# Overview of Key Patient Privacy Concepts

**Health Insurance Portability and Accountability Act (HIPAA)** is a federal law that affords patients rights over their health information, limits access and use of health information by providers and vendors, and requires implementation of safeguards and security measures to protect health information. The laws, and subsequent updates, require providers to notify patients when their information has been used, accessed or shared inappropriately; to the extent the data has been compromised. Failure to comply with HIPAA can result in both civil and criminal penalties as well as significant monetary fines.

As a vendor to Steward, please keep the following key privacy points in mind:

- The access, use or disclosure of Protected Health Information (PHI) is permitted for the purpose allowed in your arrangement with Steward. PHI may not be used for personal purposes. If PHI is not required by your arrangement, you may not access, use, disclose any PHI which you may encounter incidentally during the course of your work with Steward.
- You may not make inquiries about PHI for others who are not authorized to access it.
- When permitted to access, use or disclose PHI, only the minimum amount of PHI necessary should be used. Steward has a policy related to minimum necessary standards to ensure that access to, requests for, or use and disclosure of patient's PHI is based on a minimum needed to complete the task.
- Apply appropriate safeguards before copying or removing PHI and only do so for job-related reason and with authorization. Regardless of whether you are on-site or off-site, Steward expects all vendors will maintain, transport and destroy confidential documents in an appropriate manner. Steward has a policy related to the removal, storage and secure transportation of PHI.
- Regardless of whether you are on-site or off-site, apply reasonable safeguards before mailing or faxing PHI. For example, for mailing, check that the contents and address are correct. For faxing, ensure an appropriate fax coversheet is utilized and the recipients and contents are correct.
- Maintain all paper PHI in a secured area (e.g. locked desk, locked file cabinet or locked office) and do not leave PHI unattended in plain view in any area that is accessible to persons not authorized to view the PHI.
- Avoid discussing PHI in public areas such as lobbies, public hallways and elevators. When discussing PHI, take appropriate precautions, such as lowering your voice, to prevent unauthorized individuals from hearing the information.
- Appropriately dispose of paper PHI by shredding or similar means so that the PHI is rendered unreadable, indecipherable, and otherwise cannot be reconstructed. Trash and recycling bins are not an acceptable method of disposal for PHI.
- Immediately report any known or suspected inappropriate access, use or disclosure following the process outlined in your contract with Steward or notify your Steward Business Owner.

It is also important to keep in mind that additional privacy obligations may exist as part of your organization's contract or relationship with Steward. If you access, use or disclose PHI in the capacity of a Business Associate, please refer to the Business Associate Agreement executed with your contract. If your organization receives data electronically, your organization's contract with Steward may contain additional electronic data requirements. Finally, if you have certain access to Steward applications containing PHI, Steward's Information Systems Use and Confidentiality Agreement describes additional user commitments.

Any questions related to your obligations should be directed to your Steward Business Owner. If you are not sure who your Business Owner is, please contact the please contact the Office of Corporate Compliance and Privacy at 617-419-4732.