Checklist for HIPAA compliance

In order to ensure compliance with HIPAA, your practice should complete the following:

1. **Have a Notice of Privacy Practices (NPP):**
   - Does your practice maintain and share with your patients a NPP clearly detailing PHI use and disclosure and your patients' rights, including their rights to:
     - Prohibit the sale of their PHI or its use for marketing purposes,
     - Request privacy protections and amendments to their PHI,
     - Access their PHI,
     - Receive notice of any breach,
     - Obtain an accounting of disclosures?
   - If your practice maintains a physical site or office, is your NPP posted in a prominent location?
   - If your practice maintains a website, is your NPP posted on the website in a prominent location?

2. **Under the HIPAA Privacy Rule you must have the following policies and procedures in place and implement the policies:**

   a. **Anti-Retaliation and Intimidation Policy**
   Is there a policy in place stating that your practice will not retaliate against or intimidate any person who files a complaint or provides information regarding a HIPAA violation?

   b. **Business Associate Agreements**
   Has your practice entered into appropriate Business Associate Agreements with all of its business associates that have access to PHI?

   c. **Minimum Necessary Use and Disclosure of PHI**
   Does your practice have a policy that states when using or disclosing PHI, or when requesting PHI from another organization covered by HIPAA, reasonable efforts will be taken to limit the PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request?

   d. **De-Identifying PHI**
   Does your practice have in place a policy discussing de-identifying PHI?

   e. **Uses and Disclosures of PHI**
   Does your practice have in place a policy discussing the ways you can use and disclose PHI in accordance with HIPAA requirements and business associate agreements?

   f. **Uses and Disclosures of PHI to Personal Representatives**
   Does your practice have in place a policy regarding when you can use or disclose PHI to an individual's representative?

   g. **Right to Request Access to PHI**
   Is there a policy in place discussing an individual's right to request access to his or her own PHI in a designated record set?

Revised December 2013

h. **Amendment of PHI**
Does your practice have in place a policy discussing an individual's right to request an amendment to his or her own PHI in a designated record set?

i. **Accounting of Disclosures**
Is there a policy in place allowing a patient to request an accounting of all disclosures?

j. **Privacy Officer and Complaint Process**
Is there a policy in place appointing a privacy officer and discussing the investigation of all privacy-related complaints?

k. **Safeguards**
Does your practice have the appropriate administrative, technical and physical safeguards to protect the privacy and security of your patients' PHI?

l. **Disposal of PHI**
Does your practice have in place the appropriate steps staff members must undertake to dispose of any documents, film or hard copy materials that contain PHI?

m. **Employee Sanctions**
Are there education requirements and sanctions in place when staff members do not comply with the practice's HIPAA policies and procedures?

3. **Under the HIPAA Security Rule, the following written policies and procedures must be in place with respect to ePHI and the security measures listed in the policies must be implemented:**

a. **Risk Analysis and Security Official**
One of the most important policies under the Security Rule is the completion of a risk assessment. Accordingly, it is essential that your practice have in place a policy regarding the appointment of a security official and completion and documentation of periodic risk assessments.

b. **Risk Management**
Does your practice have in place policies discussing the appropriate security measures that should be implemented after a risk analysis?

c. **Sanctions**
Is there a policy discussing the sanctions imposed when a staff member does not comply with the practice's security measures?

d. **Information System Activity Review**
Is there a policy in place discussing how records of information system activity must be reviewed on a regular basis to prevent, detect, correct and contain security violations?

e. **Workforce Security**

Is there a policy in place discussing the security steps a staff member must undertake to access electronic PHI (ePHI), and how your practice will prevent non-staff members from accessing ePHI?

f. **Information Access Management**
Does your practice address how it will authorize, establish, maintain and modify a staff member's access to PHI based on his or her job functions?

g. **Security Awareness and Policy Training**
Is there a policy in place explaining the training process staff members must complete before accessing ePHI?

h. **Protections from Malicious Software**
Does your practice have in place a process for guarding against, detecting and reporting malicious software?

i. **Password Management**
Is there a policy in place discussing accepted standards of practice for creating, changing and safeguarding passwords to protect access to ePHI?

j. **Security Incidents**
Does your practice address how security incidents will be addressed and reported?

k. **Contingency Plan**
Does your practice have in place plans and procedures to respond to an emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster)?

l. **Facility Access Controls**
Does your practice have a policy in place that limits physical access to its electronic information systems and the facility or facilities in which they are housed, while still allowing properly authorized access?

m. **Workstation Use and Security**
Does your practice address how workstations in its facility are used and physically safeguarded to prevent unauthorized access?

n. **Device and Media Controls**
Does your practice address how it manages the receipt, removal and movement of hardware and electronic media containing ePHI?

o. **Disposal of ePHI**
Does your practice address how it will dispose of ePHI in a manner that will render it unusable, unreadable or indecipherable to unauthorized individuals?

p. **Technical Access Control**
Does your practice have in place a policy discussing what technical security measures must be implemented for its electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights?

q. **Integrity and Authentication of ePHI**
Does your practice address how it protects ePHI from improper alteration or destruction?

r. **Person or Entity Authentication**
Is there a policy so that the practice's information system verifies that a person or entity seeking access to ePHI is the one claimed?

s. **Transmission Security**
Does your practice have technical security measures implemented to guard against unauthorized access to ePHI that is transmitted over an electronic communications network?

4. **Breach Notification Rule**
The HIPAA Omnibus Rule changed what constitutes a reportable breach. Accordingly, it is important your practice have in place policies and procedures so one can accurately identify whether a reportable breach has occurred. Additionally, the policies should address who needs to be notified in the event of a breach.

5. **Training**
In an effort to ensure all staff members of your practice abide by the policies and procedures identified above, it is required that all new employees undergo HIPAA training. Additionally, all current employees should receive training once a year and anytime there is a significant change to HIPAA and/or your HIPAA policies.

For more information on HIPAA, please visit www.eatright.org/coverage.