

# HIPAA CHECKLIST FOR COMPLIANCE

## Electronic Transaction Standards

- Inventory current transactions (*e.g.*, claims, preauthorization) and interfaces for compliance with HIPAA transaction standards.
- Determine whether you are going to convert your internal systems or use an outside vendor (clearinghouse).
- Determine what financial resources will be needed to comply with the transaction standards.
- Identify payers, insurers, and health plans that your organization deals with and determine how and when they will begin accepting standardized formats and code sets.
- Develop an implementation strategy—work with health plans and other payers; start with the most complex transaction, claims.

## Privacy Standards

- Identify a security/privacy compliance officer and patient complaint contact.
- Inventory data repositories.
- Review and revise policies governing use and disclosure of confidential information.
- Determine the appropriate uses of protected health information that are allowed under the consolidated consent for treatment, payment, and health care operations.
- Develop privacy training for all employees, volunteers, trainees and any other person who is likely to have contact with protected health information.
- Review business associate agreements to determine whether you are providing access to protected health information, and if so, modify those agreements to comply with HIPAA.
- Develop procedures for removal of identifying information.
- Establish policies and procedures for patient to review, amend, or correct medical information.
- Allow for inspection and copying of records. Procedures need to be developed for accepting/denying requests for amendments and corrections of records.
- Set up documentation procedures to account for handling of requests for patient information.
- Determine your organization's policy on whether it will accept a patient's request for restricting access or use of information.

## Security Standards

- Assign security responsibilities.
- Perform a risk assessment of assets, threats, vulnerabilities and practices.
- Identify gaps and deficiencies based on the proposed security requirements.
- Decide what will be done to address the risks, and identify resources needed.
- Inventory information systems for security enhancement and imbedded identifiers.
- Set policies and guidelines on workstation use. Secure workstation locations.
- Develop and revise security policies and procedures for health information management, *e.g.*, admissions/registration, nursing, and ancillary services.
- Set up security incident procedures.
- Plan and implement employee security awareness training. Provide training and education appropriate to job description, department, level of access, type of customer and user. Design training for new employees and ongoing training to reinforce security issues.