of Dowling **(BMC Brighton Clinic is in CCP 9th floor)** (**BMC-S clinic is in the MOB 1st floor**) to be evaluated, tested, and potentially treated. If after hours, go to the ED and contact Occupational Health the following business day.





Boston Medical Center
HEALTH SYSTEM

Prophylaxis

If you have a bloodborne pathogen exposure, you may be given prophylactic medication to help avoid infection

- HIV prophylaxis is most efficacious when started as soon as possible
  - Best if started within 24 hrs
  - Must take daily for 28 days

- Hepatitis B prophylaxis for employees who are not immune
  - Injection of Hep B antibodies.
  - Pre-exposure prophylaxis with vaccine is most effective

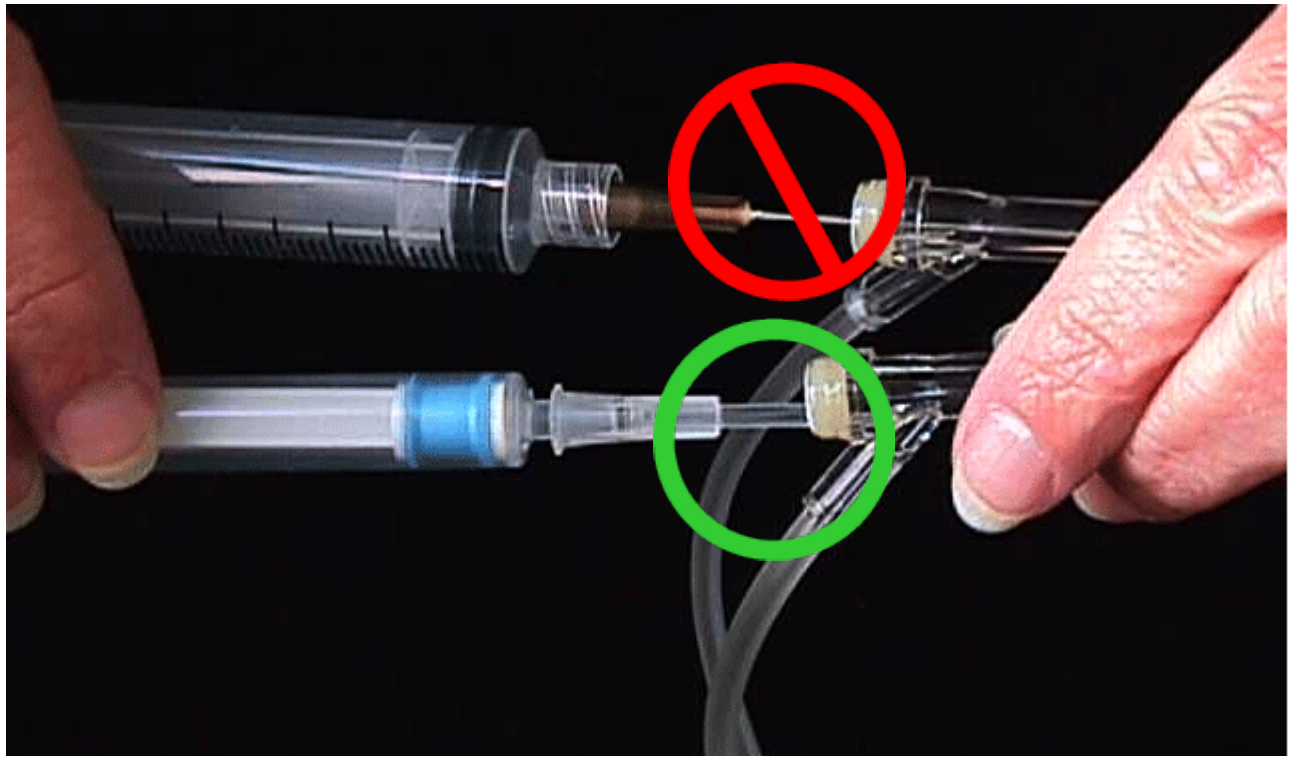
- No prophylaxis for Hep C
  - But there is a cure if infection occurs



Sharps Policies

DOs and DON'Ts

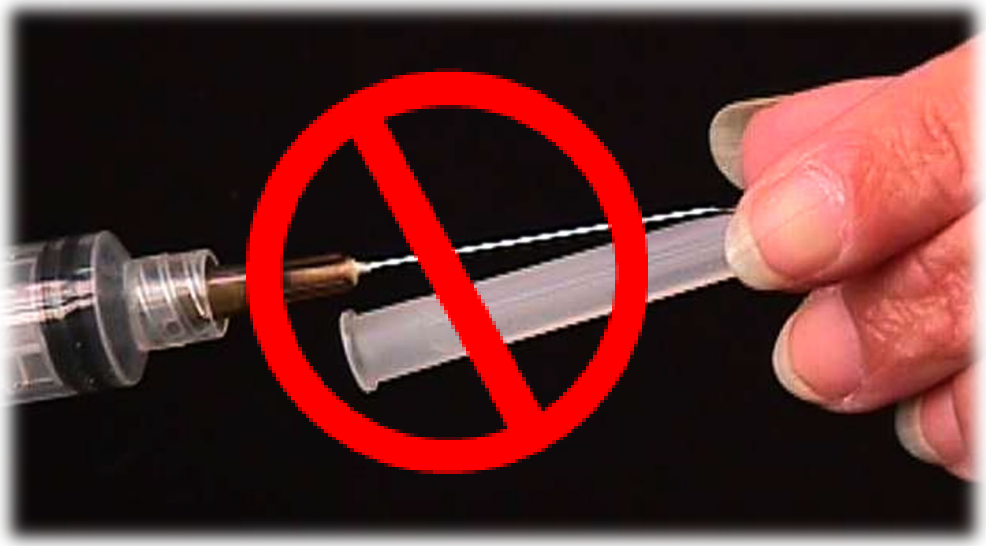
- DON'T insert exposed metal needle
- DO insert protective plastic needle



Sharps Policies

DOs and DON'Ts

- DON'T recap needles by hand



Sharps Policies

DO

Place needles into approved sharps containers



DON'T

Overfill Sharps Containers



Sharps Policies

DOs and DON'Ts

- DON'T leave exposed or used needles out in the open. Make certain they *fit all the way into sharps containers*.
- DO use safety syringes (e.g., retractable syringe, needle with safety device)





Safe Disposal of Medical Equipment and Biohazard Waste

- Discard in appropriate waste receptacle
  - Use biohazard waste receptacles for *contaminated medical items ONLY*
  - Regular trash DOES NOT go into biohazard receptacles.





Disposal of Medical Equipment and Biohazard Waste

- Biohazard waste receptacles are intended for *contaminated medical items ONLY*
  - Includes items saturated with blood or bodily fluids. Dispose in redline lined biohazard receptacles.





- Sharps, including needles, syringes, and blades, should be disposed in the sharps container.

- DO NOT dispose regular trash in the biohazard receptacles



Waste Disposal Guidelines

Understanding how to dispose of regulated waste is a necessary part of keeping BMC safe and protecting the environment. Training (on-line) is required for chemical and hazardous waste pharmaceutical management.

Regulated Medical Wastes

(Biological Waste)





Bloody items, body fluids, tissues, and sharps like syringes. Dispose in redline lined biohazard receptacles. Sharps disposed in sharps containers.

Chemical Waste

(Hazardous Waste)



Dispose of expired or spent chemicals such as cleaners, oil, lab chemicals and some medications (Hazardous Waste Pharmaceuticals) in their labeled waste containers and placed in the satellite accumulation area (SAA).

Hazardous Waste Pharmaceuticals (Black Bucket Waste)



Black buckets are typically located in the medication rooms in patient areas. A placard is posted next to each bucket identifying the hazard waste pharmaceuticals requiring this type of disposal. Other unused pharmaceuticals are sent back to the pharmacy.

Hazardous Waste Removal Contacts



CHEMO WASTE BUCKET
Call or email Environmental services (EVS)



BIOLOGICAL WASTE AND SHARPS
Call or email Environmental services (EVS)



HAZARDOUS PHARMACEUTICAL WASTE
Call or email Environmental Health and Safety (EHS)



NARCOTICS WASTE BUCKET
Call or email Environmental services (EVS)



BATTERY RECYCLE BUCKET
Call or email Environmental Health and Safety (EHS)



SATELLITE ACCUMULATION AREA
Call or email Environmental Health and Safety (EHS)

Approved Disinfectants Products

- Use only hospital-approved wipes
- All reusable medical equipment must be cleaned and disinfected according to the manufacturer's instructions to prevent patient-to-patient transmission of infectious agents.
- Contact time = wet time (keep track of wet time using clock, watch, etc)
- Super Sani Wipes ("Purple Top") = **2 minute** Contact Time
- Bleach Wipes ("Orange Top") = **4 minute** Contact Time





Transport of Instruments

- All transport containers must be **rigid** and **puncture-resistant**.
- All dirty transport containers must be **labeled biohazard**.
- All transport containers must **remain closed** at all times to prevent accidental exposure, injury, or drying of soil.
- **Soiled instruments must be kept moist at all times until returned to CPD for reprocessing.**
- **NEVER transport any contaminated instruments through the halls, from bedside to soiled utility room, uncovered, wrapped in chux, or covered with a plastic bag or gloves.**





WHAT IS A STROKE?
A STROKE CAUSES PARTS OF THE BRAIN TO BECOME DAMAGED OR DIE.



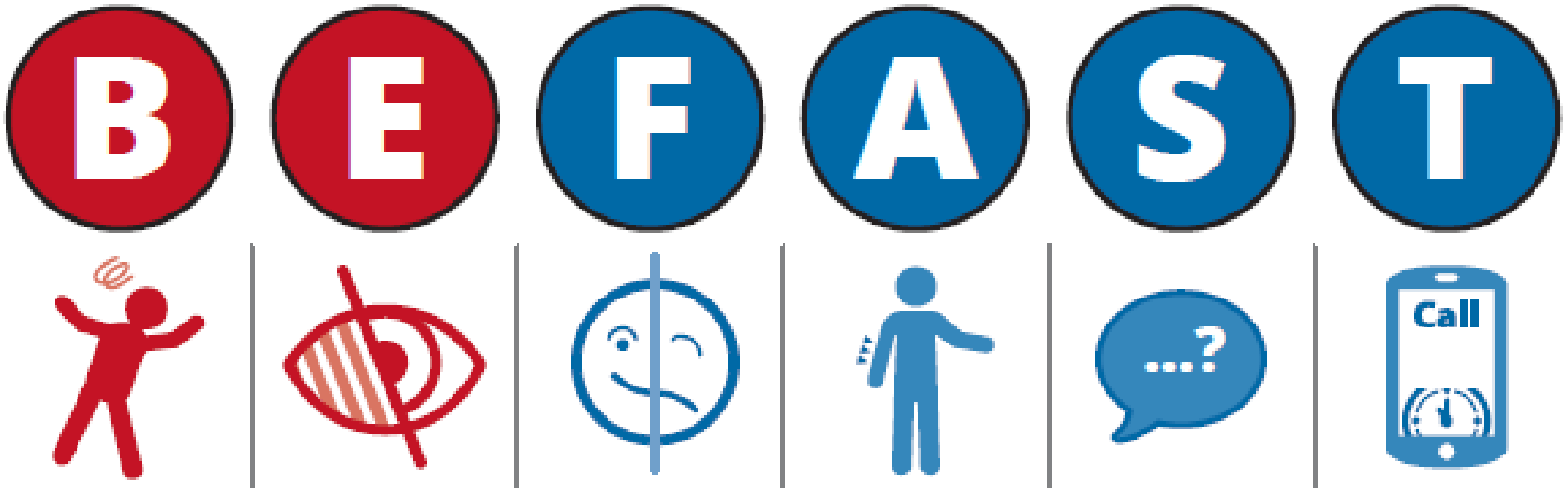
Boston Medical Center
HEALTH SYSTEM

Stroke Awareness Matters (SAM) - Start With Your Heart

About Stroke | Stroke | CDC

HOW TO SPOT A **STROKE**

SPOT A STROKE in the COMMUNITY? **DIAL 911** to ACTIVATE EMERGENCY RESPONSE



Balance
Sudden loss of balance, dizziness

Eyes
Sudden loss of vision or blurred vision

Face
Uneven smile, one side of face is drooping or numb

Arm
One arm is weak or numb

Speech
Slurred speech or difficulty speaking

Time
Time to Activate Emergency Response immediately

Boston Medical Center
HEALTH SYSTEM

Stroke Awareness Matters (SAM) - Start With Your Heart

SPOT A STROKE AT BMC?

BMC MAIN	BMC Brighton	BMC South
TO ACTIVATE EMERGENCY RESPONSE ➢ If person is INPATIENT: STATE "**CODE STROKE**" AND LOCATION ➢ If person is OUTPATIENT, VISITOR OR STAFF: STATE "**PROCEED OUT**" AND LOCATION	**Call "Code Stroke" dial 666 for all code strokes- inpatient and outpatient** **Operator should put location and room if available.**	**Call out "Code Stroke" for inpatients.** **For all others in the hospital, we call a "Rapid Response."** **The team will come to the location, patient would then be transferred to the ED for further evaluation.**
DIAL 4-7777	**DIAL 666**	**DIAL 5555**

Tuberculosis (TB) Informational

Boston Medical Center
HEALTH SYSTEM

What is TB?

TB is a disease caused by a bacterium called Mycobacterium tuberculosis (M. tuberculosis).

The bacteria usually attack the lungs, but can attack any part of the body such as lymph nodes, bones, joints, the brain, and other organs.

- If TB is treated properly, most people can be cured of TB.
- If TB is NOT treated properly, people can die or develop drug-resistant forms of TB.

The Global Threat of TB

Although TB is preventable and treatable, it is still one of the world's deadliest diseases.

An estimated 2 billion people, or one third of the world's population, are infected with M. tuberculosis.

- Each year, approximately 9 million people develop TB disease.
- 1.4 million people die of TB disease each year.

TB in the United States

Although the number of people with TB disease in the United States has been declining over the past several years, challenges remain to control TB:

- TB is reported in almost every state and is increasing in some areas
- TB affects racial and ethnic minorities disproportionately
- Drug-resistant TB is increasingly challenging to treat
- Management of patients with comorbidities, such as HIV, diabetes, and other immunocompromising conditions, is difficult
- More than half of all persons in the United States who have TB disease are foreign-born residents

TB Transmission

TB is spread through the air from person to person. Tiny water particles containing M. tuberculosis may be expelled into the air when a person with infectious TB of the lungs, airway, or larynx:

- Coughs
- Sneezes
- Speaks
- Sings

These particles, called droplet nuclei, can remain in the air for several hours, depending on the environment.

TB Transmission and the Development of TB Disease

If another person inhales air that contains droplet nuclei, they may become infected. However, not every person that is exposed to TB becomes infected with M. tuberculosis.

Additionally, not everyone infected with M. tuberculosis becomes sick. People who are infected but not sick have latent TB infection. Some people with latent TB infection go on to develop TB disease.

Thus, there are two TB-related conditions:

- Latent TB infection (**LTBI**)
- TB disease

About 5% to 10% of persons who have a latent TB infection and normal immune systems will develop TB disease at some point in their lives. The risk of developing TB disease is the highest in the first 2 years after infection.

Risk of Developing TB Disease

The risk of developing TB disease is much higher for persons with weakened immune systems than for persons with normal immune systems. For example, for people with untreated TB infection and untreated HIV infection, the risk is about 7% to 10% per year, a very high risk over a lifetime.

- HIV infection is the strongest known risk factor for progressing to TB disease.

Other people that have weak immune systems that put them at high risk for developing TB disease include:

- Children younger than 5 years of age
- Persons who are receiving immunosuppressive therapy
- Persons with silicosis, diabetes, chronic renal failure, leukemia, lymphoma, or cancer of the head, neck, or lung
- Persons who have had a gastrectomy or jejunoileal bypass
- Persons who weigh less than 90% of their ideal body weight
- Persons with substance use disorder

Symptoms of TB Disease

Persons with TB disease usually have one or more symptoms. Because different parts of the body can be affected by TB, symptoms can vary.

General symptoms of TB disease:

- Fever, chills, night sweats, weight loss, appetite loss, fatigue, malaise

Symptoms of pulmonary TB disease:

- Cough lasting 3 or more weeks, chest pain, coughing up blood or sputum (phlegm)

Symptoms of extra-pulmonary TB disease depend on the part of the body that is affected. For example:

- TB disease in the spine may cause back pain
- TB disease in kidneys may cause blood in urine
- TB disease in lymph nodes may cause swelling in the neck

BMCHS Has a Plan to Control TB Infection

- Identify patients with active TB early
  - Signs & Symptoms of TB = Productive cough — hemoptysis, Night sweats or fever, Unexplained weight loss
- Initiate airborne precautions immediately
- Initiate effective anti-TB therapy promptly
- Use a properly fitted N95 respirator or PAPR for room entry or for cough-inducing procedures
- Annually screen workforce
- Exposure follow-up process
  - At BMC Main, report to Occupational Health
  - At BMC-South, report to Employee Health
  - At BMC-Brighton, report to Employee Health



Infection Control

Since TB is an airborne disease that can be transmitted from one person to another, it is important to practice appropriate infection control procedures to protect others from getting TB.

This is especially important for health care facilities and other congregate settings. All health care facilities need an infection-control program. This program should be designed to ensure:

- Prompt detection of TB
- Airborne precautions to prevent the spread of TB
- Treatment of persons who have suspected or confirmed TB disease

Personal respirators should be worn by health care workers to prevent the inhalation of droplet nuclei. Surgical masks should be worn by infectious TB patients to prevent droplet nuclei from being expelled into the air.

Target Testing

Targeted testing is an essential TB prevention and control strategy in the US. It is used to identify and treat persons who are at high risk for latent TB infection or at high risk for progressing from LTBI to TB disease.

Identifying and treating persons who have LTBI is important because treatment can prevent progression to active TB disease in the future. This helps to stop the further spread of TB in the community and in our hospital.

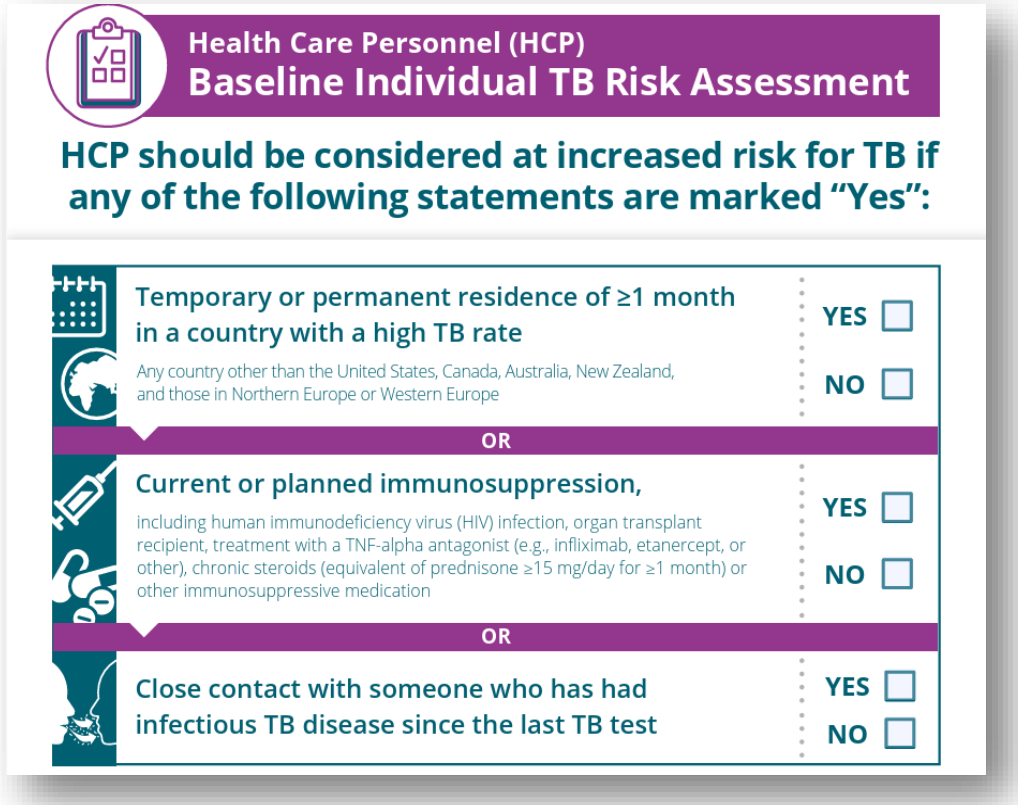
TB testing is performed:

- Upon hire for healthcare workers
- After high-risk exposure
- Annually for employees in high TB exposure risk teams

TB Screening and Testing for Healthcare Workers (HCWs)

Upon hire:

- TB risk assessment (form)
- TB symptoms screening
- TB test



If positive TB test:

- Symptoms evaluation and Chest X-Ray
- Treatment of LTBI is encouraged
- Untreated LTBI: employee will need annual TB symptoms screening

Post-exposure Screening Test

In the case of a TB exposure, exposed healthcare workers (HCWs) with a previous negative TB test result should be tested immediately to establish their baseline TB status, and re-tested 8 to 10 weeks after the last known exposure.

HCWs with a documented history of positive TB test result do not need to be re-tested after exposure to TB. They should receive a TB symptom screen and if they have symptoms of TB, should be evaluated for TB disease.



Groups at High Risk for TB Infection

- Contacts of persons known or suspected to have infectious TB disease
- People who have come to the United States within the last 5 years from areas of the world where TB is common (for example, Asia, Africa, Eastern Europe, Latin America, and Russia)
- Persons who visit areas of the world where TB is common, especially if visits are frequent or prolonged
- People who live or work in congregate settings whose clients are at increased risk for TB disease
- Health care workers who serve clients who are at increased risk for TB disease
- Populations defined locally as high risk for latent TB infection or TB disease, such as medically underserved, low-income persons, or persons with substance use disorder.
- Infants, children, and adolescents exposed to adults at increased risk for infection or disease

Annual Testing

Approved diagnostic tests that can be used to detect TB infection include:

- The Mantoux tuberculin skin test (TST)
- Interferon-gamma release assays (IGRAs)

A positive TST or IGRA result only indicates if someone has been infected with M. tuberculosis. These tests cannot identify if a person has TB disease.

Summary

- TB is spread through the air from person to person
- Many people have LTBI around the world and in the US
- Persons with LTBI are at risk to progressing to TB disease
- Detecting and treating LTBI prevents the spread of TB disease in our community and hospital
- Targeted TB testing is required for **HCW**s: upon hire, after high risk exposure and annually for a small group of **HCW**s with sustained exposure risk
- Although most **HCW**s are no longer required to complete annual testing for TB infection, annual completion of TB risk assessment remains required for all **HCW**s (even those working remotely)

Infection Prevention – Additional Resources for You

Infection Prevention Resources for BMC Main are available on the BMC intranet under the Infection Prevention and Control Department: https://hub.bmc.org/departments/infection-prevention-and-control

BMC's Infection Control Policies can be located on Policy Tech under Infection Prevention and Control

Infection Prevention personnel are available to answer any questions about the Exposure Control Plan and other infection control topics.

BMC-Main office is open from Monday through Friday from 8:00 a.m. - 4:00 p.m.

The telephone number is **617- 414 -7220**.

BMC-South, please call **508-427-3161**

BMC-Brighton, please call **617-789-2373 or 617-789-3488**

Contact Infection Prevention Department

Phone: 617-414-7220
Email: DG-Infection Prevention DG-InfectionPrevention@bmc.org
Fax: 617-638-8070
Web: https://hub.bmc.org/departments/infection-prevention-and-control

BMC Brighton
Phone: 617-789-2373 or 617-789-3488
Email: "DG-Brighton Infection Prevention" DG-BrightonInfectionPrevention@bmc.org

BMC-South: 508-427-3161
Email: Margarida.martins-pires@bmc.org or Kathleen.malm@bmc.org
Fax: 508-427-2205

Boston Medical Center
HEALTH SYSTEM

Infection Prevention + TB Annual Training Quiz

Please complete the Quiz. To begin, click on **Next**.
There are 13 questions, with a passing score of 100%

Boston Medical Center
HEALTH SYSTEM

Question:

How many people are infected with M. tuberculosis worldwide?

A. 2,000,000 = 2 Million
B. 10,000,000 = 10 Million
C. 200,000,000= 200 Million
D. 2,000,000,000 = 2 Billion (2 billion is correct)



Question:

How is TB transmitted?

A. Coughing (Coughing is correct)
B. Kissing
C. Shaking hands
D. Sharing foods
E. All the above



Question:

True or False?

People with latent TB Infection (LTBI), who do not have active TB disease, can still spread the infection to others

(correct answer is False)



To return to work after having a new positive TB Test, employees must:

a. Get a note from their doctor
b. Wear a mask at work
c. Have clearance by BMCHS Occupational Health
d. Take TB drugs each morning
e. All of the above

Which of the following activities WILL NOT help prevent an accidental needle stick:

a. Disposing of needles into approved sharps containers
b. Recapping a needle by hand
c. Using a plastic access device (instead of a needle) to access IV tubing
d. Using a safety syringe

What is a key infection prevention strategy to perform before putting on (donning) and after removing (doffing) gloves?

a. Perform hand hygiene
b. Ask the patient how they are
c. Identify other types of PPE to use
d. Put on an extra pair in your pockets in case you need them

Serious respiratory illnesses are spread by:

a. Coughing
b. Sneezing
c. Both of the above
d. None of the above

Hepatitis B vaccinations are available from Occupational Health, at no charge, to all staff who:

a. Work at the hospital
b. Are in the National Guard
c. May be exposed to blood or body fluids
d. Speak with patients

Patient care equipment that is shared (e.g. vital signs machine, glucometer's) should be:

a. Discarded after use or when a patient is disharged
b. Sent to Central Processing Department for disinfection after use
c. Disinfected between patients
d. Sent home with the patient on whom it was used

To protect patients and staff, the Centers for Disease Control recommends that healthcare workers:

a. Do not talk about work when off the job
b. Speak softly in elevators
c. Get an annual flu shot
d. Do not use patient restrooms

The symptoms of Tuberculosis (TB) are:

a. Productive persistent cough
b. Night sweats
c. Unexplained weight loss
d. All of the above

Appropriate routine management of patients with suspected of known infectious TB include:

a. Placement in airborne isolation with the door closed
b. Use of an N95 respirator for all individuals entering the isolation room
c. Patient wears a surgical grade mask when out of the room
d. All of the above

Contact time or “wet time” is:

a. How long it takes for a disinfectant to dry on a surface
b. How long a disinfectant needs to stay wet on a surface in order to be effective
c. The time required for EVS to clean high-touch surfaces in a patient room

TB Risk Assessment Screener

Per the **CDC** and **Department of Public Health**, hospital employees who have had a positive TB test in the past (i.e. has untreated LTBI) need to complete an annual TB symptom screen.

If you have **never** had a positive TB test:

- No further action is necessary, you may exit the course

If you've had a **positive TB test** in the past (**LTBI**):

Sign-in to your employee health portal to complete your TB symptom screen:

- https://webchartnow.com/bmcprod/webchart.cgi

Thank you for your cooperation.

Boston Medical Center
HEALTH SYSTEM

Environmental Health and Safety and Laura's Law

BMC Brighton

Boston Medical Center
HEALTH SYSTEM

Introduction to Safety

This course is an annual requirement and serves as a refresher to policies and procedures you have already learned through programs like New Employee Orientation.

Information included is designed to help ensure a safe environment for our patients, staff and visitors. Many of the topics included in this course are required by the Centers for Medicare and Medicaid Services (CMS), the Joint Commission, the Department of Public Health (DPH), and the Occupational Safety and Health Administration (OSHA).

Please read the content in the following screens carefully and then complete the post-test. You may want to reference other materials to answer questions. Some additional resources available to you are:

- Department specific policies
- Safety policies on the BMCHS Site Intranet
- The Emergency Instructions Flip Charts

If you have questions, please contact your Supervisor, a Clinical Educator, Nurse Manager.

Introducing Laura's Law

Boston Medical Center
HEALTH SYSTEM

Laura’s Law

Learning Objectives:

- What is Laura’s Law.
- Wayfinding - What are you as a BMC employee responsible for.
- Communication - Steps to take when communicating with disabled patients seeking emergency care.

Massachusetts passed a new law to ensure patients, and their families can find the Emergency Department at a hospital

In 2016, Laura Levis died of cardiac arrest following an asthma attack outside of an entrance to Somerville Hospital. Laura was unable to get inside of Somerville Hospital for treatment because:

- There was no signage around the hospital that showed where to the Emergency Department entrance was located
- A well-lit entrance Laura approached to get inside the hospital was locked, and no one was stationed at the security desk next to the entrance
- Laura tried to get the attention of people inside, but no one was visible and there was no emergency call box at the entrance
- 911 responders had difficulty finding Laura as they were sent to a mailing address and not the Emergency Department

Laura's Law was enacted to improve Emergency Department wayfinding in Massachusetts and prevent a tragedy like Laura's death from happening again

Emergency Department Wayfinding

Boston Medical Center
HEALTH SYSTEM

Patients and families who come to BMCmay need emergency care but are not able to find the Emergency Department.

As an employee at BMC you're expected to:

- Provide patients and families with **clear directions to the Emergency Department**
- If patients and families are not able to understand the directions, **immediately notify your supervisor for assistance**
- If your supervisor is not available, immediately **contact Public Safety for assistance**
- If a patient is having a medical emergency **inside** of a BMC building and is unable to bring themselves to the Emergency Department, **immediately notify your supervisor and Public Safety.**
- If a patient is having a medical emergency and the patient **outside** of a BMC building, **immediately notify Public Safety either by dialing 4-4444or using a Blue Call Box**

Communicating with Patients at the Emergency Department

Boston Medical Center
HEALTH SYSTEM

Specifically, there may be patients with disabilities or patients who are deaf/hard of hearing/deaf blind may need emergency care but are not able to find the Emergency Department.

- If you are unable to communicate with a patient with disabilities in need of Emergency Care, immediately contact your supervisor.

- All employees are expected to follow policies and protocols for communicating with patients with disabilities. Emergency Department (ED) employees are expected to follow department protocols as well.

- ED employees will:
  - Work to reunite patients with disabilities and their companions in the Emergency Department.
  - Engage communication support if necessary
  - Contact Interpreter Services and on-site interpreters as needed

Hazard Communication (HAZCOM)

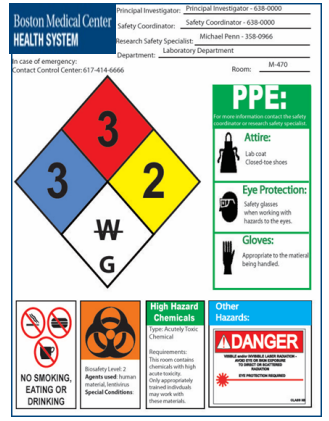
Boston Medical Center
HEALTH SYSTEM

Hazard Communication (HAZCOM) – What is it?

HAZCOM stands for the **Hazard Communication Standard** (29 CFR 1910.1200), an OSHA regulation often called the "Right-to-Know" or "Right-to-Understand" law. It requires that employees be informed about the hazardous chemicals they may be exposed to in the workplace and on the precautions to properly protect themselves.

Hazards associated with chemicals are reduced through the following:

- By reviewing safety policies
- Completing required training
- Knowing where to access Safety Data Sheets (SDS's), reviewing them prior to working with product(s).
- SDS's are located on BMC intranet for the Hospital.
- Observing safety signs and door placards
- Observing chemicals labels and warning signs



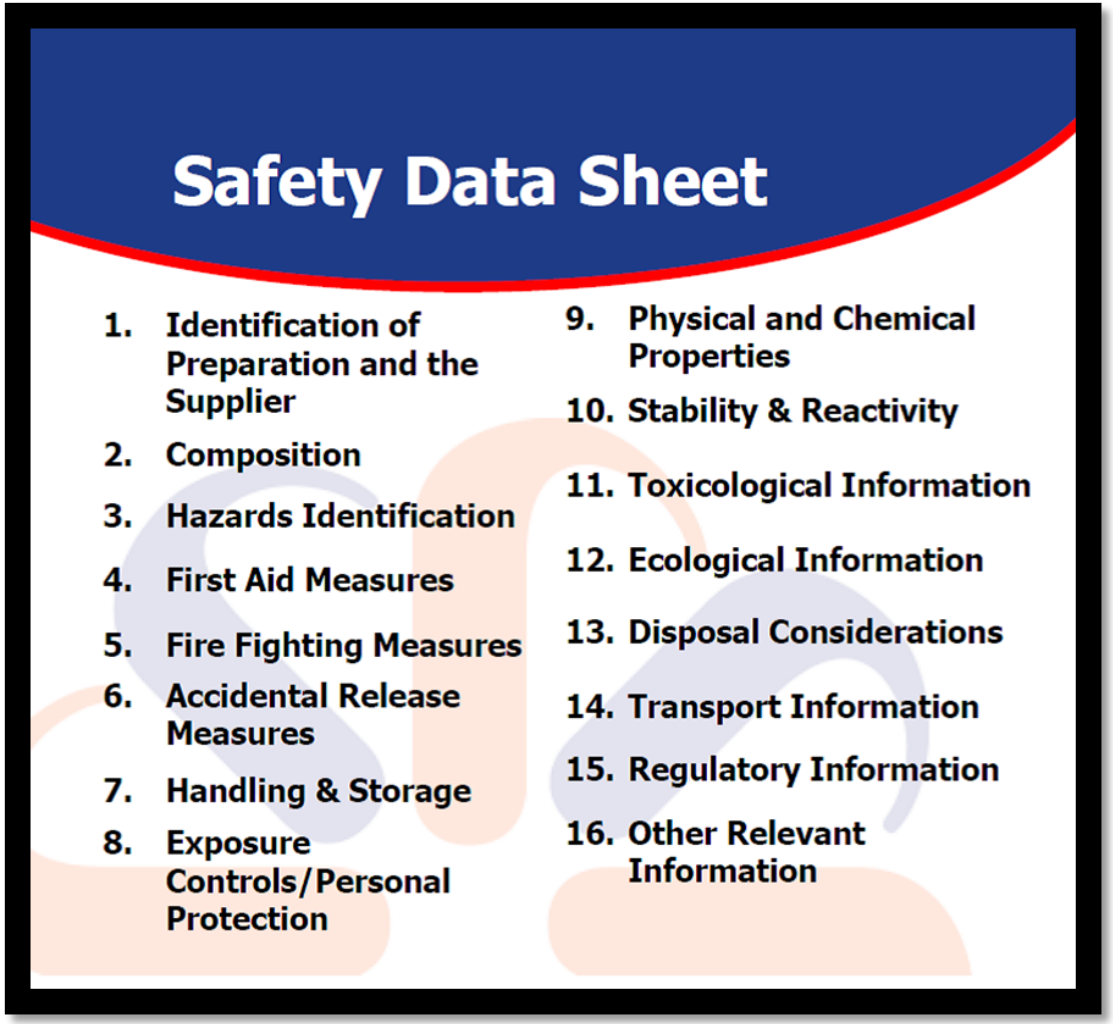




Hazard Communication (HAZCOM) - Safety Data Sheets

As required by OSHA, a Safety Data Sheet or SDS must follow a strict 16-category format. The sections of the SDS are shown here.

- Departments should continually update their SDS binders if one exists with updated SDSs. SDSs are updated periodically by the chemical manufacturer
- Several departments maintain SDSs on the BMC Intranet. Notify Safety Officer of any updates.
- SDSs can also be searched online by the chemical name and manufacturer



Questions? Contact EVS or Facilities

Hazard Communication (HAZCOM) Cont'd

Pictograms are used on product labels and SDS's to illustrate the known *hazards* associated with specific chemicals

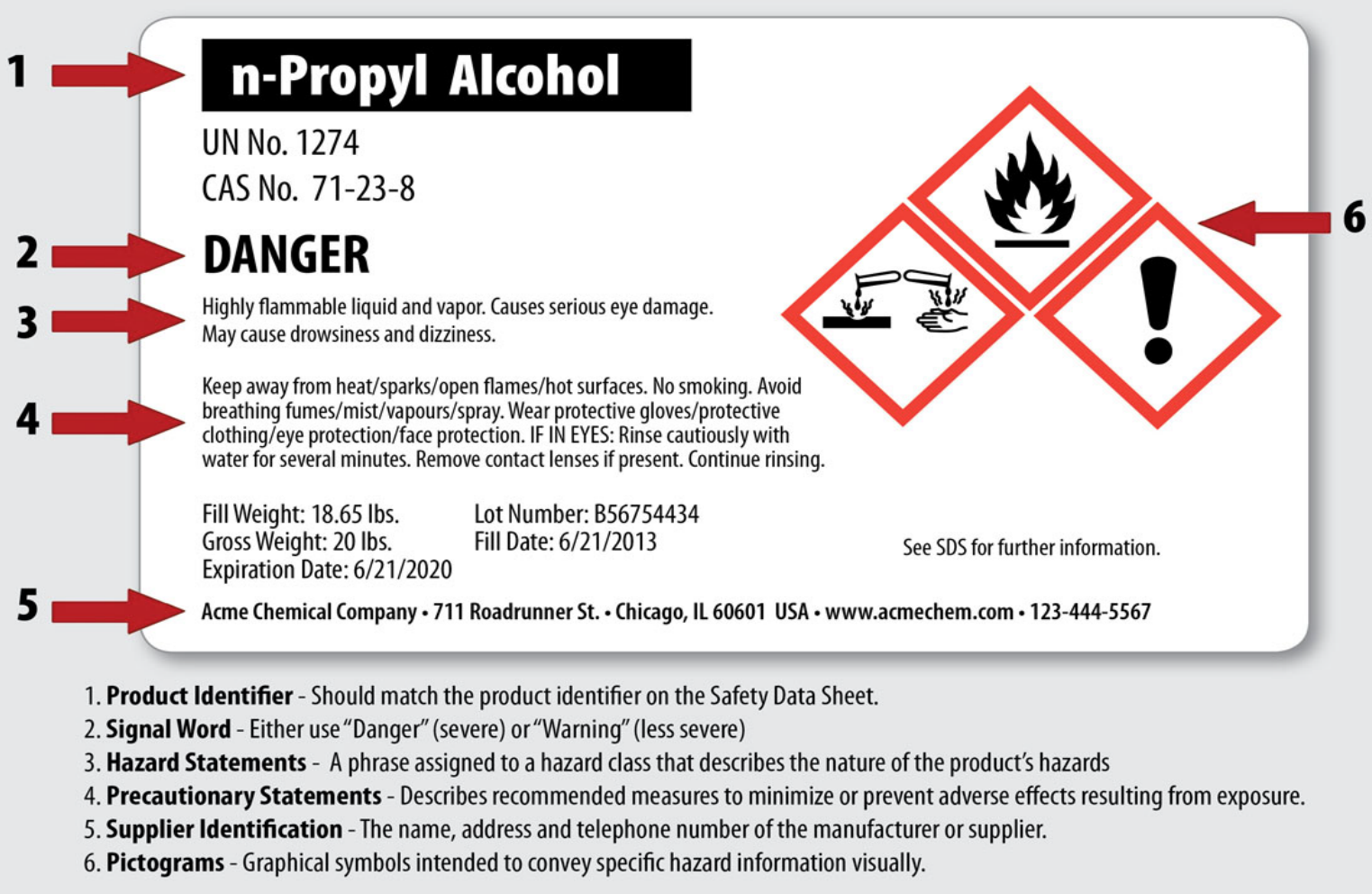
Why pay attention to symbols?

Health Hazard • Carcinogen • Mutagenicity • Reproductive Toxicity • Respiratory Sensitizer • Target Organ Toxicity • Aspiration Toxicity	**Flame** • Flammables • Pyrophorics • Self-Heating • Emits Flammable Gas • Self-Reactives • Organic Peroxides	**Exclamation Mark** • Irritant (skin and eye) • Skin Sensitizer • Acute Toxicity (harmful) • Narcotic Effects • Respiratory Tract Irritant • Hazardous to Ozone Layer (Non-Mand
Gas Cylinder • Gases Under Pressure	**Corrosion** • Skin Corrosion/ Burns • Eye Damage • Corrosive to Metals	**Bomb** • Explosives • Self-Reactives • Organic Peroxides
Flame Over Circle • Oxidizers	**Environment** (Non-Mandatory) • Aquatic Toxicity	**Skull and Crossbones** • Acute Toxicity (fatal or toxic)

This symbol denotes the need for skin and eye protection.

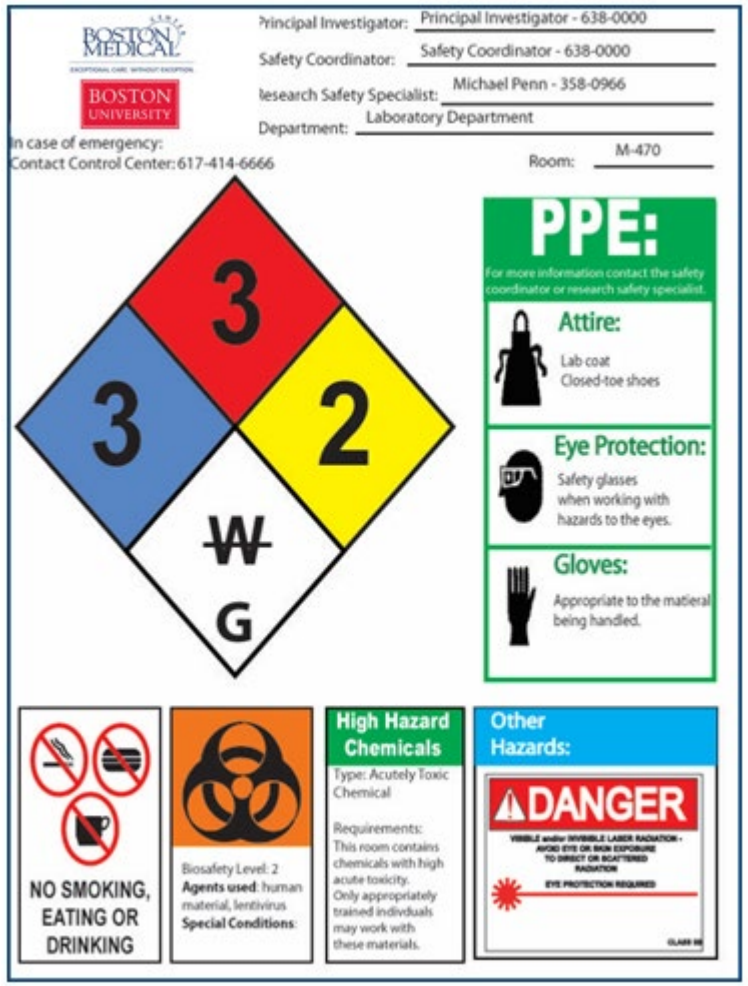
PUTTING IT ALL TOGETHER
Sample Chemical Label - 'standardized'

As required by OSHA chemical labels are standardized.
The figure below illustrates the information on each label.



1. **Product Identifier** - Should match the product identifier on the Safety Data Sheet.
2. **Signal Word** - Either use "Danger" (severe) or "Warning" (less severe)
3. **Hazard Statements** - A phrase assigned to a hazard class that describes the nature of the product's hazards
4. **Precautionary Statements** - Describes recommended measures to minimize or prevent adverse effects resulting from exposure.
5. **Supplier Identification** - The name, address and telephone number of the manufacturer or supplier.
6. **Pictograms** - Graphical symbols intended to convey specific hazard information visually.

HAZARD COMMUNICATION (HAZCOM) CONT'D
NFPA Diamond Door Placard



Door placards are another important component of Hazard Communications. Thes Placards highlight the hazards associated with chemicals in both **Clinical and Research Laboratory** space.

What It All Means



CONSULT SDS FOR FURTHER INSTRUCTIONS

RATING EXPLANATION GUIDE

HEALTH	Recommended Protection	FLAMMABLE	Susceptibility to Burning	INSTABILITY	Susceptibility to Energy Release
4	Special full protective suit and breathing apparatus must be worn.	4	Very flammable.	4	May detonate under normal conditions.
3	Full protective suit and breathing apparatus should be worn.	3	Ignites under normal temperature conditions.	3	May detonate with shock or heat.
2	Breathing apparatus with full face mask should be worn.	2	Ignites with moderate heating.	2	Violent chemical change but does not detonate.
1	Breathing apparatus may be worn.	1	Ignites when preheated.	1	Not stable if heated use precautions.
0	No precautions necessary.	0	Will not ignite.	0	Normally stable.

Personal Protective Equipment (PPE)

Personal Protective Equipment (PPE)

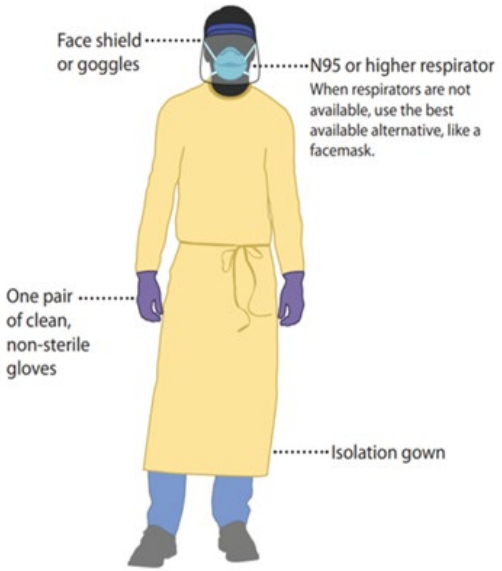
Your job may require the use of **Personal Protective Equipment (PPE)**. Whenever possible, Work with managers to **eliminate hazards** in your work area. If hazards cannot be eliminated, the use of PPE may be necessary. Keep in mind that some types of PPE require specific training, such as learning how to appropriately don and doff or undergo fit testing for N95 respirators

HAZARDOUS DRUG / CHEMO SPILL



Hazardous drug spill kits are available

CLINICAL PRECAUTION



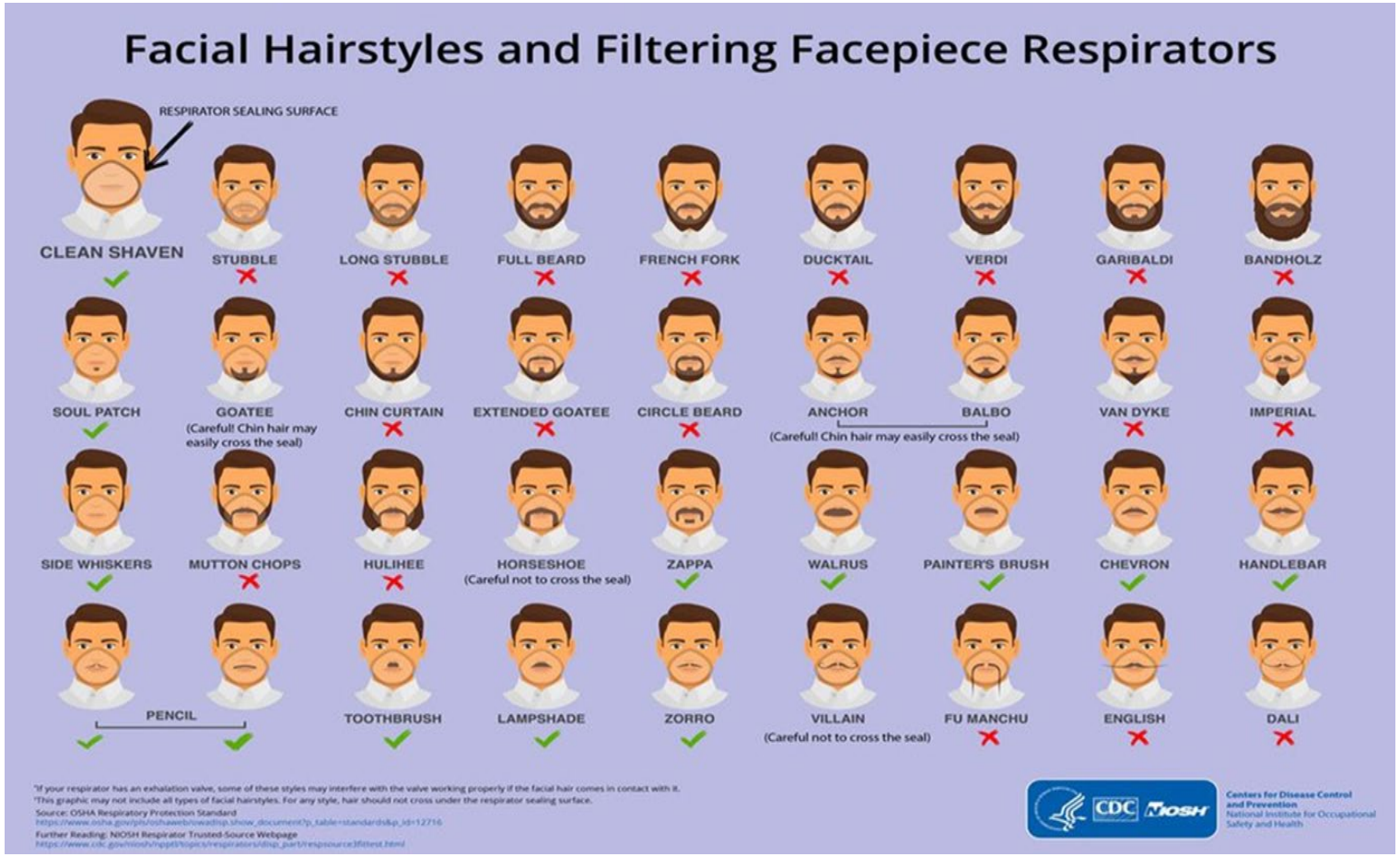
Specific precaution PPE is listed on precaution signage.

WORKPLACE SAFETY



Standard procurations should be worn when handling hazardous material.

Personal Protective Equipment (PPE) - N95 Fit testing requirements



Staff who are required to wear N95's as part of their work must do the following;

- Complete an initial health screening BMC Occupational Health.

In order to wear a N95 you must comply with the CDC facial hair infographic.

BMC Respiratory Protection Options





N95 Mask requirements

- Initial medical clearance and fit test
- Annual fit test
- No facial hair
- Only wear the mask you have been fitted too
- Available in unit supply closets or central distribution request





Powered Air Purifying Respirator (PAPR) Requirements

- Requires initial training
- Annual training required
- If unit is broken mark it with a broken equipment tag, include what specifically is broken.
- The individual who checks out a PAPR from Transport office is also responsible for checking it back in.

Responding to Chemical Spills

In the event of a **Hazardous Chemical Spill**, follow the BMC Hazardous Drug Spill policy on PolicyTech. For all other chemical spills follow guidance below.

For **large spills** or spills beyond your control, **call Public Safety immediately at 617-789-2222 or X2222** and request Environmental Services to assist. Offsite locations, follow site specific procedures for reporting emergencies.

Before attempting to clean up a spill:

- **Contain the spill** only if it can be done safely. Keep others away from spill area.
- **Identify** the chemical or chemicals involved. Pay attention to hazards created by mixed chemicals and those that are incompatible.
- **Call the Public Safety** for EHS assistance if needed.
- **Locate the appropriate Safety Data Sheet or SDS** for clean-up procedures and specific hazards.
- Use appropriate Personal Protective Equipment (PPE) to protect yourself from hazards. You can only use the correct PPE if the chemical is known.
- For unknown spills, or mercury spills regardless of size. Call Public Safety immediately for EHS assistance. Additionally, some spills may be reportable to regulatory authorities.
- **Place** in appropriate waste container including spill material.

Safety Showers and Emergency Eyewashes

Eyewash: a device used to provide flushing fluid water to irrigate and flush the eyes if they have come into contact with hazardous chemicals.

Safety shower: a unit designed to wash an individual's head and body which has come into contact with hazardous chemicals.

Safety eyewash and showers shall be easily identifiable and be unobstructed.

- Carts, chairs, glassware and closed doors can all be considered obstructions, which may slow the response in the event of an emergency



How to Use an Eyewash Station

Begin to Flush
Get your eyes directly in the stream of the flushing fluid- Immediately!

Hold Your Eyes Open with Your Fingers
Once activated, the unit will stay on. Keep your eyes open by holding your eyelids apart with your fingers.

Roll Your Eyes
Gently roll your eyes from left to right and up and down to be sure that the fluid is flushing all of the areas of your eye.

Flush for a Full Fifteen Minutes
Continue Flushing your eyes for a full 15 minutes. This is important because you want to fully dilute the chemical and wash it out of your eyes. Any time less than 15 minutes is NOT enough time to accomplish this.

Take Out Your Contacts
If you have contact lenses in your eyes, you can gently take them out while you are flushing. Don’t delay the flushing to take out your lenses but make sure that you take them out because they could trap the chemical in your eyes.

Seek Medical Help
After you have flushed, see a doctor to determine if anything more needs to be done for the preservation of your vision.



Eyewash Station Maintenance

WEEKLY EYEWASH STATION CHECK

Location (Building, Unit, Room#):_____

Inspection Day: _____ of every week. CALENDER YEAR: _____

	Week 1	Week 2	Week 3	Week 4	Week 5
Month					
January					
February					
March					
April					
May					
June					
July					
August					
September					
October					
November					
December					

WEEKLY FLUSH STEPS

1. Ensure that the eyewash station is easily identifiable and unobstructed.
2. Ensure that the eyewash station activates easily with one-handed control, the flow removes eyepiece covers, and water flows evenly and in a steady stream.
3. Allow the eyewash station to run for 1-3 minutes to flush stagnant water from the line. If this is your first time flushing the station, you may have to run it longer to ensure that the water is clean.
4. If your eyewash station does not have a drain, ensure you use a bucket to capture the water.
5. Complete an online service request for any water flow or unit deficiencies.



Confirm there are no obstructions or barriers to reaching an eyewash. Ex. Code or supply cart(s).

Weekly department/unit flushes are required. See pic of log below (available on the HUB at https://hub.bmc.org/tools-and-resources/administrative-tools-and-resources/joint-commission).

Report malfunctioning (low flow, high flow, water too hot, water too cold) eyewash stations and safety showers to Facilities at 617-789-2178. Questions on how to flush should be directed to Facilities

Hazardous Waste

Boston Medical Center
HEALTH SYSTEM

Waste Disposal Guidelines

Understanding how to dispose of regulated waste is a necessary part of keeping BMC safe and protecting the environment. Training (on-line) is required for chemical and hazardous waste pharmaceutical management.

Regulated Medical Wastes (Biological Waste)



Bloody items, body fluids, tissues, and sharps like syringes. Dispose in redline lined biohazard receptacles. Sharps disposed in sharps containers.

Chemical Waste (Hazardous Waste)



Dispose of expired or spent chemicals such as cleaners, oil, lab chemicals and some medications (Hazardous Waste Pharmaceuticals) in their labeled waste containers and placed in the satellite accumulation area (SAA).

Hazardous Waste Pharmaceuticals (Black Bucket Waste)



Black buckets are typically located in the medication rooms in patient areas. A placard is posted next to each bucket identifying the hazard waste pharmaceuticals requiring this type of disposal. Other unused pharmaceuticals are sent back to the pharmacy.

Hazardous Waste Removal Contacts



CHEMO WASTE BUCKET
Call or email Environmental services (EVS)



BIOLOGICAL WASTE AND SHARPS
Call or email Environmental services (EVS)



HAZARDOUS PHARMACEUTICAL WASTE
Call or email Environmental Health and Safety (EHS)



NARCOTICS WASTE BUCKET
Call or email Environmental services (EVS)



BATTERY RECYCLE BUCKET
Call or email Environmental Health and Safety (EHS)



SATELLITE ACCUMULATION AREA
Call or email Environmental Health and Safety (EHS)

Contact Information:
EVS x3046
PAGER 41087

Maintenance Requests

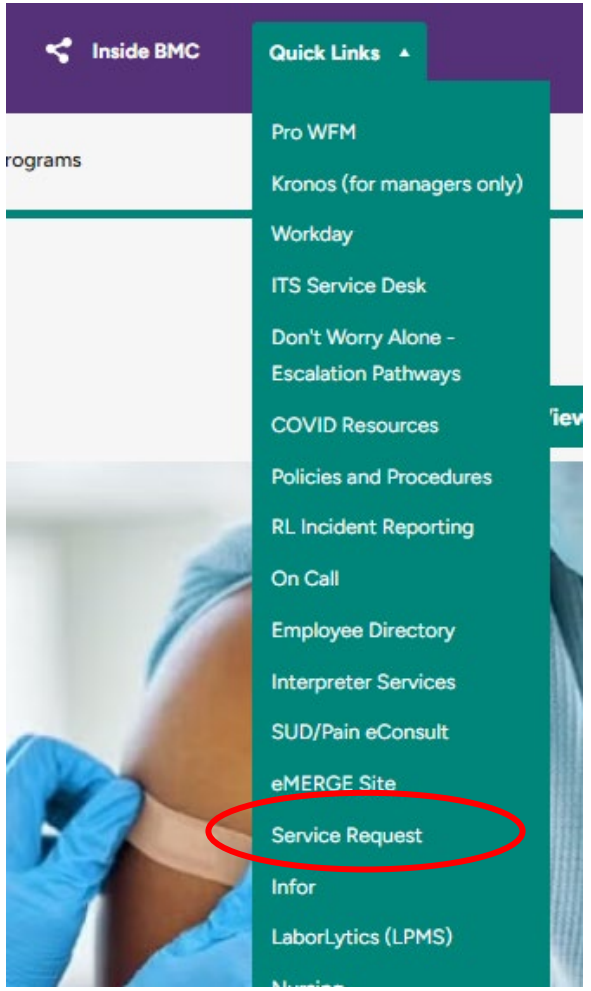
Boston Medical Center
HEALTH SYSTEM

Facilities & Maintenance Requests

Emergency number
617-789-2178
24/7 monitored







Boston Medical Center
HEALTH SYSTEM

Remember to submit a work order request!

<u>NEVER FLUSH</u> Bath-in-a-Bag, Patient/Staff Hygiene, Cleaning, or Any Kind of Wipes Down the Toilet





Over the past year, BMC has experienced a record number of plumbing backups, leading to significant interruptions in patient care and extensive damage to our facility. The affected areas include, but are not limited to, operating rooms on multiple occasions, inpatient floors and rooms, and outpatient clinics. Each of these incidents could have been avoided. **Every event was caused by a staff member, patient, or visitor flushing body/hygiene wipes or cleaning wipes down the toilet.**

Medical Equipment Maintenance

Medical Equipment Maintenance

Boston Medical Center Brighton
Clinical Engineering Department Request for Service Details
(created by Robert McNulty, Updated 2025-08-21)

Boston Medical Center Brighton Clinical Engineering is available 24/7/365.
Please note the following information for the Clinical Engineering contact details based on your need and day/time of need.

Boston Medical Center Brighton Clinical Engineering does not have an e-mail or an online ticketing process at this time. You need to contact Clinical Engineering via calling the office or contacting the page operator.

Boston Medical Center Brighton Clinical Engineering can be contacted by calling 617-789-2479 or internally by calling extension 2479. If no one is in the office the voice mail message will pick up after 8 rings so, please wait for the voice mail.

For defective equipment needing service, please remove the equipment from service, clean the equipment, tag it with a Do Not Use tag including a brief description of the issue, place it in the Clean Utility/Equipment room and call Clinical Engineerinng to report the issue as well as to pick up.

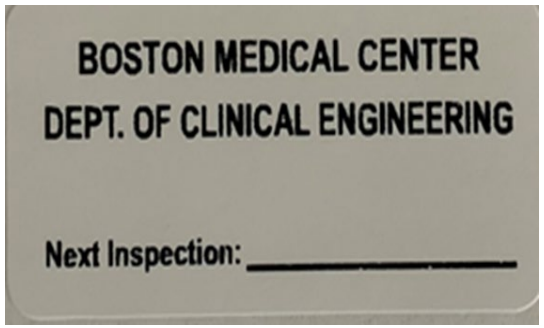
Boston Medical Center Clinical Engineering

Normal Hours of Operation, Monday – Friday 7:30am to 4:00pm
Call 617-789-2479 or extension 2479, Please leave a message if no one is available to answer.

For Equipment needs such as Infusion Pumps, Feeding Pumps, SCD's, please page our Clinical Equipment Tech from any internal phone by dialing 85, wait for the message and enter ID 41130 # and your call back extension.

For Urgent Issues Afterhours, Weekends, Holidays call the Page operator to contact the On-Call Clinical Engineering Staff 617-789-3000, Request Clinical Engineering On-Call





Your Role and Responsibility

- Remove defective equipment from service
- Identify broken equipment with the Broken Equipment Tag shown on right (or a note with like information in lieu of the tag)
- Inform others in the area not to use the broken equipment
- Contact Clinical Engineering to repair the equipment or Patient Transport to have the equipment brought to Clinical Engineering
- If an incident occurs with a device that harms (or could have harmed) a patient, file an RL Report
- Check dates on devices with a white inspection sticker (example at right) before use and notify Clinical Engineering if the date on the sticker has passed

Fire & Life Safety

BMC Fire Response Plan – R.A.C.E – Available on Red Card



R

Rescue

- Ensure immediate safety of patients and staff. If required remove yourself and person(s) from the fire scene/room.

A

Alert

- At BMC South activate the fire alarm pull station, Call x666 to provide detailed information and then 911.
- **Offsite locations** Activate the fire alarm pull station, Call 911 to provide detailed information.

C

Confine

- Prevent fire from spreading by closing all doors and windows to contain the fire. Ensure fire barrier doors are closed.

E

Extinguish/Evacuate

- Use extinguisher to put out a small fire if safe to do so or to escape a large fire. Follow department specific evac plan or building fire response plan and report to designated rally point.
- Do NOT use elevators.
- Those needing special assistance should be evacuated to nearest stairwell and notify emergency responders.

Fire Pull Stations

Familiarize yourself with the locations of the pull stations on your floor.



To do:

Find all the pull stations in your area

You will need to pull these if there is a fire



Pull stations can always be found within 5 feet of an exit stairwell

Fire Speaker and Strobe

Know where the fire speakers and strobes are on your floor







When activated, you will hear the alarm and see the strobe light flashing.
Listen carefully and follow instructions. Be alert.

Fire Speaker and Strobes

What does the “floor tone” mean?

What is the “floor tone”:

- A group of 3 short tones that keep repeating
- Follows the verbal instructions (repeated 3 times).
- Will give you an idea as to where the fire may be

Keep in mind other areas will not hear the floor tone, but will still see the strobe lights

Who will hear the “floor tone”

The floor of the fire or alarm pull

AND

The floor above the fire

AND

The floor below the fire

If There Is Visible Smoke Or Fire

What to do…



If you see smoke or fire – Pull the alarm, Follow R.A.C.E

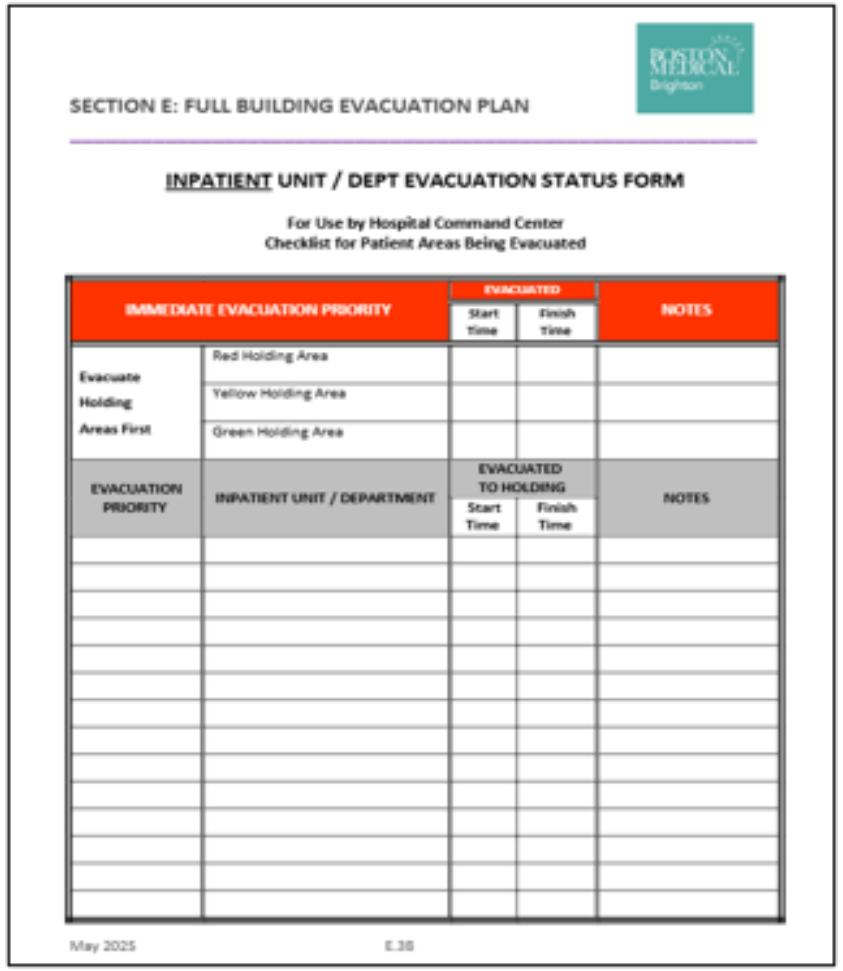
If you hear the fire alarm and the alarm is **NOT FOLLOWED** by the “floor tone”

- ✓ Shelter in Place, listen for additional information.

If you hear the floor tone **AFTER** the announcement;

- ✓ For in-patient spaces follow your unit specific evacuation plan located on the HUB. All others follow your department or building specific response plans.
- ✓ Contact Public Safety 617-789-2222 or X2222 to report and request assistance with a mobility impaired patients/visitors including location ex. staircase and floor.
- ✓ Wait by the staircase with patient. The fire department will come to you.

BMC Unit Specific Fire Response Plan



SECTION E: FULL BUILDING EVACUATION PLAN

INPATIENT UNIT / DEPT EVACUATION STATUS FORM

For Use by Hospital Command Center
Checklist for Patient Areas Being Evacuated

IMMEDIATE EVACUATION PRIORITY		EVACUATED Start Time	EVACUATED Finish Time	NOTES
Evacuate Holding Areas First	Red Holding Area			
	Yellow Holding Area			
	Green Holding Area			

EVACUATION PRIORITY	INPATIENT UNIT / DEPARTMENT	EVACUATED TO HOLDING Start Time	EVACUATED TO HOLDING Finish Time	NOTES

May 2025 E.38

EVACUATION

The movement of patients, staff, and visitors from an area when the environment cannot support clinical operations

- All personnel will remain available for reassignment and may be asked to perform functions outside of normal responsibilities
- Evacuation operations will depend on the location and evacuation type

BMCHS executes two types of evacuation: *Emergent and Controlled*

- **Emergent Evacuation – Immediate risk to life safety for patients and staff**
  - *In-patient areas will proceed horizontally through a smoke barrier to an adjacent safety zone*
  - *Ambulatory areas will begin a vertical evacuation (exit via stairs or safest route)*
- **Controlled Evacuation - Planned urgent or non-urgent movement of patients and staff**
  - *Authority to order a controlled evacuation of an in-patient area is subject to incident type and on-scene resources*

Fire Safety: The Use of Fire Extinguishers

Before using a fire extinguisher, always activate the fire alarm. Use if the fire is small (no bigger than waste basket size) and safe to do so. Or to create a safe egress pathway. Know where they are located and how to use them always within 75' of you. The three (3) main classes of fire are A, B, and C as described in the graphic below. Additional fire response and extinguisher training is available by Public Safety.

What will my ABC extinguisher put out:

A	Paper, Wood, Plastics, Fabric, Rubber, Trash	
B	Gasoline, Oil, Grease, Some Paints and Solvents	
C	Energized Electrical Equipment, Appliances, Computers, Circuit Breakers, Wiring	



General Fire Safety Facts And Requirements

- ❑ Maintain 18” from fire sprinkler heads to the top of storage to allow the system to function properly in the event of a fire. Items stacked underneath will delay its activation and impede water pattern.
- ❑ Report missing or damaged ceiling via work order system. Missing tiles may allow heat to rise past the sprinkler head or smoke detectors delaying the fire alarm and sprinkler systems.
- ❑ Report doors not closing, blocked, or propped open. Doors help contain smoke and fire during emergencies.
- ❑ Some doors are delayed-opening. Once the panic hardware is activated, the door will open after a 15-seconds. These doors are identified with large, red signs. During a building fire alarm activation, there is no 15-second delay.
- ❑ No taping door latches in the open position.
- ❑ Do not store equipment or beds in front of pull stations, extinguishers of between smoke barrier doors.



Fire Safety – Holiday Decorations Policy

Strict observation of these rules is required Facilities and Safety personnel will remove any unsafe decorations.

- Decorations and artificial trees can only be used in open areas and are prohibited in elevator lobbies, stairways, confined areas, and any locations that obstruct exits or the visibility of exits.
- No combustible or flammable decorations are allowed.
- Only UL approved lights may be used for lighting.
- If strings or strands of lights are to be used, no more than 3 strands are allowed.
- Lighting is prohibited on metallic aluminum artificial trees.
- Extension cords are prohibited.
- No natural evergreen trees, wreaths, boughs, laurel rope, etc. may be used.
- All decorations must be non-combustible or flame-resistant.
- Do not place or hang decorations from sprinkler heads, door frames, exit signs or other fire safety equipment. Do not place or hang decorations, signs, etc. on doors that are identified as an EXIT or anywhere that may obstruct the view of exit signs, fire extinguishers, fire alarm pull stations, or wayfinding signs.
- Do not place or hang decorations that may obstruct free passage through corridors, hallways, or exits. Do not hang decorations on handrails.



Life Safety

Boston Medical Center
HEALTH SYSTEM

Oxygen E-Cylinder Storage

The Joint Commission expects organizations to physically segregate FULL & EMPTY cylinders.

Full cylinders should be place in the full/unopened rack.

Partial and empty cylinders should be place in the partial/opened/empty rack.

Cylinders should never be free standing and secured at all times.

Empty cylinders need to have their valves closed and protection caps in place.

Clear labelling to differentiate between full and empty cylinders is required.

Compressed gas cylinders (empty of full) must not be stored in corridors, stairways, or any ro

Cylinders should be kept away from sources of ignition, combustibles, and heat sources such hot piping. Excessive pressure due to heat may cause cylinders to burst.



Oxygen Tank Usage

Oxygen Tank Ready for Use



"FULL" or GREATER or Equal to 200 Liters





Blue ring = Full Tank

Oxygen Tank Empty



"EMPTY" or LESS than 200 liters





NO Blue Ring = Empty Tank

Egress Corridors

WHAT IS ALLOWED IN THE EGRESS CORRIDORS?

The simple answer is nothing BUT there are some exceptions:

Emergency medical equipment not in use (i.e. Code Carts and patient lift and transport equipment)

Medical Equipment and carts “in use”

IMPORTANT NOTE: All of which must be relocated out of the patient corridors upon fire alarm activation.

WHAT DOES “IN USE” MEAN?

“In use” means that an item is not idle in one location for more than 30 minutes and the user is nearby on the unit.



BLOCKING OF LIFE SAFETY SYSTEMS

- Blocking of **pull stations, fire extinguishers, exit doors, corridor doors, electrical panels/closets and med gas valve boxes** is **PROHIBITED** at all times.









Do Not Prop ANY Doors



Electrical Safety & Utility Related Emergencies

Space Heater Policy – Prior To Use all space heaters need to be approved by facilities.

Portable space heaters are a potential source of fire if not used properly. The requirements listed below, applicable code requirements, and manufacturer's recommendations must be followed to maintain a safe environment.

If a space cannot be adequately heated via the installed building heating system, do the following:

Contact Facilities Operations, you may use the online Facilities Service Request system or call 617-789-2178 to report the condition.

If the installed system cannot be repaired in a timely manner, Facilities MAY recommend a temporary space heater meeting **ALL** requirements listed below.

1. All heaters must be Underwriters Listed (UL) or Factory Mutual approved for their intended use.
2. Heaters must have a thermostat to automatically shut down the unit when the desired temperature is achieved.
3. Heaters must be mineral oil filled and have a tip over automatic shutdown feature.
4. Heaters must be kept at least 3 feet (36 inches) from all combustible materials e.g. file cabinets, desks, trash cans, paper boxes, etc.

Space Heater Policy – Prior To Use all space heaters need to be approved by facilities.

Portable space heaters are a potential source of fire if not used properly. The requirements listed below, applicable code requirements, and manufacturer's recommendations must be followed to maintain a safe environment.

If a space cannot be adequately heated via the installed building heating system, do the following:

Contact Facilities Operations, you may use the online Facilities Service Request system or call 617-789-2178 to report the condition.

If the installed system cannot be repaired in a timely manner, Facilities MAY recommend a temporary space heater meeting **ALL** requirements listed below.

1. All heaters must be Underwriters Listed (UL) or Factory Mutual approved for their intended use.
2. Heaters must have a thermostat to automatically shut down the unit when the desired temperature is achieved.
3. Heaters must be mineral oil filled and have a tip over automatic shutdown feature.
4. Heaters must be kept at least 3 feet (36 inches) from all combustible materials e.g. file cabinets, desks, trash cans, paper boxes, etc.

Fire Hazard – Space Heater

Examples of fires caused by a Space Heater

In 2022 a space heater ignited a fire and subsequent evacuation of a BMC office building.

Pictures are examples of what can happen when space heaters malfunction or are left unattended.

Stay safe! call facilities with temperature concerns.











Space Heater Policy – Prior To Use all space heaters need to be approved by facilities.

Only oil filled radiators and with facilities permission are authorized on BMC property.









Open coil or fan space heaters are forbidden on BMC property. Never plug a heater into a power strip.





Space Heater Safety Requirements

If facilities has authorized the use of a portable space heater, ensure you follow these safety tips:

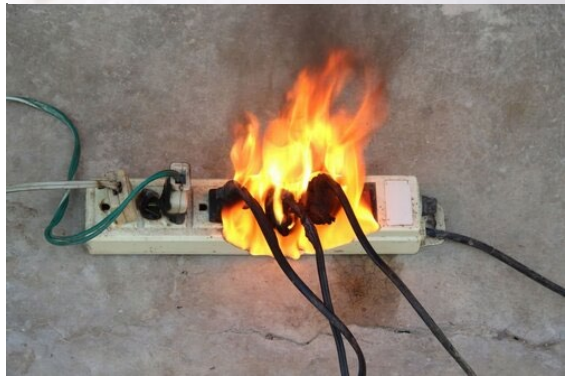
- Do not place heaters under desks or other enclosed areas.
- Heaters must be monitored when in operation.
- Plug heater directly into a wall receptacle. Never plug it into an extension cord.
- Heaters need to be monitored daily. Those heaters missing guards, control knobs, feet, etc. must be taken out of service immediately and repaired by a competent person.
- Do not use heaters in rooms that will not be continually occupied.
- Keep doors and windows closed, including storm windows. This will help prevent freeze-ups.
- Keep space heaters away from exit ways, walkways and paths of travel.
- Do not use space heaters in wet areas like bathrooms or kitchens.
- Do not use portable space heaters if small children are expected in the area.
- No open-coil space heaters are permitted in any university buildings.
- Space heaters of any type are prohibited in laboratories.

Electrical Safety

Observe the following safety procedures when using electrical devices:

- Electrical devices must be properly grounded: 3-prong or double insulated. All devices inpatient areas must have an in-house inspection sticker. These electrical devices have either been checked by Clinical Engineering or Facilities.
- Check for electrical defects including frayed wires or damaged plugs (missing grounding or third prong)
- Do not use extension cords or power strips in patient areas. In non-patient areas these are highly discouraged. It's preferred that you work with facilities for an alternate solution. Never over-load electrical outlets by plugging in too much or incorrect equipment.
- Always review and follow manufacturers requirements before plugging in equipment.





Electrical Safety

No unauthorized or used electric appliances should be used on BMC South property.

- All electric appliances must be purchased through BMC South.
- All appliances must be inspected by BMC prior to use.
- Examples include, but not limited to;
  - Toaster ovens
- Do not bring appliances in that were purchased second hand or bring them in from home.

Example: Electric Tea Kettle



"Electrical faults are a common cause of electric kettles burning. These faults can include frayed wires, damaged plugs, or faulty switches. Electrical faults can cause the kettle to short circuit, which can lead to overheating or burning."

Daisy-Chaining Power Strips





Only equipment on the IV pole can be plugged into power strip. No daisy chaining!

Utility Loss

In the event of a utility loss, call the Control Center immediately. At off-site locations, report losses to supervisor and follow site specific emergency procedures. Utilities at BMC Brighton include:

- Elevators
- Heating, Ventilation and Air Conditioning (HVAC) equipment
- Plumbing
- Water
- Medical gases



Connect critical medical devices and equipment in **red electrical outlets.** Red outlets remain powered in the event of a local power outage.

Radiation Safety

Radiation Safety

- BMC is committed to limiting radiation exposures of staff, patients, and visitors to levels that are **A**s **L**ow **A**s **R**easonably **A**chievable as required by the Nuclear Regulatory Commission and Massachusetts Department of Public Health Radiation Control Program
- **Anyone working directly with radioisotopes and radiation generating devices (including LASERS) must complete radiation safety training and may be required to wear a monitoring device.**
- BMC personnel who do not work in areas where radiation is used should stay out of those areas. Anyone who works where radiation is used, but doesn't work directly with it, should be aware of the posted area and should not spend unnecessary time in those areas.

Use the following procedures to **protect yourself from radiation**:

- Observe postings
- Do not go into a posted area if there is no need
- Do not touch anything marked 'radioactive'
- Do not put radioactive waste into regular trash



Magnetic Resonance Imaging (MRI) Safety

How strong is the magnetic field of a MRI unit?

Either 30,000 or 60,000 times of the strength of Earth's magnetic field. The magnet is on 24/7.

What hazards can MRI create?

Mainly two kinds:

- Projectile effect and tissue damage. Ferromagnetic or metal objects can get pulled into the MRI scanner at very high speed which can cause severe or fatal injuries (*projectile effect*).
- Metal implants or devices can be dislodged or heated and cause tissue tear or burn (*tissue damage*).





What can you do to avoid these hazards?

1. **Do not** enter MRI area without the supervision of a MRI technologist. Observe all MRI warning signs
2. **Listen** to MRI technologists inside MRI area. They are there to help protect you from hazards.
3. **Do not** bring any ferromagnetic or metal objects into the MRI area. If you are not sure, do not guess! Ask the technologist!
4. **Notify** MRI technologist if your patient or yourself has metal implants, pacemakers, aneurysm clips, insulin pumps, stimulators, bullets, shrapnel, or tattoos.

Employee Injuries

Employee Injuries – What to do if injured on the job

Non- Emergency Work Related Injury

Employees who sustain an incident, injury, or occupational illness while at work should report injury or illness to the BMCHS Occupational Health Clinic by following these guidelines:

- ❑ Inform your manager or supervisor of your injury.
- ❑ You or you manager should report event in the RL system on the HUB.
- ❑ Contact Employee Health to be evaluated.
- ❑ Call the BMC Workers Compensation insurance administrator, Sedgewick, at **844-295-8266** to file a claim.

To be evaluated outside of Employee Health clinic hours staff should present to the ED and follow up with Employee Health the following day

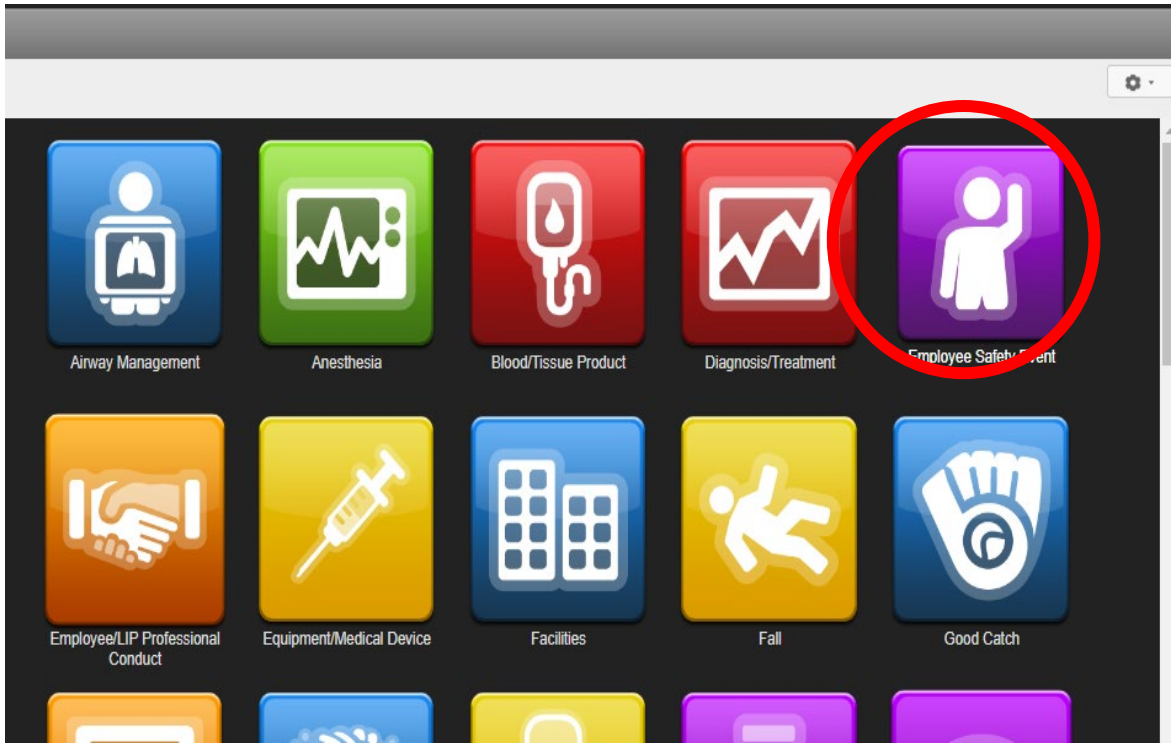
Employee Injuries – What to do if injured on the job

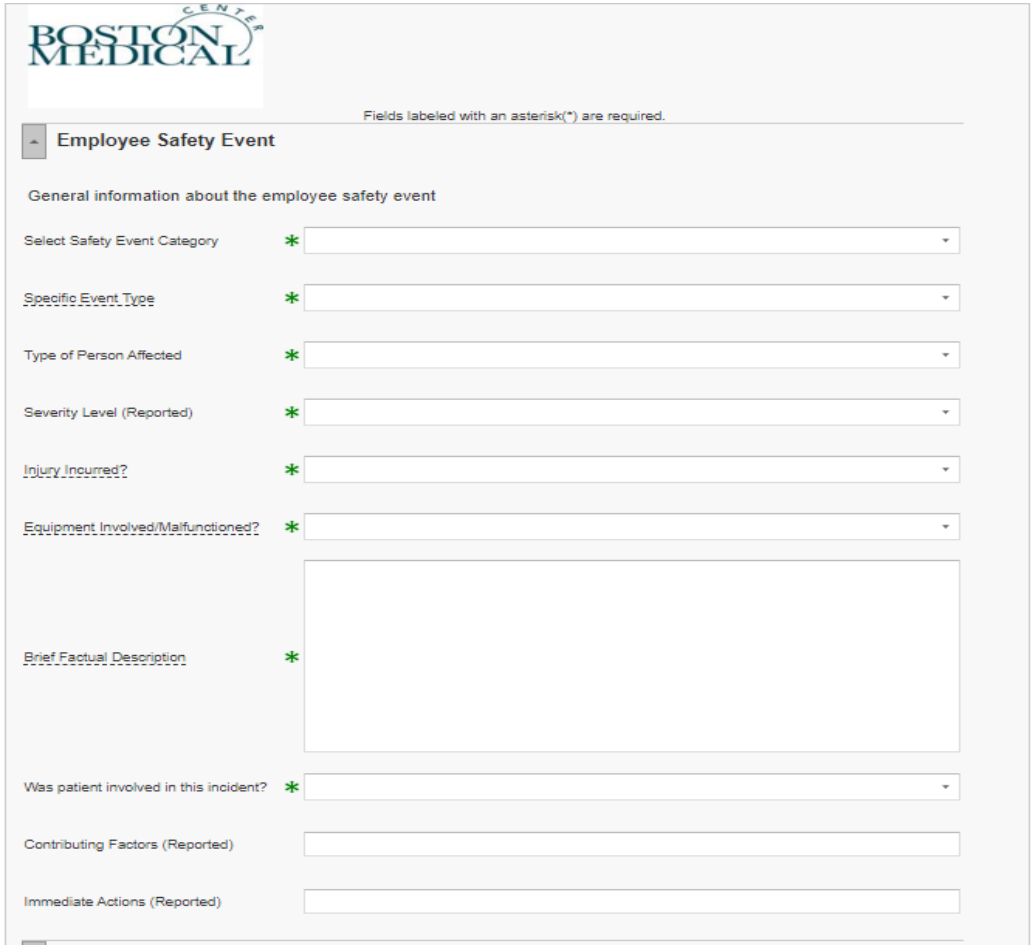
Emergency or Outside Of Normal Business Hours Work Related Injury

- Employees who sustain an incident, injury, or any occupational illness while at work should seek immediate help with their injury.
  - If able report to the BMC ED, otherwise contact 911 for emergency assistance.
  - Inform the ED that this is a work-related injury.
- **When able to:**
  - Inform your manager or supervisor of your injury.
  - You or your manager shall complete an RL incident report on the HUB.
  - Report injury to Occupational Health Clinic.
  - Contact the BMC Workers Compensation TPA, Sedgewick at **844-295-8266** to file a claim.

Employee Injuries, Accidents and Near Miss events

How to report events at BMC? Use RL on the HUB to report any injuries, accidents, or near miss events.





Thank you for your time.

Boston Medical Center
HEALTH SYSTEM

AI is not a replacement for human intelligence.

AI shall not be used to make clinical decisions or benefit and eligibility determinations.

DO	DON'T
Prioritize Privacy & Security ✓ Do protect patient and member data at all times ✓ Do follow Privacy & Security Policies and Procedures available on Policy Tech ✓ Do use encrypted and secure AI systems ✓ Do contact Compliance if you have questions about BMCHS Privacy and Security Policies	**Don't Share Sensitive Data** ○ Don't enter any protected health information (PHI) or personally identifiable information (PII) into non-secure or non-approved AI systems ○ Don't research with BMCHS data using external and unapproved tools ○ Don't use BMCHS proprietary data in any commercial AI application
Understand Artificial Intelligence Limitations ✓ Do understand that AI is a tool to assist and not replace clinical judgement ✓ Do cross-verify AI suggestions with clinical guidelines and professional judgement	**Don't Over-rely on Artificial Intelligence** ○ Don't use AI as a sole decision-making tool for patient or member care ○ Don't use unverified or suspicious adverse outputs generated by AI
Use Artificial Intelligence Ethically ✓ Do inform patients and members if AI has been used to process their data ✓ Do be transparent about AI capabilities and limitations ✓ Do apply your clinical expertise and consider patient/member specific factors ✓ Do notify Compliance if you notice unfair patterns in AI decisions	**Don't Ignore Bias** ○ Don't assume AI is always fair – Bias can exist even in well-intentioned models ○ Don't disregard patient or member specific context – AI may not fully account for individual histories, preferences, or unique conditions
Stay Educated ✓ Do check with your supervisor if an AI tool is vetted by the responsible AI committee and approved by BMCHS ✓ Do complete required Artificial Intelligence trainings ✓ Do ensure you are aware of AI outputs including confidence levels and error margins ✓ Do ensure you are aware of the types of data at BMCHS and what is and IS NOT permitted to be used in AI tools	**Don't Use Unauthorized Artificial Intelligence Tools** ○ Don't use general consumer AI tools, including personal free or pay accounts or browser extensions, such as ChatGPT on work devices or for work purposes (as these tools can continue to run in the background and capture information) ○ Don't assume all AI tools are alike or that everyone is authorized to have access
Report Concerns & Ensure Effective Resolution ✓ Do document and escalate concerns about errors or issues ✓ Do work with IT teams, RAI governance committee, and report to compliance inaccuracies or malfunctions	**Don't Skip Testing and Validation** ○ Don't assume the fairness and accuracy without testing and validating output - Different models have varying levels of accuracy, fairness, and reliability ○ Don't rely on a single validation technique

Boston Medical Center
HEALTH SYSTEM

Policy #:	40.01.024
Issued:	4/2025
Reviewed/ Revised:	
Section:	ITS, Corporate Compliance

Appropriate Use of Technology

Purpose & Scope:

The purpose of this policy is to establish guidelines for the appropriate use of technology within Boston Medical Center Health System (BMCHS). This policy outlines the responsibilities of staff and defines acceptable use of technology resources to ensure security, confidentiality, and ethical conduct.

Policy Statement:

Access to BMC networks, information systems and/or electronic confidential information is restricted to properly authorized users for acceptable use as set forth in this Policy. All users are expected to act responsibly and maintain the confidentiality, integrity and availability of all BMC information systems and related resources. Users, application owners, and network systems administrators must guard against abuses that disrupt or threaten the viability of any company information systems.

The Information Security department should be notified promptly about known or suspected violation of BMC Security policies or other IS polices, as well as actual information security breaches, or any other potential flaws in the security of the information systems. Under no circumstances is a user authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing BMC information systems, BMC networks, or other BMC IS resources.

Applications

This policy applies to all employees, contractors, volunteers, and any other individuals granted access to BMCHS's technology resources including the workforce members of the BMCHS hospitals, Clearway Health, Boston University Medical Group (BUMG), Inc. and members of the BMC Medical Dental Staff. This policy is not applicable to Wellsense Employees.

Exceptions:

None

Procedure:

Acceptable Use:

1. Technology resources provided by BMCHS, including but not limited to computers, networks, email, and software applications, are to be used for business purposes only.
2. Personal use of technology resources is permitted within reasonable limits, provided it does not interfere with work responsibilities or violate any other policies.
3. All use of technology resources must comply with applicable laws and regulations, including those related to patient privacy and data security.

Security:

1. Users are responsible for safeguarding their login credentials and preventing unauthorized access to technology resources.

2. Users must adhere to security protocols, including regular password changes and the use of encryption when transmitting sensitive information.
3. Users should report any suspected security breaches or vulnerabilities to the IT department immediately.
4. Users should not attempt to modify, physically move, or remove computer equipment, software, or peripherals without proper authorization from the applicable IS department.

Confidentiality:

1. Users must respect the confidentiality of patient information and refrain from disclosing any protected health information (PHI) unless authorized to do so.
2. PHI should only be accessed on a need-to-know basis, and users should ensure that screens are not visible to unauthorized individuals when accessing sensitive information.
3. Any unauthorized access or disclosure of PHI is strictly prohibited and may result in disciplinary action, including termination and legal consequences.

Data Management:

1. Users are responsible for ensuring the accuracy and integrity of data entered into technology systems.
2. Data should be stored securely and backed up regularly to prevent loss or corruption.
3. Users should follow established protocols for data retention and disposal, in compliance with relevant laws and regulations.

Professional Conduct:

1. Users should conduct themselves professionally in all electronic communications, including email, messaging, and social media.
2. Offensive, harassing, or inappropriate content is prohibited and may result in disciplinary action.
3. Users should refrain from engaging in activities that could damage the reputation of BMC or compromise patient care.

Enforcement:

1. Users will cooperate fully with the IS staff and the Information Security Officer in their operation of information systems as well as in the investigation of misuse or abuse.
2. Violation of this policy may result in disciplinary action, up to and including termination of employment or legal action, depending on the severity of the offense and any applicable laws or regulations.

Responsibility:

The BMCHS ITS Department is responsible for the safety and security of data on its network and the equipment used to run the network infrastructure. This policy applies to all individuals that are responsible for the installation of new information resources, the operations of existing Information Technology resources, and individuals charged with Information Technology resource Security at BMCHS and its subsidiaries.

Acknowledgement:

By using BMCHS's technology resources, users acknowledge that they have read, understood, and agree to comply with this policy.

Other Related Policies/Protocols/Guidelines:

38.02.001 Privacy and Confidentiality on Social Media
40.01.012 Information Security and Privacy Agreement

38.01.003 HIPAA Minimum Necessary Standard

Initiated by:
Chief Information Officer

Contributing Departments:
ITS, Corporate Compliance

Date	Version	Author	Change Description	Change
11/19/2024	1	Cyber Security Policy & Documentation Specialist	Draft document with generic information	Created

Boston Medical Center

CODE OF CONDUCT



BOSTON MEDICAL CENTER

BMC's CORE PURPOSE, VISION AND VALUES 2

CARING FOR OUR PATIENTS WITH INTEGRITY

- Quality Care 3
- Patient Safety 3
- Patient Rights 4
- Non-Discrimination 4
- Advocating for our Patients and their Families and Caregivers 5
- Protecting Patient Privacy 6
- Financial Assistance for Patients 7
- EMTALA (The Emergency Medical Treatment and Active Labor Act) 8

INTEGRITY IN OUR WORKPLACE

- Equal Employment Opportunity for All Employees 9
- Professional Conduct 9
- Safe and Secure Workplace 10
- BMC is a Green Workplace 10
- Credentialing and Licensing 10
- No Retaliation 11
- Conflicts of Interest 11
- Substance Abuse or Impairment at Work 12
- Excluded Providers 12
- Political Contributions and BMC's Not-for-Profit Status 12
- Use of BMC Assets 13
- Confidential Business Information 13
- Cybersecurity 14
- Intellectual Property 14
- Advertising and Marketing 14
- Media Relations and Communications 15

MAINTAINING INTEGRITY IN VENDOR RELATIONSHIPS

- Vendor Relationships 16
- Vendors on Campus 16
- Relationships with Referral Sources 17

WORKING WITH INTEGRITY WITH GOVERNMENT

- Compliance with Federal and State Laws 18
- Documentation, Coding and Billing 18
- False Claims Acts and the Deficit Reduction Act 19
- Cost Reports 19
- Record Retention 20
- Responding to Government Inquiries 20
- Accreditation Efforts and Surveys 20
- Research 21
- Protecting the Marketplace 21

THE BMC COMPLIANCE AND PRIVACY/SECURITY PROGRAMS PROMOTE INTEGRITY

- The BMC Compliance Program 22
- The BMC Privacy and Security Programs 22
- Duty to Comply, Report and Cooperate 23
- The BMC Compliance Hotline 23
- Special Role of Managers and Supervisors 23
- Discipline Imposed Fairly and Firmly 24

RESOURCES 25

Si quiere leer el Código de Conducta en español, por favor vaya a la página web del Departamento de Cumplimiento bajo la pestaña "Departments" (Departamentos) en el sitio de Intranet de BMC y haga clic en Código de Conducta, o envíe un correo electrónico a compliancehelp@bmc.org para solicitar una copia impresa.

Si ou vle li Kòd Konduit la nan lang Kreyòl Ayisyen, tanpri ale nan paj sitwèb Depatman Konfòmite a anba onglè "Departments" sou sit Entranèt BMC epi klike sou Kòd Konduit la oswa voye yon imèl ba compliancehelp@bmc.org pou mande yon kopi enprime.

Para ler o Código de Conduta em português, acesse a página da web do Departamento de Conformidade (Compliance Department), na guia "Departments" (Departamentos) do site da Intranet do BMC e clique em Code of Conduct (Código de Conduta) ou envie um e-mail para compliancehelp@bmc.org para solicitar uma cópia impressa.



Dear Colleagues,

The Compliance Department is here to provide support to each of you in making decisions that affirm our commitment to equitable patient care, our workforce, and the broader community and healthcare system. In addition to doing a range of functions including conducting investigations alleging fraud, waste, abuse and HIPAA violations, one of the most important things that Compliance does is provide guidance and assistance with complex questions you may encounter during your job at Boston Medical Center.

Do you have questions about accepting gifts from vendors, attending conferences sponsored by pharmaceutical companies, serving on external healthcare institution boards, collaborating with non-BMC researchers, billing, or sharing patient information with their family members? The Compliance Department is there to help you manage these situations and address related questions or concerns.

BMC's Code of Conduct places a strong emphasis on integrity, which is the foundation upon which we provide exceptional care to our patients and our staff without exception. Thank you in advance for taking the time to review and understand the Code of Conduct and complete the annual compliance training course, which will be assigned to all employees each year.

The success of our compliance program depends on all of our participation. Thank you for all you do, and for your attention and commitment to delivering patient care with integrity at BMC.

Alastair

Alastair Bell, MD
President & CEO
Boston Medical Center ***Health System***

BMC'S CORE PURPOSE, VISION AND VALUES

Our Core Purpose

Exceptional Care. Without Exception.

Our Vision 2030

Make Boston the Healthiest Urban Population in the World.

Our Three Core Values



- **Above all, care.**
- **What matters to you?**

- **Make it happen.**
- **We ask why.**
- **We ask why not.**





- **Inclusion always.**
- **Diversity is our heart and soul.**

CARING FOR OUR PATIENTS WITH INTEGRITY

Quality Care



Caring for our patients with integrity means providing high quality, effective, compassionate and appropriate care to every patient. We are committed to the delivery of honest and necessary care, regardless of the patient's ability to pay. We always put the patient first in everything we do.

We ensure the quality of the patient care we provide by continuously monitoring and improving it. We meet the quality of care standards set by The Centers for Medicare and Medicaid Services (CMS), The Joint Commission (TJC) and other accrediting institutions. Every BMC colleague is responsible for ensuring that we provide high quality care to every patient.

In any circumstance where you question whether BMC is providing the highest quality care possible, you have an obligation to raise your concern with your manager, with Quality and Patient Safety (page SAFE [7233]) or Compliance and ensure that it is satisfactorily addressed and resolved.

Patient Safety

Caring for our patients with integrity also means keeping our patients safe at all times and avoiding preventable harm. At BMC, we work to create an effective patient safety culture. A "culture of safety" is one where all employees are always mindful of the risks inherent in our work and continuously strive to eliminate them.

We do this by:

- Asking for help or offering help in uncertain circumstances;
- Reporting adverse events, including errors, near misses and unsafe situations, by paging SAFE (7233) and filing a RL Incident Report;
- Seeking to understand the root causes of adverse events; and
- Participating in problem-solving and process improvement to prevent errors and increase patient safety.

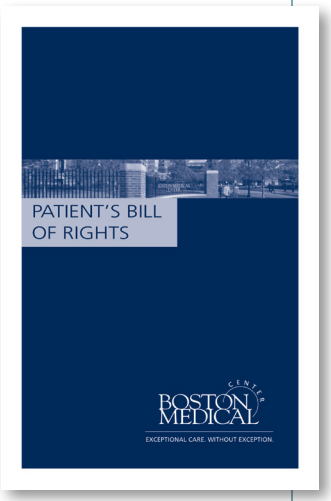
It is imperative that all BMC colleagues report any incident or unsafe situation they see or are involved in that could or did cause harm to patients or visitors, our colleagues or BMC.

For more information, please consult BMC policy "Online Incident Reporting Policy #04.01.000."

Q I almost gave a patient an incorrect dose of medication. Do I need to report this "near miss" even though no harm occurred?

A Yes. Reporting this incident to the RL system allows BMC to understand the root cause and make any changes in process needed to prevent this from happening again.

Patient Rights



Our patients have rights that are guaranteed by **both** federal and Massachusetts **state** laws. Patients have a right to review and receive copies of medical records (for a nominal copying fee in some cases), the right to privacy during medical treatment or care and the right to informed consent. BMC ensures that the rights described in the Patients' Bill of Rights are **always** respected.

We also believe that all our patients have the right to consistently excellent and accessible health care services regardless of status or ability to pay. We serve all patients and their families with dignity and respect. We are sensitive to the ethnic, religious, language and cultural differences of our patients.

To protect our patients' rights, we:

- Involve patients in all material aspects of their care, including obtaining informed consent for treatment;
- Communicate effectively with patients, families and caregivers and use BMC Interpreter Services as needed;
- Treat patients in a culturally-appropriate manner that preserves their dignity, autonomy and civil rights;
- Inform each patient (or representative) of his or her rights in advance of providing or discontinuing care; and,
- Respect patients' decisions even when we do not agree with them.

Q I need to obtain a copy of the Patients' Bill of Rights. Where can I find it?

A The Patients' Bill of Rights can be found on BMC's external website, **www.BMC.org**.

For more information, please consult BMC policies "Patient Rights and Responsibilities," "Patient Consent," and "Interpreter Services Department."

Non-Discrimination

BMC treats all patients with integrity regardless of race, color, national origin, sex, age or disability consistent with the requirements of Section 1557 of the federal Affordable Care Act, which prohibits BMC from discriminating against patients based on any of these factors. The law requires that **all individuals** be treated equally in the health care they receive**,** and also prohibits the denial of health care or health coverage based on an individual's sex, including discrimination based on pregnancy, gender identity and sex stereotyping.

For individuals with disabilities, the law requires BMC to make all programs and activities provided through electronic and information technology accessible, to ensure the physical accessibility of newly constructed or altered facilities and to provide appropriate auxiliary aids and services for individuals with disabilities. BMC also must take reasonable steps to provide meaningful access to individual**s** with limited English proficiency eligible to be served or likely to be encountered in their health programs and activities. Patients who are denied any of these rights can make a complaint to the Office of Civil Rights of the U.S. Department of Health and Human Services.

In addition, BMC respects the personal dignity and rights of each patient and is committed to providing transgender and gender non-conforming patients with professional, considerate and respectful care. When transgender and gender non-conforming patients present for health care services, they will be addressed and referenced on the basis of their self-identified gender identity, using their preferred pronouns and names, regardless of appearance, surgical history, legal name or sex recorded at birth. All BMC patients may use the restrooms and facilities that match their gender identity. BMC patients also may request that the Health Information Management Department change their name or gender marker in their electronic medical record.

Q If a patient's gender expression does not clearly indicate the patient's gender identity, how should I address this person?

A You should use the patient's name and discreetly and politely ask what pronoun the patient uses.

For more information, please consult BMC Policies "Gender Identity and the Transgender/Gender Non-conforming Patient" and "Medical Record Amendment or Correction."

Advocating for our Patients and their Families and Caregivers

Our goal is to create a care environment in which patients and their families receive exceptional care without exception. One way we do this is by advocating for our patients, at the bedside and in the community. Despite our best efforts, we may not always meet our patients' expectations. When this occurs, we want to learn from our patients so that we can remedy their concerns.

BMC's Patient Advocacy Program serves as the liaison between patients, families and the BMC community. The program advocates collaborative work with staff to address and resolve patients' expressions of commendation and concern. This program ensures a prompt and sensitive response to each patient.

Patient advocates assist patients and their families in the following areas: patients' rights and responsibilities; patients' rights to make a complaint; the Health Care Proxy; and, problems, concerns or unmet needs of patients and their families.

Patient advocates:

- Seek solutions to the concerns and unmet needs of our patients and their families;
- Empower patients to become active participants in their own health care;
- Educate the community about patients' rights and responsibilities;
- Facilitate effective communication among patients, families and staff;
- Encourage our patients and their families to share their concerns with BMC colleagues or the BMC Patient Advocacy Program; and,
- Provide guidance to patients regarding Advance Directives, including the Massachusetts Health Care Proxy.

Q My patient has questions about a health care proxy. Who do I call?

A Call the Patient Advocacy Office at 617.414.4970

For more information, please consult BMC policy "Patient Advocacy Program."

Protecting Patient Privacy

We maintain the privacy and security of our patients' protected health information and other personal and financial information at all times. The Health Insurance Portability and Accountability Act of 1996, (HIPAA), and other federal and state laws, prohibit the use or disclosure of patient information without patient consent, unless it is for treatment, payment or hospital operations. These rules also apply to BMC colleagues when they receive medical care at BMC.

Accessing or sharing patient information in violation of HIPAA, other laws or BMC policy is a serious matter that can result in significant individual criminal or civil liability, including but not limited to, fines and imprisonment. Any BMC colleague who violates these laws may be subject to disciplinary action up to and including immediate termination of their employment or BMC affiliation.

We protect the confidentiality and security of patient information by:

- Never disclosing a patient's confidential information to anyone, including family and friends, except to complete BMC work (i.e., for treatment, payment or hospital operations) or as permitted by law and BMC policy;
- Not accessing or obtaining any patient information other than that which is necessary to do our jobs;
- Using only devices that are approved for use in the BMC IT Security policies and only when they are password protected and encrypted;
- Never discussing confidential patient information in public areas or other locations where we may be overheard by others;
- Releasing patient information only to persons who have the patient's written authorization or who are authorized by law to receive it;
- Never discussing BMC patients or posting patient information or photos on social media sites, even if the patient authorizes it;
- Remembering only the BMC Communications Department may answer health care questions asked by others on BMC's social media sites;
- Never creating a new BMC social media site without the express consent of the BMC Communications Department;
- Acknowledging our obligation to protect BMC's confidential information, including patient and business information;
- Contacting the BMC Privacy Officer if we have a question about releasing patient information before we release it; and,
- Reporting to your supervisor or manager or the BMC Privacy Officer any actual or suspected unauthorized use, access or disclosure of patient information.

Q How can I protect patient privacy when I am caring for patients in shared rooms?

A You can close the curtains around the bed, speak as quietly as possible to the patient and make sure the patient is willing to discuss treatment and care if visitors are present.

Q A colleague has been admitted to BMC and our department is worried about him. Can I look at his medical record to see how he is doing?

A Absolutely not. HIPAA protections apply to BMC employees who also are patients. You can only look at the medical record if your job duties and responsibilities require you to do so.

HIPAA also provides patients with certain rights regarding their protected health information. Patients can request an amendment or correction to the information contained in their medical records and an accounting of all disclosures of their protected health information. Patients also can choose to opt out of the hospital directory to maintain their privacy. When first registering at BMC, all patients must be given a Notice of Privacy Practices, which informs them of these and other rights.

Identity theft is a growing problem for health care providers throughout the United States. It occurs when a patient's personal and financial information is illegally obtained from a provider and then used to open credit accounts or obtain goods and services. We follow the requirements of the BMC Identity Theft Prevention Program and take all possible actions to prevent the improper or illegal use of patient information.

If you have any questions about the release of patient information or identity theft, you should contact the BMC Privacy Officer at 617.414.1800. For more information, please consult BMC policies "Release of Medical Records and Protected Information," "Confidentiality and Use of Information," "HIPAA Minimum Necessary Standard," "Red Flags and Identity Theft Prevention Program," "Social Media," and "Notice of Privacy Practices."

Financial Assistance for Patients

We work with patients who are uninsured or underinsured to assist with applying for available financial assistance programs that may cover some or all of their unpaid hospital bills. In order to help uninsured and underinsured patients find available and appropriate financial assistance programs, BMC provides all patients with a general notice of the availability of programs in both the bills that are sent to patients as well as in general notices that are posted throughout BMC. The goal of these notices is to assist patients in applying to a financial assistance program, such as MassHealth Qualified Health Plans Health Safety Net, for coverage or to assist with a Medical Hardship application to help pay for bills already received. We provide, upon request, specific information about the eligibility process to be a Low Income Patient under the Massachusetts Health Safety Net Program or additional assistance for patients who are low income through BMC's own internal financial assistance program.

For more information, please consult BMC policies "Credit and Collection Policy," and "Self-Pay."

EMTALA (The Emergency Medical Treatment and Active Labor Act)

The Emergency Medical Treatment and Active Labor Act, known as EMTALA, requires us to perform a medical screening examination and stabilize every patient who arrives in our Emergency Department or elsewhere on the BMC campus with an emergency medical condition, regardless of the patient's ability to pay. "Emergency medical condition" includes pregnant women who are in active labor.

Patients can be transferred to another medical facility at their request or when an authorized BMC clinician determines that the patient's medical needs cannot be met at BMC because we do not have the capability or capacity to treat the patient. Patients must consent to the transfer and all other EMTALA transfer requirements must be fulfilled.

At BMC, we carefully follow all of the requirements of EMTALA. We do not delay the medical screening examination or stabilizing treatment in order to seek financial or insurance coverage information. We do not admit, discharge or transfer patients with emergency medical conditions based on their ability or inability to pay or any other discriminatory factor.

For more information, please consult BMC policy "Treatment and Transfer of Emergency Patients."

INTEGRITY IN OUR WORKPLACE

Equal Employment Opportunity for All Employees

BMC is proud to be an integral part of the diverse community of Boston. BMC draws upon this community, which is comprised of people from a wide variety of cultures and backgrounds, as a resource for our employees and patients. BMC is committed to creating and sustaining a workplace where we respect and value our employees, not in spite of, but because of the differences in their backgrounds and cultures.

We believe there is strength in diversity, not only of race, gender, age, religion and disability, but also of education, family status, national origin, sexual orientation, gender identity and expression and all of the other factors that make each of us individuals. Honoring the diversity of our community promotes and ensures the mutual respect, collaboration and productivity that is necessary to provide the highest quality health care.

For more information, please consult BMC policies "Affirmative Action/EEO Statement" and "Diversity Statement."

Professional Conduct

Everyone affiliated with BMC is expected to conduct themselves in a professional and collegial manner at all times. BMC complies with all laws and regulations governing all aspects of employment, including hiring, promotion and termination. We do not tolerate harassing or discriminatory conduct and we do not permit retaliation against or intimidation of anyone who makes a good-faith complaint of discrimination, harassment or retaliation. We investigate and take appropriate action on all reports of such actions that are made to supervisors, Human Resources at 617.638.8582 or the Compliance Hotline, 800.586.2627.

In order to provide the highest quality patient care, we must collaborate, communicate and cooperate at all times. We can achieve this only if we treat each other with respect, courtesy, dignity and understanding. For this reason, BMC does not permit disruptive or abusive behavior by anyone in the workplace. Examples of such conduct

include threatening or intimidating behavior or words, taunting, jeering, mocking or humiliating another person, physical demonstrations of anger (such as throwing equipment), screaming or yelling or any other behavior that interferes with the optimum delivery of health care services.

If you observe or have been subjected to abusive or disrespectful conduct, you should report it immediately to your supervisor, Department Chair, the Chief Medical Officer, the Office of General Counsel, Human Resources at 617.638.8582 or the Compliance Hotline, 800.586.2627. All reports will be investigated promptly and resolved appropriately.

For more information, please consult BMC policies "Discrimination and Harassment Policy," "Employee Conduct" and "Medical/Dental Staff Policy Regarding Unprofessional Relationships and Disrespectful and Abusive Conduct."

Safe and Secure Workplace

BMC prioritizes the well-being and personal safety of its employees and anyone who does business with us. Acts of violence and threats of violence in the workplace are prohibited. Violent acts include physical violence, stalking, threats and similar acts. Workplace violence also includes any conduct that is offensive or intimidating enough to make an individual reasonably fear for his/her personal safety or the safety of family, friends or property. BMC does not permit firearms, weapons, explosive devices or other dangerous materials in our facilities.

Any BMC colleague, regardless of position, who commits or threatens to commit an act of workplace violence will be subject to disciplinary action up to and including the termination of employment. You must immediately report all threats of or actual violence to your supervisor or another member of management and Public Safety at 617.414.4444. We will promptly and thoroughly investigate all reports and will not tolerate retaliation against anyone who makes a good faith report.

For more information, please consult BMC policies "Workplace Violence" and "Employee Conduct."

BMC is a Green Workplace

BMC is committed to being nationally recognized as one of the greenest hospitals in New England. BMC has established a Green Advisory Committee to provide direction and information about environmentally sustainable products and practices in order to promote the health of patients, visitors, employees, our local community and the global community. Current initiatives include:

- Engaging in hospital-wide diversion efforts that have resulted in a 25% recycling rate;
- Cutting emissions by 50% and entering into a solar power purchase agreement;
- Creating a roof top farm which is providing fresh produce to our patients and employees; and,
- Diverting four tons of food waste per month to BMC's bio-digester which keeps this waste out of landfills.

As a result of these and other efforts, Becker's Hospital Review named BMC one of the 50 greenest hospitals in America. Practice Greenhealth gave three awards to BMC in 2017, including the highest honor the organization bestows on hospitals.

Credentialing and Licensing

BMC employs only those individuals who are properly licensed and credentialed for the position for which they are hired. Proper credentialing and licensing are important ingredients of high-quality patient care and are required by federal and state laws. We conduct credentialing reviews before providers commence their work for BMC and we re-credential them at regular intervals in accordance with regulatory requirements. We also conduct criminal background checks on all colleagues before they are employed by or affiliated with BMC.

For more information, please consult BMC policies "Competency" and "Criminal Offender Record Information (CORI)."

No Retaliation

BMC does not permit retaliation against, or intimidation of, any BMC colleague who makes a good-faith report of a violation of law, this Code or BMC policies and procedures. This applies equally to reports made internally and to reports made externally to government entities. Retaliation is prohibited by both federal and state laws and will not be tolerated at BMC.

We seek to have an open and supportive environment where colleagues feel comfortable raising issues and everyone works to resolve them as quickly as possible. BMC colleagues are protected against retaliation and intimidation even if the situation giving rise to the report is ultimately determined not to have a factual basis. However, false reports made for malicious reasons may subject the reporter to discipline.

Q I was told by my supervisor that I am going to be interviewed by Compliance about a report made by one of my co-workers. I am worried that I will be retaliated against if I tell the truth. What can I do?

A You are required to participate in the Compliance investigations and to tell the truth, but you cannot be retaliated against for doing so. If you believe you have been subject to retaliation, please contact the Chief Compliance Officer.

If you believe that you are being retaliated against for making a report or for participating in an investigation, please contact the Chief Compliance Officer at 617.638.7919.

For more information, please consult BMC policy "BMC Compliance Policy Against Retaliation."

Conflicts of Interest

BMC makes clinical and business decisions based solely on the best interests of our patients and best business practices. Your outside financial or other person interests must not influence – or appear to influence – your professional decision-making on behalf of BMC. You also may not personally benefit from any actions that you take on behalf of BMC. You must put BMC's interests ahead of your own at all times.

In order to identify and manage potential conflicts of interest, you are required to disclose any potential or actual conflicts of interest to the BMC Chief Compliance Officer at 617.638.7919. Certain BMC colleagues are required to file annual disclosure forms that describe any potential or actual conflicts of interest the individual may have. The Chief Compliance Officer reviews the disclosures and determines how to manage or resolve any conflicts. Most can be resolved easily. In some instances you may be required to refrain from participating in certain decision making activities.

If you have not been asked to file an annual disclosure form but believe you may have a potential conflict of interest, please contact the Chief Compliance Officer.

For more information, please consult BMC policy "Conflict of Interest."

Q My wife just took a job with a vendor who sells medical supplies to BMC. What should I do?

A Contact the Chief Compliance Officer at 617.638.7919 to disclose this potential conflict. The Chief Compliance Officer will determine any actions that should be taken to manage the potential conflict.

Substance Abuse or Impairment at Work

We prohibit the use of alcohol, drugs or unsafe medications in the workplace. Abusing substances or working while impaired can lessen your ability to perform your responsibilities and compromise the safety of our patients, colleagues and the public. On-the-job use, possession, theft or sale of drugs or alcohol is strictly prohibited. BMC reserves the right to test an employee for drugs or alcohol when there is a reasonable suspicion that the employee is under their influence in the workplace.

For more information, please consult BMC policy "Drug and Alcohol Policy."

Excluded Providers

Federal law prohibits BMC from hiring, credentialing or contracting with any "ineligible person." An "ineligible person" is any individual or entity that is currently excluded from participation in state and federally-funded health care programs such as Medicare and Medicaid or that has been convicted of a criminal offense related to the provision of health care items or services and has not yet been reinstated after a period of exclusion or ineligibility.

We routinely screen all BMC colleagues against the Excluded Provider lists published by the federal government and the State of Massachusetts. If you are excluded from participation in the federal or state health care programs, you must notify the Chief Compliance Officer immediately at 617.638.7919. You also must notify the Chief Compliance Officer if you become aware that a BMC colleague has been excluded.

For more information, please consult BMC policy "Screening for Ineligible and Excluded Persons."

Q I just received notice that I have been excluded by the Office of Inspector General. What should I do?

A Inform you supervisor and immediately call the Chief Compliance Officer at 617.638.7919.

Political Contributions and BMC's Not-for-Profit Status

We do not use any BMC resources, including email, to engage in political activity either personally or on behalf of BMC. BMC is a 501(c) (3) tax-exempt, not-for-profit corporation, so BMC cannot take positions on political elections, campaigns or candidates. BMC also does not make contributions or expenditures, directly or indirectly (or through the use of intermediaries, consultants or otherwise) on behalf of any candidate for political office, political party or political committee. This prohibition includes monetary contributions and non-monetary contributions, such as colleagues' work time or BMC telephones, vehicles or premises.

BMC may, however, engage in public policy debates by making independent expenditures related to political speech. For example, BMC may provide relevant, factual information about the impact of public policy decisions on health care operations.

We can participate as individuals in political activities during our non-working time. However, we must be sure that we keep our personal political activities separate from our job duties and responsibilities and we can never suggest or imply that we are representing BMC when we participate in these activities.

For more information, please consult BMC policy "Political Contributions."

Use of BMC Assets

We do not use BMC resources, such as materials, supplies and equipment, for personal use. Generally, you should not conduct personal business during working hours and you should not use BMC's assets for personal financial gain. Occasional use of certain assets is permissible if the cost to BMC is negligible. However, you should not expect that any such activities are private, as BMC reserves the right to monitor and review your communication usage and content and to impose discipline when your usage violates BMC's policies.

For more information, please consult BMC policies "Internet Access and Use" and "Email and Voicemail Acceptable Use."

Confidential Business Information

We expect colleagues to protect BMC's confidential business information, such as our services in the market, key costs, employee compensation and marketing plans. Generally, confidential information cannot be shared and can only be used to perform our jobs. We exercise caution when we share the information with competitors and at trade association meetings. Our competitors include other health systems and facilities in markets where we operate.

We also respect our competitors' confidential information. We gather information about competitors ethically and do not accept information if we suspect it was obtained inappropriately.

The following are examples of the types of information that are considered confidential:

- Information that is not publicly known;
- Organizational strategies;
- Patient information;
- Cost data;
- Marketing plans;
- Salary and wage information;
- Business partnerships;
- Affiliations and mergers; and,
- Other financial data.

For more information, please consult BMC policies "Confidentiality and Use of Information" and "Internet Use and Access."

Cybersecurity

Threats to our electronic systems are increasing. BMC is doing everything possible to protect our systems against malicious attacks. Every BMC colleague has an important role to play in this effort. We have to be careful when using our email system so that we do not inadvertently introduce malware or other problems.

In order to protect our systems, all BMC colleagues should:

- Never click on an attachment or a link in an email unless you know the source
- Never provide your username or password in response to an email request, even if the email appears to be from BMC. BMC will never request your username and password by email.
- Ensure that all devices used to access BMC systems are password protected and encrypted
- Report any suspicious email you receive to the BMC Service Desk at 617.414.4500
- Shut down or log off your computer when not in use
- Never share your username or password with anyone

If you have any questions about cybersecurity, please contact the BMC Service Desk at 617.414.4500. For more information, please consult BMC Policy "ITS Written Information Security Program (WISP)."

Intellectual Property

We comply with all applicable intellectual property laws. We respect these laws as they apply to publications, media and other forms of expression and communication. We only use software that has been properly licensed and we use it in conformity with the terms of the license.

BMC's intellectual property rights are valuable business assets. Any work of authorship, invention or creation by a BMC colleague during the scope of his or her employment is BMC property. This includes, for example, patents, trademarks and trade secrets. We have a shared responsibility to protect BMC's property rights during our employment with BMC and afterwards. Please notify the Chief Compliance Officer at 617.638.7919 if you become aware of any new work that could benefit from intellectual property protection. We also respect the intellectual property rights of others and do not knowingly infringe on any valid third-party rights.

For more information, please consult "Patent Policy and Agreement Boston University Medical Center" located at www.internal.bmc.org, Research tab, Grants Administration Pre-Award, Internal forms.



Advertising and Marketing

Advertising and marketing are useful ways to inform the community, educate patients and their families, and attract clients, business partners and employees. We engage in truthful, informative and non-deceptive marketing and advertising. All marketing activities, including the development of websites by clinics and departments, must go through BMC's Marketing Department.

For more information, please contact the Marketing Department at 617.638.8990 and consult BMC policy "Use of PHI for Marketing."

Media Relations and Communications

The BMC Office of Communications is responsible for our media and public relations and all other types of communications within BMC and between BMC and the public. All news and other information that is released to the media by BMC must be approved by and coordinated through the Office of Communications. If you believe that non-public information from or about BMC has been or will be released inappropriately without the consent of the Office of Communications, please notify your supervisor or the Office of Communications immediately.

For more information, please consult BMC policy "Media Requests for Information, Interviews and Photographs."

Q A Boston Globe reported called me for comment on BMC's new Grayken Center for Addiction Medicine. Can I talk with the reporter?

A No. You need to contact the Office of Communications first and describe the inquiry. Communications will decide how best to handle it.

MAINTAINING INTEGRITY IN VENDOR RELATIONSHIPS

Vendor Relationships

BMC recognizes that relationships between providers and vendors can further a mutually beneficial exchange of information about products or services relevant to patient care. At the same time, these relationships may create potential conflicts of interest or opportunities for abuse or unfair advantage. For this reason, BMC has adopted a strict policy that prohibits BMC colleagues from accepting any form of personal gift, regardless of value, from health care vendors or their representatives. This prohibition includes food funded, directly or indirectly, by vendors and provided on the BMC campus.

This policy also sets forth the basic requirements for consulting relationships between providers and vendors, attendance by providers and others at educational conferences and other activities sponsored by vendors, vendor access to BMC facilities, educational grants and scholarships funded by vendors and the disclosure of provider/vendor financial relationships.

For more information, please consult BMC policy "Policy for Interactions with Industry by BMC Clinicians and Staff."

Vendors on Campus

The BMC policy on interactions with industry also contains requirements for vendor representatives who come to our campus. Under these requirements, vendor representatives:

- Cannot visit our campus without an appointment;
- Must check in at a RepTrax® kiosk before traveling around our campus;
- Generally cannot interact with trainees on campus; and,
- Are not permitted in patient care areas, except in limited circumstances.

All of the policy requirements must be followed by BMC colleagues in order to ensure the integrity and transparency of our industry relationships and to assure our patients that we provide the best and most appropriate care for each individual, free from the influence of industry or personal self-interest.

For more information, please consult BMC policies "Policy for Interactions with Industry by BMC Clinicians and Staff" and "Pharmaceutical Vendor Representatives: Rules and Regulations for Conduct."

Relationships with Referral Sources

The Federal Anti-Kickback Statute

The federal Anti-Kickback Statute and other laws prohibit the receipt of anything of value in return for making referrals of patients who are beneficiaries of federal or state health care programs. These laws also bar the payment or receipt of anything of value in return for directly purchasing, leasing or ordering (or for recommendations to purchase lease or order) any goods, facilities, services or items covered reimbursable under the Medicare or Medicaid programs. A similar law in Massachusetts applies these prohibitions to all patients, regardless of payer source.

BMC is committed to complying with these federal and state laws. All BMC colleagues are expected to be vigilant in identifying potential violations and reporting them immediately to the Chief Compliance Officer at 617.638.7919 or to the Compliance Hotline, 800.586.2627.

For more information, please consult BMC policy "Compliance with Anti-Kickback Laws."

The Federal Stark Law

The federal Stark Law generally prohibits a physician from referring a patient for certain health services to an entity in which the physician (or his/her immediate family) has a financial interest. There are certain specific exceptions to this rule, such as contracts for professional services and fair market value leases.

Patient referrals are important to the delivery of appropriate health care services. It is our policy that patients, or their legal representatives, are free to select their health care providers and suppliers, subject to the requirements of their health insurance plans. The choice of hospital, diagnostic facility or supplier should be made by the patient with guidance from his/her physician as to which providers are qualified and medically-appropriate.

For more information, please consult BMC policy "Patient Referrals: Compliance with Stark."

Q What actions might influence referrals and violate the Anti-Kickback Statute?

A Three examples are: a hospital providing discounted office space to a physician to induce the physician to make referrals; a pharmacy routinely waiving co-payments to encourage patients to get their prescriptions filled there; and, a gift from a health care vendor to thank hospital staff for or to encourage their purchases.



WORKING WITH INTEGRITY WITH GOVERNMENT

Compliance with Federal and State Laws

At BMC, we comply with all applicable federal and state laws, regulations and professional standards governing our operations and the delivery of health care services and products. These laws, regulations and standards are numerous, complex and technical in nature.

BMC colleagues whose positions may affect BMC's compliance with those laws, regulations and standards are expected to attend educational or training programs offered by BMC for the purpose of knowing and understanding those laws, regulations and standards and to certify their intent to comply with them.

It is important to remember that violation of any of these laws may result in personal criminal and civil sanctions and penalties. Some laws even subject violators to imprisonment, fines of up to $100,000 per occurrence, loss of licensure or exclusion from participation in the Medicare and Medicaid programs for a specified number of years or permanently.

Because the penalties can be severe, BMC cautions and advises all colleagues to always act wisely and in strict accordance with all applicable laws, regulations and professional standards. You can contact the Compliance Office at 617.638.7919 or by emailing compliancehelp@bmc.org to get support and guidance in complying with the laws.

Documentation, Coding and Billing

BMC is committed to complying with all federal and state regulations governing health care documentation and the coding and billing of claims submitted for payment. Complete and factual documentation in medical records is essential for accurate coding and billing. Accurate records also demonstrate our credibility as a health care provider and allow us to make the best decisions possible regarding the treatment and care of our patients.

All BMC colleagues involved in documentation, coding or billing should:

- Carefully follow departmental procedures for documenting in the medical record;
- Never alter, falsify or destroy any information in a medical record; and,
- Ensure that any contractors or agents who perform billing or coding work for BMC comply with our policies and all applicable laws.

For more information, please consult BMC policy "Documentation Requirements for Medical Record."

False Claims Acts and the Deficit Reduction Act

The federal and state False Claims Acts and the federal Deficit Reduction Act protect government programs such as Medicaid and Medicare from fraud, waste and abuse. It is a violation of the False Claims Acts to knowingly submit, or cause another person or entity to submit, false claims for payment by the government. These Acts also allow individuals with actual knowledge of alleged false claims to sue on behalf of the government and provide protection against retaliation for filing a false claims action.

It is illegal to submit claims for payment to the government that we know or should know are false. No specific intent to defraud the government is required for the claim to be deemed false. The False Claims Acts define "knowing" to include not only actual knowledge, but also deliberate ignorance or reckless disregard of the truth or falsity of a claim. Filing false claims may result in fines up to three times the amount of each false claim submitted for payment, other penalties, imprisonment and exclusion from participation in federal and state health care programs.

Q What are some examples of false claims?

A Examples could include billing for services not provided; billing for a higher level of service than was actually provided; billing under one provider's name/NPI for a service provided by another provider; and, billing for services not documented in the medical record.

Under federal law, all identified overpayments must be refunded to the government payer within 60 days of identification. Failure to do so can result in fines and other penalties. Colleagues who make good-faith reports regarding potential or actual violations of the False Claims Acts may not be subjected to retaliation or intimidation.

For more information, please consult BMC policies "Billing and Claim Submission Policy – Compliance with False Claims Act and Whistleblower Laws" and "Reporting and Returning Overpayments to Medicaid and Medicare."

Cost Reports

Federal and state laws require BMC to submit reports of our operating costs and statistics, known as cost reports. These laws define what costs are allowable and describe the appropriate methodologies to claim reimbursement for the cost of services provided to government program beneficiaries. BMC is committed to the preparation, submission and settlement of accurate, timely and complete cost reports.

Q We found boxes of old medical records when we cleaned out a storage area recently. What should we do?

A Please report your discovery to the BMC Privacy Officer at 617.638.7919.

Record Retention

Federal and state laws require that we retain medical and other records for specified periods of time. We carefully follow the rules for each type of record. All BMC colleagues are responsible for ensuring that our records are accurate, up-to-date and maintained in compliance with the law and BMC policies. BMC may suffer serious consequences up to and including sanctions, fines and loss of accreditation if we fail to comply with legal requirements.

For more information, please consult BMC policies "Policy for Retention and Destruction of Medical Records" and "Policy for Retention and Destructions of Documents Other than Medical Records."

Responding to Government Inquiries

BMC fully cooperates with all appropriate government requests for information, site visits, audits and investigations. These interactions with government authorities may have significant legal and financial impacts on BMC and you.

It is vitally important that you notify your supervisor and the BMC Chief Compliance Officer at 617.638.7919 immediately if you are contacted by a government agent for information relating to your work at BMC or if any government agency initiates a non-routine site visit. In this situation, you should ask for the government representative's official identification, the reason for the visit and whether he/she has a subpoena or warrant. You should then notify your supervisor and the Chief Compliance Officer and ask the government agent to wait while you do so.

If you are approached by a government agent regarding your relationship with BMC, you have the right to:

- Speak with the agent;
- Schedule an interview at a time and place that is convenient for you;
- Have counsel present;
- End the discussion with the agent at any time for any reason; or,
- Decline to talk with the agent.

For more information, please consult BMC policy "Responding to Government Inquiries."

Accreditation Efforts and Surveys

BMC holds a number of accreditations and certifications which are vitally important to our continued successful operation. We maintain these accreditations and certifications by participating in surveys and audits. We must always be direct, open and honest when we interact with accrediting bodies and surveyors. We cannot mislead these agency representatives or conceal or alter any documents in preparation for or during a survey or encourage our colleagues to do so.

Research

BMC conducts research that will lead to improvements in health care and health status for all people and further scientific advances in medicine. All research must be conducted according to the highest ethical standards and in compliance with all applicable policies, federal and state laws and regulations. We protect the rights and well-being of our patients who choose to participate in research studies. Refusal of a patient to participate in research will not compromise their access to our services or the care they receive at BMC.

We require our Institutional Review Board (IRB) to review and approve all research that involves human subjects. We engage human research participants in a meaningful informed consent process. We also maintain an environment that fosters privacy and security.

BMC will not tolerate acts of plagiarism, falsification or fabrication of data, or other research misconduct. We are committed to full compliance with our policy for responding to allegations of research misconduct. Our research investigators are expected to be accountable for the funds received from sponsors of research and to comply with the terms and conditions of research grants and contracts.

If you have any questions or concerns about research, please contact the Research Compliance Officer at 617.638.7919 and consult BMC policy "Research and Scholarship Misconduct."

Protecting the Marketplace

BMC strives to win business by providing high quality and cost-effective services. We comply with antitrust laws, which prohibit agreements between competitors that undermine the principles of fair competition. We do not tolerate behavior that fixes prices, divides markets, manipulates competitive bidding processes, causes boycotts of competitors or places unreasonable restraints on competition.

For more information, please consult BMC policy "Compliance with Antitrust Laws."



THE BMC COMPLIANCE AND PRIVACY/SECURITY PROGRAMS PROMOTE INTEGRITY

The BMC Compliance Program

The mission of the BMC Compliance Program is to protect public confidence in BMC's clinical and business practices through:

- Education;
- Establishment and enforcement of standards that comply with applicable laws and regulations; and,
- Identification and prompt resolution of instances of non-compliance.

The Program partners with BMC leadership and operational departments to promote an ethical workplace through adherence to this Code of Conduct and BMC's policies and procedures. The Program is designed to detect and prevent fraud, waste and abuse and to ensure our adherence to the many laws and regulations that govern the provision of health care. It also is a vehicle for preventing violations of law and enabling BMC to rectify any situation before it becomes a problem or a legal violation.

BMC expects good-faith cooperation from all colleagues to make the program effective. Compliance is everyone's responsibility.

The Program also promotes ethical decision-making. When you are confronted with a difficult decision at BMC, ask yourself:

- Is it legal?
- Does it comply with our Code of Conduct and policies?
- Is it the fair and honest thing to do?
- Is it in the best interests of our patients and BMC?
- Would I be comfortable if my decision were published on the front page of a newspaper or a website?

If you answer to all of the above questions is "yes," you are making the right decision.

The BMC Privacy and Security Programs

The BMC Privacy and Security Programs are designed to implement the requirements of HIPAA and other federal and state laws that govern the use and disclosure of patient medical, financial and personal information. The Security Program, which is led by our IT Department, ensures the security of our electronic systems, communications and confidential patient information. The Privacy Program provides education and training on patient privacy issues and conducts regular audits of BMC patients' medical records to ensure that records have been accessed only as needed to perform job duties and responsibilities. It also receives reports of potential and actual privacy violations and investigates and resolves them appropriately. Finally, the Program can give you guidance regarding the release of patient and other confidential information.

For more information, please contact the Security Program at 800.586.2627 and the Privacy Officer at 617.414.1800.

Duty to Comply, Report and Cooperate

Everyone at BMC has a duty to comply with this Code of Conduct, BMC policies and procedures and all applicable federal and state laws. If you become aware of any actual or potential violation of these requirements, you must report the situation to the Chief Compliance Officer at 617.638.7919 or to the Compliance Hotline, 800.586.2627, immediately.

BMC will not take any action against any BMC colleague who reports, in good faith, any violation, actual or threatened, regardless of whether the situation giving rise to the violation is ultimately determined to not have a factual basis. If you fail to report a violation, you may be subject to disciplinary action.

The BMC Compliance Hotline

BMC has a Compliance Hotline to encourage all BMC colleagues to ask questions, seek support and report concerns. The Hotline, 800.586.2627, is operated by an outside vendor and is available seven days a week, 24 hours a day. You can make a report using your name or anonymously if it is more comfortable for you. The Hotline provides interpreter services for individuals with limited English proficiency.

You are encouraged to report any concerns to your supervisor or to the Compliance Department at 617.638.7919 directly. You do not have to report the matter to your supervisor before calling Compliance or making a report on the Compliance Hotline. You also can send an email to the Compliance Department at compliancehelp@bmc.org.

Q I want to report a problem but I'm afraid my supervisor will find out I made the report. What can I do?

A You can call the Compliance Hotline 800.586.2627 at any time to make an anonymous report.

As stated earlier, BMC will not retaliate against anyone who brings a compliance matter to the attention of our organization. All reports will be investigated, generally within 30 days of receipt, and appropriately resolved under the direction of the Chief Compliance Officer.

For more information, please consult BMC policy "Compliance – Availability and Use of Compliance Hotline."

Special Role of Managers and Supervisors

BMC managers and supervisors have special responsibilities to educate their team members about Compliance, Privacy and Security. Managerial staff members also serve as role models for their colleagues and BMC expects them to treat everyone with respect and to act with compassion, honesty and integrity at all times.

It is the duty of BMC managers and supervisors to create an environment where BMC colleagues feel comfortable expressing concerns or raising issues without fear of reprisal. For this reason, managers and supervisors are required to know and understand this Code of Conduct and the Compliance, Privacy and Security policies and procedures and to support the programs at every opportunity.

Managers and supervisors requiring additional information or training about Compliance, Privacy and Security should contact the Compliance Department at 617.638.7919.

Discipline Imposed Fairly and Firmly

BMC enforces its standards of conduct through appropriate disciplinary action taken on a fair, equitable and consistent basis for every employee, regardless of position. Any BMC colleague who violates the provisions of this Code of Conduct or BMC policies and procedures will be subject to disciplinary action. The appropriate action will be determined on a case-by-case basis. BMC policy provides for a range of possible disciplinary actions, from a verbal warning to discharge from BMC employment or termination of affiliation with BMC.

Regardless of the violation, BMC reserves the right to impose any level of discipline, including immediate discharge from BMC employment, based on our assessment of all of the circumstances of the violation, including, but not limited to, the seriousness of the violation, the frequency of the violation, the actual or potential consequences of it and the employee's prior disciplinary and performance record.

For more information, please consult BMC policy "Employee Conduct."



BMC Compliance Office

960 Massachusetts Ave, 3rd Floor
Boston, MA 02118
Phone: 617.638.7919

The office hours are 8:00 am – 5:00 pm. Walk-ins are welcome or you can call the Compliance Office to make an appointment.

Compliance email: compliancehelp@bmc.org

Compliance Hotline: 800.586.2627

Intranet website: **www.internal.bmc.org/compliance**

BMC Privacy Officer

Phone: 617.414.1800

Email: Privacyofficer@bmc.org

Intranet website: **www.internal.bmc.org/compliance**

BMC Director, Pharmacy Compliance

Phone: 617.638.5843

Other Boston Medical Center Resources

BMC Office of Communications

85 E. Newton Street, 4th Floor
Boston, MA 02118
Email: communications@bmc.org

The Communications Office is available 24 hours a day, 7 days a week to assist you. For staffing information and phone numbers, please visit:
www.bmc.org/about/news/communications.htm

After hours, call 617.638.8405 and ask to be connected to the on-call staff person

BMC Human Resources Division

85 E. Concord Street, 1st Floor
Boston, MA 02118
Phone: 617.638.8582

Intranet website: **www.internal.bmc.org/hr/humanresources.htm**

BU/BMC Institutional Review Board (IRB)

560 Harrison Avenue, 3rd Floor
Boston, MA 02118

Phone: 617.638.7207
Fax: 617.638.7234

Email: medirb@bu.edu

Office hours: 8:00 am – 4:30 pm

BMC Interpreter Services Department

Phone: 617.414.5549
Fax: 617.414.5017

Office Hours: 8:30 am – 5:00 pm, Monday-Friday
Off-hours beeper number: 6042

Intranet website: **www.internal.bmc.org/interpret**

BMC Office of General Counsel

960 Massachusetts Ave, 3rd Floor
Boston, MA 02118
Phone 617.638.7901 (regular business hours)
617.638.7243 (on call attorney – after hours)

BMC Office of Patient Advocacy

Phone: 617.414.4970

To reach a Patient Advocate, please call the number above. A Patient Advocate is available on-site from 8:00 am – 4:30 pm, Monday through Friday. After hours and on weekends, a Patient Advocate is available by page through the phone number above.

BMC Office of Public Safety

85 East Concord Street, 4th Floor
Boston, MA 02118
Phone: 617.414.4444

Website: **www.bumc.bu.edu/publicsafety**

BMC Patient Safety

Pager number for serious incidents with clear harm: SAFE (7233)

Federal Government Resources

Centers for Medicare and Medicaid Services

www.cms.hhs.gov

US Department of Health and Human Services, Office of Inspector General (OIG)

www.oig.hhs.gov

US Department of Health and Human Services, Office of Civil Rights (HIPAA)

www.hhs.gov/ocr/privacy

Massachusetts Resources

Massachusetts Department of Public Health

www.mass.gov/eohhs/gov/departments/dph

Board of Registration in Medicine (BORIM)

www.mass.gov/eohhs/gov/departments/borim

Compliance Department
Boston Medical Center
960 Massachusetts Avenue, 3rd Floor,
Boston, MA 02118