

## Privacy Self Assessment

Listed below is a self assessment checklist to see how you are coming along with your HIPAA Privacy and Security compliance plan.

The self assessment can be structured in a number of ways. Possible areas for inclusion in your self assessment include:

- Patient sign in sheets must include only limited information;
- Leaving medical charts around the office site and use of clear plastic chart holders on exam room doors;
- The posting of patient schedules;
- Holding confidential conversations where they can be easily overheard by third parties;
- Computer screens in plain view;
- Staff regularly changing passwords and safeguarding access to work areas;
- Information accessible only to authorized staff, including medical records, lab reports, and faxes;
- Safeguards documented regarding transfer of paper and electronic medical records, orders, images, and lab specimens;
- HIPAA complaint, confidentiality statements and written privacy policies;
- Documented policies and procedures when employment terminated, including return of all keys, cards, and change codes and locks;
- Employee handbook/documentation HIPAA compliant with respect to security training, termination policies and procedures, etc.;
- Documented procedures to protect confidential information, if office equipment or files are taken from the premises;
- Policies, procedures and training in place for off-site functions, e.g., transcription, accounting or claims filing;
- Inventory of computer systems, and software;
- Regular virus check and mitigation program in place;
- Disaster plan to include contingency plans in event of systems failure;
- Confidential information stored electronically, with appropriate safeguards;
- Internet and phone transmissions secure; and
- Protection of e-mail communications that contain confidential information.