Tips for PCI DSS Compliance

1. Identify who in the organization is responsible for pursuing compliance with Payment Card Industry Data Security Standard (PCI DSS)
2. Determine the organization’s “merchant level” and “merchant type”
3. Identify **all** locations where credit card transactions are taking place, i.e. in-person, by mail, by phone, by web, etc.; locations may include patient registration/checkout, patient financial services (billing), the gift shop, cafeteria, foundation/fundraising, outpatient pharmacy, DME rental, educational classes for the community, etc.
4. Create a transaction workflow diagram that demonstrates the path of credit card data internally and externally to the organization; include wireless devices; evaluate the need to store credit card data, especially for recurring charges; look for credit card data in paper documents (patient billing statements/remit forms), email attachments, office applications (e.g. Excel spreadsheets, Access databases, Word files, etc.) and backup media
5. Identify all applications and systems involved in handling and processing credit card transactions
6. Create an inventory of all point-of-sale (POS) terminals, workstations, and cash register systems that process credit cards
7. Maintain all devices with the latest security updates and patches
8. Conduct an initial self-assessment using a “Self-Assessment Questionnaire” (SAQ) that is appropriate for the scope of the organization; contact the payment processing vendor and request their help in identifying the correct SAQ form to use and ask for any assistance they will provide in helping with this assessment
9. Create a report of findings for the organization’s executives
10. Develop an action plan to remediate vulnerabilities and compliance gaps
11. Create / update policies to address handling of credit card data, including information security for all applicable staff
12. Begin user education / awareness for those staff members that process credit card transactions; training should be done upon hire and annually thereafter; have staff sign an acknowledgement of this training
13. Conduct an annual internal audit
14. Conduct quarterly vulnerability scans as well as after any significant change in the network; use of an Approved Scanning Vendor (ASV) is required
15. Conduct an external penetration test annually as well as after any significant upgrade or modification
16. Obtain proof of PCI DSS compliance from service providers, e.g. collection agencies, website providers (for online bill paying)

Things to Keep in Mind:

- PCI DSS requirements are not mandated by the federal government. Instead, they are established by the PCI Security Standards Council which represents the credit card industry.
- Until PCI DSS compliance is achieved, the organization may be charged a monthly "non-compliance fee" by the credit card processing provider. This fee is not insurance. It is a fee where your organization is basically admitting it is not compliant with PCI DSS. Your organization would still be liable for the impact of any credit card data breach, e.g. consumer notifications, reissuance of cards, etc.