Checklist for Compliance with HIPA

Physicians should consider the following checklist to evaluate their compliance with privacy legislation:

1. Patients should know what information is being collected about them and why it is being collected.

- A poster, sign or brochure should be freely available in the clinic that states:
  - Possible uses of patient information
  - Patients' right of access to their records
  - Patients' right to request amendments to their records
- Information collected should be limited to that which is necessary for the care of the patient and for registration and billing purposes.

2. There should be a process for appropriate patient consent to collection, use and disclosure of information.

- Consent must be informed and free of any coercion.
- Deemed (or implied) consent is generally sufficient for the ongoing care of the patient after the original presentation, including referrals to other caregivers. Release of information within the care team should be on a need-to-know basis.
- Express (usually written) consent should be obtained for use or disclosure of information for any purpose other than the original purpose for its collection.
- Patients have the right to limit consent.
- Patients can withdraw consent at any time. The consequences of withdrawal of consent should be discussed explicitly with the person and documented.

3. The office must have a process to permit patient access to personal health information.

- Patients must be permitted to see information in their records and to have copies of the records upon request. The physician should retain original documents.
- There are limited circumstances in which patients may be refused access to all or part of their record. Generally this is limited to circumstances in which disclosure is likely to endanger the mental or physical health or safety of the patient or another person, would disclose confidential information about someone other than the patient, or would identify a third party who provided information to the physician in confidence.
- Prudent physicians will ensure that patient access to records is supervised.
- Physicians may charge a reasonable fee for providing access and/or copies. The SMA Relative Value Guide provides some recommended cost recovery fees that may be charged.

4. There should be a mechanism to update and correct information in personal health records.

- Registration and billing data must be updated as required.

- Clinical records should be complete and accurate. Amendments to the clinical record should not erase any previous entries to the chart, should be dated and should indicate clearly that an addition or amendment is being made.
- Corrections can be made to inaccurate or incomplete factual information. A physician is not required to make an amendment to a patient record merely because a patient disagrees with the physician's diagnosis or opinion.
- Physicians who use electronic medical records should ensure that their medical record software tracks additions/amendments.

5. All personal information (registration data, billing data, health records, staff/employee records, etc.) should be kept appropriately secure.

- Consider locks, alarms and other physical security devices.
- Electronic records should be password protected, and electronic systems should have appropriate firewalls and other electronic security mechanisms. Consider handcuffing (limiting access to portions of the electronic record to defined users.)
- Office policies and procedures should ensure that records are kept secure, that written information cannot be seen by unauthorized persons, that conversations cannot be overheard, and that all physicians and employees understand the importance of complete confidentiality.
- If an information manager (computer support person, offsite storage company, etc.), has access to patient information, a written agreement should be in place whereby the information manager agrees to ensure confidentiality and limit access to the records.

6. The office must designate an individual (ideally a physician) to act as Privacy Officer to oversee management of personal information.

- The Privacy Officer should be familiar with the obligations under HIPA.
- This individual should develop and implement the privacy policies for the clinic and provide clinic staff with advice regarding HIPA compliance.
- All employees should know who this person is.

7. All staff should understand what types of information may be disclosed, to whom, and under what conditions.

- Disclosure within the "circle of care" (i.e. among health care professionals in the course of providing patient care) does not generally require explicit consent.
- HIPA allows disclosure without consent in a limited number of other situations (e.g. to a proxy for the patient in the case of advanced care directives, to a quality of care committee, for professional review/audit, to minimize danger to the health or safety of an individual). Disclosures of this type should be well-documented and overseen by the clinic's Privacy Officer.
- The office should have explicit policies that define whether staff may respond to requests for information about patients.

- Where information is shared among providers (or among trustees as defined in HIPA), consideration should be given to formal data sharing agreements signed by both parties. Data sharing agreements may be particularly important when data are shared electronically. Such agreements should bind both parties to comply with privacy requirements.
- The default position should always be to require explicit consent from the patient prior to any disclosure.
- When in doubt, staff should forward requests for information to the Privacy Officer.

8. Clinics should have a specific office policy for information management. All staff members should receive training about the policy and sign confidentiality agreements.

- Staff policies and procedures should contain an explicit privacy policy. Non-compliance with the privacy policy should be grounds for disciplinary action.
- Staff should receive regular in-service training on issues related to information handling.
- Staff should be required to sign a confidentiality agreement at the time of hiring. Consider annual renewals of the agreement. The Agreement should state that:
  - The employee is familiar with the office privacy policies
  - The employee will not read, use or disclose information in any patient record unless required for patient care, or to fulfill their job responsibilities.
  - The employee will not disclose any patient information to anyone except in accordance with the clinic's policies or as directed by the clinic's Privacy Officer.
- The clinic's privacy policy should be available to patients upon request.

9. The office should follow accepted guidelines for the retention and destruction of personal information.

- Guidelines for retention are usually those determined by the licensing authority or other professional oversight body.
- Destruction of personal information should always be by a method that removes personal identifiers and minimizes the chance of any inadvertent disclosure of information.
- If the office utilizes a third party to store or destroy records, there should be a signed agreement in which the third party agrees to maintain confidentiality with respect to the information in those records.

10. A process should be in place for handling complaints about management of personal information.

- The process should be defined in the office privacy policy, and usually should be handled by the Privacy Officer.
- In the event that a complaint cannot be resolved, the Privacy Officer or designated individual should know the mechanisms for referral of the complaint to the College of Physicians and Surgeons or to the Office of the Information and Privacy Commissioner.