MODEL HIPAA COMPLIANCE PROGRAM

Prepared for AACE Members

Prepared by:
AACE General Counsel

Christopher L. Nuland, Esq.
The Law Offices of Christopher L. Nuland
1000 Riverside Avenue, Suite 115
Jacksonville, Florida 32204

(904) 355-1555
(904) 355-1585 (Facsimile)

Copyright 2011, Christopher L. Nuland. All Rights Reserved, except where noted otherwise
Table of Contents

I. Foreword 3

II. Introduction 4

III. Basic Questions and Answers 6

IV. Initial Steps 8

   A. Selection of HIPAA Compliance Officer 8
   B. Corporate Resolutions 10

V. The HIPAA Compliance Program 11

   Education of Employees 11
   The Privacy Standards 11
   Standard 1: Consent 12
       Sample Consent Form 13
       Sample Privacy Notice 15
   Standard 2: Minimum Necessary 16
       Policies and Procedures 16
       Sign-In Sheet Example 18
   Standard 3: Oral Communications 19
   Standard 4: Business Associates 20
       Sample letter to Business Associates 21
   Standard 5: Parents and Minors 22
   Standard 6: Health-Related Communications and Marketing 23
   Standard 7: Research 23
   Standard 8: Restrictions on Government Access to PHI 24
   Standard 9: Use of PHI for Payment Purposes 25

VI. Medical Records Information 26

VII. The Security Standards 30

   Administrative Safeguards 30
   Physical Safeguards 37
   Technical Safeguards 38

VIII. Worksheets 40
Foreword

This packet contains a model HIPAA Compliance Program developed on behalf of the American Association of Clinical Endocrinologists (AACE) to help its members comply with the impending Privacy and Confidentiality Regulations of the Health Insurance Privacy and Accountability Act of 1996.

The Model Program is divided into the following four sections:

I. Introduction, which provides a quick overview of the law and answers to the most frequently asked basic questions.

II. Initial Steps, which guides the medical practice through the preparatory steps to establish the Program.

III. The Program itself, including materials which can be distributed to staff as part of the educational component

IV. A checklist to assist in your compliance efforts.

The Program is specifically designed for the small practice which usually cannot afford the corporate compliance programs offered by larger law firms. Moreover, AACE and its staff remain ready to assist members with the implementation of the Program.

Christopher L. Nuland
June 2011
I. INTRODUCTION

First passed in 1996, the "Administrative Simplification" section of the HIPAA law became effective in October 2002, with additional requirements having taken effect over the succeeding four years.

The HIPAA requirements, as applied to physicians, are divided into three parts. The first of these parts governs electronic transactions, and became effective on October 16, 2002. In order to comply with the rules that are designed to make all such technology uniform, many software programs and office procedures both had to be redesigned. Scores of vendors vied for the lucrative business of updating software, although many managed-care organizations provided this service for a nominal fee.

On December 28, 2000, the Department of Health and Human Services issued its final privacy regulations with regard to patient privacy. The regulations, required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), became effective on April 14, 2003.

The Security Rules was released in February of 2003, became effective 26 months later, and are intended to accomplish four major functions:

1. Ensure the confidentiality, integrity, and availability of all electronic protected health information (PHI) the covered entity creates, receives, maintains, or transmits;
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
3. Protect against any reasonably anticipated uses or disclosures of such information not otherwise allowed by law; and
4. Ensure compliance by its workforce.

In determining whether a covered entity has complied with these rules, the Department of Justice takes into account the size of the office, its technical infrastructure, the potential cost of security measures, and the potential threat to the security of the information. In other words, a “reasonable approach” is what is required. In order to show compliance, a covered entity should be able to document that it has addressed the Security Rule’s 18 standards, many of which may already have been addressed while complying with the Privacy Rule.
Together, the rules have been designed to protect the privacy and security of patient records, and impact not only physicians, but also insurance companies and scores of other entities that may come into contact with such information. Perhaps of most importance to the physician are the rules allowing patient access to medical records. Under the HIPAA regulations, patients not only have the universal right to inspect and copy their records, but also a limited right to amend the record itself and the right to prevent disclosures to certain entities and the right to ascertain what entities have been granted access to the private information.

One key element of the final rule is the restriction on what information must be given to an entity that may have the right to review the medical record. For instance, a health insurer that may have the right to audit records may not be granted access to records that do not pertain to the claim being audited. Such a requirement means extra work for physician staff, who are forced to redact certain information from many files.

Compliance with the Rules requires the covered entity to establish systems of alerting patients to the new requirements, as well as educating staff on the new requirements. Moreover, the covered entity is expected to develop procedures for tracking the disclosure of medical information and to be able to provide such tracking information to patients in a timely fashion. It should also be noted that the Rules do not preempt existing state laws regarding medical record confidentiality. Therefore, each office is keenly aware not only of the HIPAA requirements, but also the interaction of HIPAA and the existing state laws that pertain to patient privacy.

As always, AACE will be tracking the new rules as the implementation date approaches. Moreover, staff remains available to members that may have specific questions regarding these and other federal statutes and rules.
BASIC QUESTIONS AND ANSWERS

What is HIPAA?

The Health Insurance Portability and Accountability Act of 1996.

What Does HIPAA do?

Creates national standards to protect individuals' medical records and other personal health information?

To Whom Does HIPAA Apply?

Any physician (including one that submits claims through a billing agent) that submits claims electronically. Even those who submit only paper claims must comply if they accept Medicare and employ ten or more full-time employees.

When Does It Become Effective?

Although effective on April 14, 2001, its privacy provisions did not affect physicians until April 14, 2003. Electronic transactions are governed by HIPAA as of October 16, 2002.

What is PHI?

Protected Health Information (PHI) is any information through which a patient may be identified (e.g., name, address, social security numbers, phone numbers, pictures with distinguishing characteristics, etc.).
What Must a Physician Do to Comply?

1. Provide information to patients concerning their privacy rights.
2. Adopt clear, written privacy standards for the practice.
3. Train employees.
4. Designate a compliance officer.
5. Secure patient records.

What Recent Changes Have Been Made?

Based upon comments to the Rules, the Department of Health and Human Services adopted amendments that allow:

1. Phone-in prescriptions
2. Referral appointments
3. Inter-practitioner communication
4. "Minimum Necessary" changes
5. Release of records to other health care practitioners, even without consent
INITIAL STEPS

A. Selection of HIPAA Compliance Officer

The HIPAA Compliance Officer is the most important person in the entire program, as it is the responsibility of this individual to ensure that each segment of the Program performs in the manner set forth in this document. As a result, the Corporate Compliance Officer should be an individual who has sufficient time to devote to the project, sufficient respect from the physicians and staff to ensure their adherence to the Program, sufficient knowledge of the Rules to effectively administer the Program, and sufficient independence to ensure that decisions critical of the Practice’s leadership can be made free of undue influence.

Ideally, the HIPAA Compliance Officer will be a full-time employee with no additional duties. Recognizing the financial limitations of most endocrinologists’ offices, however, many Practices will either hire a consultant to perform this duty or make these duties a significant portion of a full-time employee who also holds other duties. It is for this reason that the overall budget for the Program be established prior to embarking upon the search for the appropriate individual to hold this position.

The following is a sample Evaluation Sheet for those individuals who may be interviewed as candidates for the HIPAA Compliance Officer position:
## HIPAA Compliance Officer Selection Criteria
(100 points Maximum)

Name of Applicant _____________________________________________

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Pts Allowed</th>
<th>Pts</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Knowledge of HIPAA Rules/Regulations</td>
<td>30</td>
<td>___</td>
</tr>
<tr>
<td>B. Knowledge of the Practice</td>
<td>20</td>
<td>___</td>
</tr>
<tr>
<td>C. Ability to Garner Respect</td>
<td>10</td>
<td>___</td>
</tr>
<tr>
<td>D. Independence</td>
<td>15</td>
<td>___</td>
</tr>
<tr>
<td>E. Cost</td>
<td>15</td>
<td>___</td>
</tr>
<tr>
<td>F. Accessibility</td>
<td>10</td>
<td>___</td>
</tr>
<tr>
<td><strong>Total Points</strong></td>
<td></td>
<td>___</td>
</tr>
</tbody>
</table>
B. Corporate Resolutions

Because the Practice must demonstrate a commitment to the Program, it is recommended that the Practice take official action to adopt a HIPAA Compliance Program. These steps should be taken in the form of a Board resolution, which may appear as follows:

RESOLVED, that the Corporate Compliance Program presented by (name of legal counsel) be adopted and implemented by the Practice.
THE HIPAA COMPLIANCE PROGRAM

A. Education of Employees

As education of all employees is a fundamental tenet of all Compliance Programs, all staff should receive ongoing education. In addition to reading materials, staff should receive in-person instruction training, either from the Compliance Officer, Legal Counsel, or other competent educator.

It is recommended that the first educational session occur within one month of the Board’s approval of the Compliance Program, and that other educational sessions be held throughout the year. Attendance should be taken to ensure that all employees attend each and every session. If time constraints and/or duties preclude the presentation of information to all employees in one session, alternative session times should be made available.
**Standard 1**

**Consent**

*Standard:  Physicians should obtain patient consent to carry out treatment, payment, or health care operations (TPO).*

- Consent is necessary for any provider who has a direct patient relationship
- Exception for emergency care and indirect providers (labs, etc.)
- Physician may refuse to treat patient that refuses to sign a consent form
- A consent form may only cover one provider at a time (groups OK). A valid release to another provider should be obtained before the release of medical records to another health professional, except in emergencies.
- Form must state how information may be used, allow access to practice's privacy notice, and to request restrictions or revoke consent
- Must be signed and dated
- Consents must be kept for at least 6 years
- Pre-existing consents need not be redone
Sample Consent Form

Patient: ____________________
Physician: ____________________

In connection with the medical services that I am receiving from ______________________, P.A., and its medical staff, I hereby authorize ______________________, the above-named physician, and their respective agents to disclose any and all information concerning my medical condition and treatment (including, but not limited to, super-confidential information concerning sexually transmitted diseases, mental health, chemical dependence, or other such information), including copies of applicable hospital and medical records to:

A. any third party payor covering the medical services of the patient;
B. other health care professionals and institutions involved in the delivery of health care to the patient;
C. The proponent of any legally sufficient subpoena, or in response to a court order;
D. Employees and agents of the practice, to the degree necessary to facilitate the provision of health care services and payment for such services;
E. Pharmacies; and
F. As otherwise required by law.

I further consent that photographs may be taken of me or parts of my body, under the following conditions:

1. The photographs may be taken only with the consent of my physician and under such conditions and at such times as may be approved by him.

2. The photographs shall be taken by my physician or by a photographer approved by my physician.

3. The photographs shall be used for medical records and, if, in the opinion of my physician, medical research, education or science will benefit from their use, such photographs and information relating to my case may be published and republished, either separately or in connection with each other, in professional journals or medical books, or used for any purpose which he may deem proper in the interest of medical education, knowledge, or
research. In such instances, however, it is specifically understood that in any such publication or use I shall not be identified by name and reasonable steps shall be taken to preserve my identity.

4. The aforementioned photographs may be modified or retouched in any way that my physician, in his discretion, may consider desirable.

When providing information to me, information may be transmitted to me by any or all of the following means (initial all that apply):

___ Telephone messages on an answering machine
___ Messages to the following family members or friends:
___ E-mail to the following address: ______________________________

5. I also consent to the release of Protected Health Information to the following individual(s):

In each case, the practice shall take reasonable steps to ensure that only the minimum necessary information is disclosed in accordance with the above. I further understand that I have been given access to the physician's privacy notice and that I have had the opportunity to place special restrictions upon the consent hereby given:

Special Restrictions:
____________________________________________________________________________
____________________________________________________________________________

This consent is valid from the date executed until revoked in writing by the patient.

Signed: __________________________
Date: __________________________
Witness: __________________________
Sample Privacy Notice

In accordance with the Health Insurance Portability and Accountability Act of 1996, patients of this Practice are entitled to the greatest degree of privacy possible. This office will strive to ensure that patient information is used only for authorized purposes as agreed to by the patient.

Patients are advised that they have a right to review their medical files upon reasonable notice to the Practice and during normal business hours, and to make comments to the same.

For further information, contact HIPAA coordinator __________________at____________. All complaints will be addressed without reprisal to the complainant.
Standard 2

Minimum Necessary

Standard: Disclosures of PHI must be the minimum necessary to accomplish the intended purpose.

- Exceptions include:
  a. Communications with other health care providers, especially in emergency situations
  b. Disclosure to patient
  c. Uses or disclosures authorized by patient
  d. Mandated disclosures
  e. Residency programs, etc.

- Internal Policies and Procedures must delineate who has access to PHI.

Policies and Procedures:

1. Before any records are released, staff will review to ensure that only the minimum information necessary has been released.
2. Before any records are released, staff will review to ensure that the release has been authorized by the patient or is otherwise permitted by law.
3. Except in emergencies, basic health care operations, or as required by law, the patient (or the patient's agent) shall be notified before any records are released.
4. Single sign-in sheets shall be used in the waiting room. Appointment logs will be kept out of sight from patient areas.
5. Only authorized members of the staff shall have access to medical records.

6. At the close of business each day, all medical information shall be secured either in the Practice's medical storage facility or in a physician, physician assistant, or ARNP office.

7. Medical records are not to be removed from the building. Physicians desiring to take records home must sign out such records. A log of such signed-out records shall be kept by each such professional or their personal assistant.

8. The practice shall maintain records of all releases of information, including the date, to whom, the information was sent, and the material included, in such form as could be immediately retrieved.

9. Before any PHI is released, the HIPAA Compliance Manager, or delegate thereof (one being appointed for each practice location), shall review the request and proposed documents to be released to ensure:

   a. That the request is from an authorized source (i.e., the patient or legally authorized representative). No PHI will be released to a non-medical third party without a consent to such release from the patient.

   b. That the request is for documents that may legally be released (a general release for "all medical records" is insufficient to release super-confidential records; a reply should be sent that the records "may contain super-confidential information that may not be released without the patient's express consent."

   c. That the documents to be released are the "minimum necessary" to achieve the purpose of the request. For instance, an insurer's request for records should produce only the records pertaining to the claim in question.

10. Each physician in possession of a medical chart is ultimately responsible for returning files to the file room.
Sign-in Sheet Example:

Patient Name: ____________________
Appointment Time: ____________________
Physician: ____________________
Time of Check-In: ____________________

Please deliver this sheet to the receptionist upon completion.
Standard 3

Oral Communications

Standard: Physicians must include standards on oral communications in their Policies and Procedures.

Practice Policies and Procedures:

- Oral PHI should be done away from general patient areas. Except in emergencies, all discussions regarding patient care shall be conducted either in that patient's examination room or in the physician's private office.
- Oral PHI should not involve unnecessary parties. Discussions concerning patients should never be made in another patient's examination room.
- Common area conversations concerning patients are to be avoided.
- Out-of-office conversations regarding PHI are forbidden.
- Requests for medical information, even from patients, will not be provided by telephone without the patient having provided their name, social security number, or date of birth.
**Standard 4**

**Business Associates**

**Standard:** Physician must obtain assurances that business associates (e.g., billing agencies) will use PHI only for the purposes for which they were engaged by the practice.

- Physician is not liable for privacy breaches of business associate if the physician has obtained "satisfactory assurances" of compliance from associate.
- "Business Associates" include all persons who may have physical access to PHI. They include contracted billing and collection personnel, accountants, janitorial companies, and sales representatives if they are given access to parts of the office in which medical records are maintained.
Sample Letter to Business Associates:

Dear ______________:

As a medical office committed to the privacy of our patients, we are taking all reasonable steps to ensure that patient information remains confidential at all times. Toward this end, we must insist that all representatives, agents, and subcontractors of your company:

a. Receive patient information only from authorized practice employees and agents;

b. Refrain from independently seeking to obtain patient information;

c. Take all steps to ensure that patient information to which you have access is kept confidential and used only to the extent necessary to fulfill the terms of our business relationships;

d. Make any patient information received available to the patient or us for inspection and amendment, and to authorized government authorities;

e. Report to us any and all unauthorized receipt of patient information and take reasonable steps to document and mitigate any such unauthorized disclosure(s);

f. Keep logs of all disclosures of patient information; and

g. Return or destroy all patient information upon termination of the contract.

We thank you for your efforts in the past to ensure our patients' privacy and look forward to your continued compliance with the above requirements, which we ask that you agree to by signing the bottom of this letter and returning it to the above address.

Thank you.

Sincerely,
Standard 5

Parents and Minors

Standard: Only the parent or legal guardian of child has right to access records.

- Exceptions include:
  a. State law pre-emption (e.g., Florida law concerning pregnancy or sexually transmitted diseases)
  b. Court order
  c. Potential abuse or neglect
  d. Parent or guardian consent

Policies and Procedures

1. The charts of all minors shall indicate the name of each parent to whom records may be released.
2. The minor's age of majority shall be noted on each chart.
3. Prior to release of any records concerning a minor to a parent or guardian, staff shall ensure that:
   a. The patient has not reached the age of 18;
   b. Only an authorized person is receiving the record; and
   c. The record does not contain super-confidential information for which minor’s have right of consent.
Standard 6

Health-Related Communications and Marketing

Standard: Any use of PHI for marketing must be specifically authorized by patient.

Policies and Procedures

All marketing involving PHI must be approved by the HIPAA Compliance Officer, who must ensure that all appropriate consents have been executed.
Standard 7

Research

Standard: Use of PHI for research is allowed so long as identifiable health information is redacted.

- PHI must be used only for research.
- Use of Institutional Review Board or Privacy Boards required.
- Safeguards against inadvertent disclosure are included.

Policies and Procedures

1. Research PHI will have all personal identifiable information redacted before release.
2. The release of PHI for research purposes shall be recorded on a log to be kept by the HIPAA Compliance Administrator.
3. Only the minimum necessary information shall be released to the researchers.
4. Researchers shall identify the IRB and/or Privacy Board under which they are operating, with this information to be included in the HIPAA Compliance Administrator's log.
Standard 8

Restrictions on Government Access to Health Information:

Standard: Medicare and Medicaid must comply with the new requirements.

- Office of Civil Rights may require records "pertinent to ascertaining compliance" with the Rule.

**Policies and Procedures:**

All government requests for HIPAA records must be approved by the HIPAA Compliance Officer.
Standard 9

Payment

Standard: Physicians may use PHI for payment purposes.

• Includes

  a. pre-authorization,
  b. billing,
  c. collection,
  d. utilization review, etc.
MEDICAL RECORDS

Introduction

Without fail, each and every physician is aware of the requirement to maintain medical records as part of his practice. Yet few physicians are trained in the legalities of medical records, such as the requirements as to exactly what constitutes a medical record and what minimum information must be contained within such a chart.

The Purpose of the Medical Record

Although most physicians recognize the medical record as a necessary tool to the provision of quality medical care, other reasons also exist for the maintenance of substantive and legible medical records:

(a) To serve as a basis for planning patient care and for continuity in the evaluation of the patient’s condition and treatment.
(b) To furnish documentary evidence of the course of the patient’s medical evaluation, treatment, and change in condition.
(c) To document communication between the practitioner responsible for the patient and any other health care professional who contributes to the patient’s care.
(d) To assist in protecting the legal interest of the patient, hospital, and the practitioner responsible for the patient.
In other words, the medical record is used both medically and legally. From a medical perspective, the record is utilized to provide a medical history, to determine if past treatments have been effective, and to obtain the input of previous health care practitioners. From a legal perspective, the medical record can be used by either the patient or health care practitioner to their advantage in any potential malpractice suit.

Contents of the Medical Record

The medical record should contain sufficient information to identify the patient, support the diagnosis, justify the treatment and document the course and results of treatment accurately, by including, at a minimum, patient histories; examination results; test results; records of drugs prescribed, dispensed and administered; and reports of consultations and hospitalizations. Evident from this list is that one-line summations of a patient’s progress will not meet the above criteria. Rather, the medical record should be detailed enough to meet each of the above standards.

Not only should a medical record contain a myriad of medical information, as is outlined above, but each entry should be signed, or at least initialed, by the endocrinologist.

Finally, the endocrinologist should maintain patient medical records in a legible manner and with sufficient detail to clearly demonstrate why the course of treatment was undertaken or why an apparently indicated course of treatment was not taken. Emphasis must be placed upon the word “legible,” as many governmental agencies and most juries assume that an illegible record equates to a missing record, and such a finding could seriously jeopardize any legal proceeding in which the medical record is to be used as evidence.
Maintenance of Medical Records

With the advent of microfilm and other reproduction technology, many offices have inquired as to how a medical record may be transposed into a more manageable form without jeopardizing its authenticity. If a medical record is to be converted into a computerized or microfilmed form, it must be done so in accordance with a written policy, and the copy must be capable of being reproduced in its original form. Finally, a custodian of records should be appointed within the office, whose job it is to ensure that all copying is done in conformity with the written policy.

Confidentiality of Medical Records

In general, records may not even be discussed with anyone other than the patient, the patient’s legal representative, or other health care practitioners involved in the care or treatment of the patient, unless the records are subpoenaed. Another exception involves Workers Compensation cases, in which the defendant/employer may request relevant medical information.

In some cases, medical records cannot be released even if they are subpoenaed by a court. Except with a patient’s consent, “highly confidential” records may not be released, even if a general release is presented. Examples of such records in California include psychotherapy notes, information about mental health and developmental disabilities, substance abuse and treatment, HIV testing, diagnosis and treatment, communicable diseases, genetic testing, domestic or elder abuse.
THE SECURITY RULE

A. Administrative Safeguards

1. Security Management Process Standard:

Required Elements:

*Risk Analysis and Information System Review:* The checklist found in Appendix A is a useful tool in performing a risk analysis and Information system review. Upon completion, the HIPAA Security Officer should meet with other members of the compliance team to note deficiencies and create appropriate responses:

*Risk Management:* Based upon the Risk Analysis and Information System Review, the Practice has adopted the following additional standards in order to maximize the security of its Protected Health Information:

1.
2.
3.
4.
5.
6.
7.
8.
*Sanction Policy: Violations of the Practice’s Privacy and Security Policies will be dealt with in the following manner:

a. **Mistakes Made in Good Faith (no knowing violations)**
   
i. First Offense: Warning
   
ii. Second Offense: Required additional education
   
iii. Third Offense: Probation
   
iv. Fourth Offense: Two week suspension without pay and report to licensing board and CMS
   
v. Fifth Offense: Termination and report to licensing board and CMS

b. **Knowing Violations**
   
i. First Offense: Two week suspension without pay and report to licensing board and CMS
   
ii. Second Offense: Termination and report to licensing board and CMS

2. **Assigned Security Responsibility Standard:**

   **Required Element:** Appointment of HIPAA Security Compliance Officer

   The following has been designated by the Practice as the HIPAA Security Compliance Officer:
3. **Workforce Security Standard:** The Practice must determine who should have access to PHI and under what circumstances, and must ensure that such access is terminated upon termination of an employment.

The responses to this standard are found in the Tab 3 of the survey found in Appendix A.

**Required Elements:**

- All keys, hardware and software are returned upon termination of employment.
- Passwords are deleted upon termination of employment.

4. **Information Access Management Standard:** The Practice must have policies and procedures as to how authorized persons may access information, such as passwords for electronic information.

Based on the responses to Tab 3, the Practice has adopted the following policies:

- A. No electronic personal health information shall be available without a password.
- B. Upon the termination of employment of a staff member with access to a PHI password, the password will be changed.
- C. Unauthorized personnel shall not be granted access to medical record areas or PHI.

5. **Security Awareness and Training Standard:** All staff must be trained in the new security standard. This training must be performed no less than annually, and may be combined with the HIPAA Privacy training.
6. **Security Incident Procedures Standard:** The Practice must have policies and procedures to deal with unauthorized disclosures.

**Required Elements:**

* Policies must require the identification and response to unauthorized disclosures.

* Policies must mitigate harmful effects.

* Policies must call for the Practice to document the incidents and their outcomes.

In response to the above, the Practice has adopted the following Procedures:

A. Business Associate contracts must require business associates to disclose unauthorized releases;

B. Upon discovery of any unauthorized disclosure, the HIPAA Security Officer shall be notified immediately;

C. The HIPAA Security Officer will, if possible, contact the person responsible for the disclosure and ascertain the recipients of any such disclosure;

D. The HIPAA Security Officer will then take such actions as are necessary to authorize the disclosure or ensure that the PHI involved is not forwarded, is returned to the Practice, and/or is destroyed immediately. All such efforts shall be documented;

E. In the event that the PHI cannot be secured, the patient involved shall be so notified.
7. **Contingency Plan Standard:** Likewise, the office must have policies to deal with the sudden loss of PHI.

**Required Elements:**

* Data backup;

* An emergency plan;

* Testing revision procedures.

In response to the above, TOI has developed the following policies and Procedures:

A. All electronic PHI files shall be backed up no less than monthly. Back up files shall be retained by the HIPAA Security Officer and shall be kept physically separate from the original files;

B. In the event of the loss of PHI through fire or other catastrophe, patients will be notified immediately and be given the opportunity to resubmit personal histories and other relevant information. Any patient file so recreated will be marked as a recreation, noting the date the original was lost, the cause of the loss, and the date the reconstruction;

C. No less than quarterly, back up files shall be tested for completeness.

8. **Evaluation Standard:** This standard requires the Practice to periodically evaluate itself to determine if it is in compliance with the Security Regulations. Again, compliance with this standard does not necessarily require the engagement of outside personnel. However, the person(s) responsible for this task will document the results of such an audit, as well as the date of such audit, and shall present to the Board of Directors the findings. Any necessary corrective action will be taken no later than 30 days after such a finding is made.

A Sample template for such an evaluation is attached as Appendix B.
9. **Business Associates Standard:** As in the Privacy Rule, Business Associates must guarantee that they will provide security for PHI.
B. Physical Safeguards

10. Facility Access Controls Standard: The Practice must have policies and procedures to control access to PHI and the facility itself.

   A. Only authorized staff shall have keys to the facility;
   B. Only authorized staff members shall have access to PHI passwords;
   C. Only authorized staff shall have access to PHI, and such access shall be restricted to a need to know basis. Should a staff member be found to have violated this policy, disciplinary action will be taken in accordance with this Manual;
   D. Any unauthorized release of PHI shall be deemed a cause for discipline as otherwise set forth in this Manual.

11. Workstation Use Standard: The Practice must have policies and procedures detailing what may or may not be done at a workstation.

   A. Internet access may not be used for personal reasons.
   B. At the close of each work day, workstations shall be secured.

12. Workstation Security Standard: Policies and procedures must be developed and implemented to ensure that only authorized employees have access to workstations.

   A. Patients and guests shall not be allowed in workstation areas;
   B. Computers shall have screen savers that are enacted upon no more than one minute of inactivity;
   C. Workstation computers shall be located in such a way so that the screens may not be regularly visible by patients or guests.

13. Device and Media Controls Standard: Offices must have policies to ensure that hardware, software, and media storage (e.g., floppy disks) are erased before being disposed, reused or leaving the building.

   A. All hardware, software, and/or media storage units shall be erased before being removed from the building for disposal;
   B. All paper charts shall be shredded upon being discarded;
   C. All long-term storage facilities shall execute a business associate agreement.
C. Technical Safeguards:

14. **Access Control Standard:** Access to electronic PHI must be restricted by office policies.

   Required Elements:

   * Unique user identification.
   * Emergency access procedures.

   In response to the above, the Practice has adopted the following Policies and Procedures:

   A. All electronic PHI shall be accessible only through a password;
   B. Off-hours access to PHI shall only be available in cases of a patient health emergency and with the approval of a physician or the HIPAA Security Officer;
   C. Off-site access to electronic PHI shall be available only to the HIPAA Security Officer and physicians working in remote treatment areas (e.g., hospitals).

15. **Audit Controls Standard:** The actual systems that house PHI must be audited/inspected periodically to ensure the integrity of electronic PHI.

16. **Integrity Standard:** Policies and Procedures must be in place to ensure that electronic PHI cannot be inappropriately altered or destroyed.

   A. Electronic PHI may not be altered or destroyed from a remote location;
   B. Any change to PHI may only be performed upon the request of a treating health care professional;
   C. Any change to PHI must be recorded (either electronically or manually).

17. **Person or Entity Authentication Standard:** A mechanism must be in place to authenticate the identity of those who gain access to electronic PHI. Passwords are a typical form of authentication.
A. Each staff member allowed access to PHI shall be assigned a password, which must be used before electronic PHI may be retrieved;
B. A record (either electronic or manual) of all electronic PHI activity shall be maintained.

18. **Transmission Security Safeguard:** The Practice must take steps to minimize the chance of unauthorized access to electronic transmissions of PHI.

A. Appropriate business associate letters must be obtained from all routine non-TPO recipients of electronic PHI;
B. No less than quarterly, PHI transmissions shall be randomly tested to ensure that no unauthorized distribution has taken place;
C. All payment transmissions shall be appropriately encrypted.
BEGINNING TASK LIST

DATE

___________________________________________________________

Organization Name

Use the following list to begin a HIPAA assessment of your practice. Attach additional sheets if necessary. It is recommended that these items be kept in a binder or folder with tabs to indicate the various sections.

TAB 1: Administration

Tab I should include this list, plus:

• The minutes of all meetings of the HIPAA compliance group, if applicable,

• Any administrative memos or notes relevant your HIPAA compliance project, and

• Any budget information relevant to your HIPAA compliance project.

1. Individual in Charge of HIPAA Compliance:
   Name __________________________________________________________
   Contact Information: _____________________________________________
                        __________________________________

2. Other Individuals in HIPAA Compliance Group:
   a. Name ______________________________________________________
      Contact Information: __________________________________________
                          __________________________________

   b. Name ______________________________________________________


Contact Information: ______________________________________________

______________________________________________

3. Compliance Record Keeper: ________________________________

4. Compliance Budget:
   a. Through March 31, 2002: ________________________________
   b. Through March 31, 2003: ________________________________

5. Meeting Schedule:
   _______________________________________________________

6. Meeting Location(s):
   _______________________________________________________


# TAB 2: Record Keeping

Tab 2 should include all information and materials relevant to the locations where patient information is kept.

7. How Are Paper Medical Records Kept? (Note All Which Apply.)
   
   a. Open Shelves Accessible to All: ______________________________
   
   b. Open Shelves Accessible to Staff Only: _________________________
   
   c. Open Shelves in Locked Room: _______________________________
   
   d. Filing Cabinets with No Locks: _______________________________
   
   e. Shelves/Filing Cabinets with Locks: ___________________________
   
   f. Off-Site Storage, No Security: _______________________________
   
   g. Off-Site Secure Storage: ____________________________________
   
   h. On Separate Sheet List All Sites Where Paper Medical Record Are Kept.

8. How Is Paper Claims and Billing Information Kept? (Note All Which Apply.)
   
   a. Open Shelves Accessible to All: ______________________________
   
   b. Open Shelves Accessible to Staff Only: _________________________
   
   c. Open Shelves in Locked Room: _______________________________
   
   d. Filing Cabinets with No Locks: _______________________________
   
   e. Shelves/Filing Cabinets with Locks: ___________________________
   
   f. Off-Site Storage, No Security: _______________________________
   
   g. Off-Site Secure Storage: ____________________________________
   
   h. On Separate Sheet List All Sites Where Paper Claims or Billing Information Is Kept.
9. How Is Other Patient Information on Paper Kept? (Note All Which Apply.)
   a. Open Shelves Accessible to All: ____________________________________
   b. Open Shelves Accessible to Staff Only: ______________________________
   c. Open Shelves in Locked Room: ____________________________________
   d. Filing Cabinets with No Locks: ____________________________________
   e. Shelves/Filing Cabinets with Locks: _________________________________
   f. Off-Site Storage, No Security: _____________________________________
   g. Off-Site Secure Storage: __________________________________________
   h. On Separate Sheet List All Sites Where Other Patient Information on Paper Is Kept.

10. How Is Electronic Patient Information Kept? (Note All Which Apply.)
    a. Not Applicable: _________________________________________
    b. Personal Computer(s), No Network Connections: ______________
    c. Personal Computers, Internal Network: ______________________
    d. Personal Computers, Internet Connection: ____________________
    e. Off-Site Personal Computers/Laptops Permitted Remote Access (Dial-In, Internet, etc.): __________________________________________
    f. Floppy Disks/CDs/Backup Tapes: ___________________________
    g. Handheld Devices (Palm Pilot, Jornada, etc.): _________________
    h. On Separate Sheet List All Equipment on Which Patient Information is Kept in Electronic Form.

11. Copy and Attach All Policies Concerning:
    a. Access to Files Containing Patient Information
    b. Access to Rooms, Shelves, Filing Cabinets Where Patient Records Are Kept
    c. Access to or Use of Electronic Equipment on Which Patient Information is Stored
Tab 3: Personnel/Workforce

Tab 3 should include all information and materials relevant to those individuals in your organization who are allowed to have access to, use or disclose patient information. You should include not only employees, but also trainees and volunteers who are under your organization’s control.

12. List All Individuals Who Work in Your Organization. For Each Individual, State:
   a. Job Title and Description
   b. Whether He/She Is Permitted Access to:
      i. Patient Clinical Information
      ii. Patient Billing and Claims Information
      iii. Other Patient Information
   c. Whether He/She Has Signed a Confidentiality Agreement and/or
   d. Whether His or Her Employment Agreement Has Confidentiality Provisions

13. Copy and Attach All Policies Concerning:
   a. Confidentiality of and Access to Patient Information
   b. Use and Disclosure of Patient Information by Staff
   c. Disciplinary Procedures for Breach of Patient Confidentiality
Tab 4: Patient Relations

Tab 4 should contain all relevant materials concerning the way your organization permits patients to have access to, copy or otherwise exercise some degree of control over the records which pertain to them.

14. Copy and Attach All Policies Concerning:
   a. Patient Review and Copying of Records
   b. Patient Requests to Amend Records
   c. Accounting to Patients for Disclosures of Patient Information
   d. Use or Disclosure of Patient Information for Marketing or General Contact Purposes

15. Copy and Attach:
   a. Standard or Customary Patient Release of Information Forms
   b. Any Notice of Information or Privacy Practices Published or Available to Patients
   c. Any Patient Brochures You May Publish
   d. Any "Patients' Rights" Notices You May Provide
**Tab 5: Business Associates**

Tab 5 should include an inventory of the individuals and organizations with which you exchange, from which you receive or to which you disclose patient information, not including the patients themselves. You should include copies of all your existing contracts or agreements with such individuals or organizations.

16. List All Individuals and Organizations to Which You Regularly Disclose:
   
   a. Patient Clinical Information
   
   b. Patient Billings and/or Claims Information
   
   c. Any Other Patient Information

17. List All Individuals and Organizations from Which You Regularly Receive:
   
   a. Patient Clinical Information
   
   b. Patient Billings and/or Claims Information
   
   c. Any Other Patient Information

18. Attach Copies of All Contracts or Agreements Currently in Effect with Individuals and Organizations to or from Which You Regularly Disclose or Receive Patient Information.