BON SECOURS MERCY HEALTH

Corporate Responsibility & HIPAA

HIPAA Privacy & Security Prohibited Actions

HIPAA privacy and security laws protect personal and health information of patients. The information called **P**rotected **H**ealth **I**nformation or **PHI** can be in many forms. 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 Officer 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 > Report an Incident > select the Disclosure or Misappropriation of Confidential Information, HIPAA Compliance or Information Security Category

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

All HIPAA concerns are specifically sent to the Privacy Officer.

Privacy Officer Contact Information:

The Privacy Officer contact list may be found at BSMH Ethics Help Line or click here.

PLEASE REFRAIN FROM:

Electronics / Computer / Passwords

- Sharing your passwords or allowing others to use your computer while you are logged on so they can access medical records, accounts or data
- Bypassing security precautions so that log-in is not needed or is quicker
- Leaving your cell phone or computer containing PHI in a location without proper security measures 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 and then losing the files and/or failing to secure information from the view of family members
- Leaving PHI unattended on computer screen displays 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 directly without making a request to Health Information Management
- 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
- Sharing "patient lists" with other individuals or outside vendors who are not involved in the direct care of the patients listed
- Accessing the medical record on matters related to employment without obtaining the employee's consent through Human Resources
- 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 can

Email / Fax / Mail

- Emailing information or documents containing PHI without using encryption and password protection
- Faxing PHI to the wrong number 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 to the wrong person or wrong address without first checking the address is correct and current
- Sending PHI to personal e-mail addresses, 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
- 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 to do so or when outside of internal policy or job function
- 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