BON SECOURS MERCY HEALTH

Compliance & HIPAA Privacy

HIPAA Privacy & Security Prohibited Actions

HIPAA privacy and security laws protect a patient's **Protected Health Information (PHI**), which is any oral, written, or electronic Individually identifiable health information that is maintained or transmitted in any form or medium (e.g., electronically, on paper, orally). Individually identifiable health information includes demographic information and any information that relates to a past, present, or future physical or mental condition of an individual; or the past, present, or future payment for the provision of health care to any individual. Potential breaches and violations of HIPAA can also take many forms. To prevent prohibited access or disclosures of PHI, you must be careful in how you use, share, and transmit PHI. Below are common actions that can lead to potential HIPAA breaches or violations. You as an individual, as well as the organization, are "at risk" for financial and personal liability resulting from HIPAA violations.

Contact the Bon Secours Mercy Health (BSMH) Ethics Help Line or any Privacy Team Member if you have questions about what you can or cannot do with PHI or to report any HIPAA privacy or security issues or concerns.

BSMH Ethics Help Line:

Website: BSMHEthicsHelpLine.org > Select "On-line" > Select "BSMH Compliance and Privacy Concern Form" > Select the "HIPAA Privacy" Category

Phone: 888-302-9224 The Ethics Help Line is open 24 hours a day, 365 days a year.

To reach a Privacy Team Member, please email Privacy@BSMHealth.org. All HIPAA concerns are specifically sent to the Privacy Team.

PLEASE REFRAIN FROM:

Electronics / Computer / Passwords

- Sharing your passwords and/or allowing others to use your computer while you are logged on. If an assigned user ID or password has been compromised, stolen, or used inappropriately, immediately notify the BSMH Service Desk (833- 691-4357 or 833-MY1-HELP) and change your password.
- Leaving your cell phone or computer containing PHI in a location without proper security measures in place including encryption, password protection or physical security (i.e., not visible and locked).
- Taking information containing PHI home via computers, thumb drives or other data files which may result in loss of the data, and/or failing to secure information from the view of family members.
- Leaving PHI unattended on a computer screen in public areas, on your desk or counters, copiers, fax machines or printers.
- Sharing your ID badge or borrowing someone else's ID badge for any reason.
- Printing or copying PHI indiscriminately. Only the minimum amount of PHI necessary to complete the task should be printed or copied.

Medical Records & Documents

- Accessing your medical record. Workforce members may not use access privileges associated with their workforce role to view or modify their own medical records. Workforce members can make a request to Health Information Management or utilize MyChart to view their own medical record.
- Accessing the medical record, accounts or data of a family member, friend, co-worker or other party (i.e., leader, VIP, famous person) out of curiosity or concern about their condition, care or treatment. Workforce members cannot access the records of coworkers, family, or friends, unless they are directly involved with the care of that patient. This includes a workforce member using their access privileges associated with their workforce role to view or modify their minor child's record(s).

- Sharing "patient lists" with other individuals or outside vendors who are not involved in the direct care of the patients listed.
- Accessing a medical record on matters related to employment without first obtaining the associate's written authorization.
- Giving police officers PHI without a search warrant, court order or other proper legal right to it.

  Throwing documents or materials (i.e., prescription labels, remits, claim forms, etc.) containing patient information in trash cans or recycling bins. Protected Health Information must be shredded or otherwise disposed of in accordance with BSMH destruction policies.

Email / Fax / Mail

- Emailing information or documents containing PHI without using encryption and password protection
- Faxing PHI without first checking the fax number; or not dialing "1" for long distance faxes (many fax machines automatically dial numbers last called or dial the first seven digits)
- Mailing information containing PHI without first verifying that the address is correct and current
- Sending PHI to personal e-mail addresses, and/or printing PHI on non-BSMH devices.

Cell Phones / Social Media / Conversations

- Using your personal cell phones or other devices to take pictures of a patient or patient injury not authorized under internal policy
- Texting confidential information- Only BSMH approved, encrypted, and authorized messaging applications (e.g., PerfectServe) may be used for texting confidential information. Communicating patient information via text message or IM is strictly prohibited
- Sharing pictures, videos, information or PHI about patients on social media (i.e., Twitter, Facebook, YouTube) even if you do not use the person's name
- Discussing the medical condition of a patient with others or visitors without the patient's permission or outside of internal policy. Discussing a patient's case in public areas without taking reasonable precautions to prevent the conversation from being overheard (e.g., lower your voice; find less crowded area)
- Disclosing to others the names of other individuals who have been recently treated for similar medical conditions without their permission.