AMERICAN SOCIETY OF PLASTIC SURGEONS®
THE PLASTIC SURGERY FOUNDATION™

Executive Office
444 East Algonquin Road • Arlington Heights, IL 60005-4664
847-228-9900 • Fax: 847-228-9131 • www.plasticsurgery.org

ASPS RECOMMENDED HIPAA COMPLIANCE CHECKLIST

Medical records have always included some of the most intimate details of a person's life; however, federal laws regulating the privacy of that information were nonexistent until 1996.

As healthcare documentation and billing have become more systematic, federal laws have been enhanced to further modernize the flow of health information and provide protection of any health records held by physicians. Known as the Health Insurance Portability and Accountability Act, the mandate gives patients an array of rights with respect to any protected health information, which can include patients' names, date of births, Social Security numbers, email addresses, phone numbers, medical record numbers, photos, driver's license numbers, etc.

With the development of computerized health information storage, the requirements to be HIPAA compliant became even more stringent. In 2008, the HITECH Act was created to focus on the increasing use of electronic storage and communications systems. Covered Entities were now required to disclose any breach of unsecured PHI.

If HIPAA and HITECH Act were not enough, a new rule called "the Omnibus Final Rule" came to life to further protect patients' privacy, provide individuals new rights over their health information, and strengthen the government's ability to enforce the law.

Complying with the HIPAA Privacy and Security Rules can be a complex undertaking. The rules themselves have multiple elements and ongoing responsibilities. New methods of communication between patient and provider, and the many entities that can handle that data continue to grow. Recent updates to the rule have added a new level of compliance, with civil enforcement actions (including fines) routinely leveled against entities unable to comply with the rules.

Keeping in mind that penalties for noncompliance can reach up to $1.5 million per violation, and wanting to help members prepare and implement the most current list of HIPAA security rules, ASPS has created the following checklist. It provides a practical overview of the various office procedures that should be reviewed to ensure compliance with HIPAA.

Disclaimer*: This checklist is not meant to be a complete or formal list guaranteeing HIPAA compliance. Following each item on the checklist does not guarantee you will be HIPAA compliant. This document is meant as an overview checklist that will point you in the right direction.* **To ensure HIPAA compliance with respect to your individual needs, be sure to consult an attorney and assign a Privacy Officer**.

1. Definitions

Term	Definition
PHI	*Protected health information* means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. Note that there are some exceptions (e.g. records covered by the Family Educational Rights and Privacy Act).
Covered Entities include:	a) Health plans: With certain exceptions, an individual or group plan that provides or pays the cost of medical care. b) Health care clearinghouses: An entity that either process or facilitates the processing of health information from various organizations. c) Health care providers: Care, services, or supplies related to the health of an individual, including: 1) preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual that affects the structure or function of the body; and 2) sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.
Required	Required means that the given standard is mandatory and, therefore, must be complied with.
Addressable	Addressable means that the given standards must be implemented by the organization unless assessments and in depth risk analysis conclude that implementation is not reasonable and appropriate specific to a given setting. Addressable does not mean optional.

2. Administrative Safeguards

☐	Risk Analysis (required) – Perform and document a risk analysis to see where PHI is being used and stored in order to determine all the ways that HIPAA could be violated. ○ Example: Conduct a "walk-through" of the practice to identify areas where non-authorized individuals (patients and others) potentially have access to patients' medical and non-medical Protected Health Information (PHI).
☐	Risk Management (required) – Implement security safeguards and controls. Also monitor for changes and respond with enhanced strategies. Examples include: ○ Identifying new risks and document them ○ Reviewing previously documented risks ○ Setting a target date to rectify identified risks ○ Are computer screens visible to patients in waiting areas?
☐	Information Systems Activity Reviews (required) – Regularly review system activity, logs, audit trails, etc. See examples below: ○ Are all staff provided with a unique password for program access? ○ Do staff log out prior to leaving terminal unattended?
☐	Officers (required) – Designate security and privacy officers, and designate staff members to process complaints, patient requests for access and disclosures, review denials of patient requests, and process patient requests to make changes to records.

☐	Employee Oversight (addressable) – Implement procedures to authorize and supervise employees who work with PHI, and for granting and removing PHI access to employees. Ensure that an employee's access to PHI ends with termination of employment. Ensure your procedures answer the question below: ○ Do new employees receive privacy training as part of their new employee orientation? Have all existing employees undergone training?
☐	Sanction Policy (required) – Implement sanction policies for employees who fail to comply. Ask yourself the following question- does every practice employee have a signed workforce confidentiality agreement in their personnel file?
☐	Training Schedule (addressable) – Establish HIPAA compliance training schedule and curriculum, and train each member of staff about HIPAA. Example: Have each training member sign a statement certifying: ○ Date of training ○ Willingness to honor the privacy policies and procedures ○ Ability to re-certify every two years Keep signed paperwork for your records.
☐	Minimum Necessary (required) – Policy and procedure to limit disclosure to the MINIMUM NECESSARY to achieve the purpose of the disclosure – routine and non-routine disclosure (for non-routine also should have a policy to review PHI requests).
☐	Multiple Organizations (required) – Ensure that PHI is not accessed by parent or partner organizations or subcontractors that are not authorized access.
☐	ePHI access authorization(addressable) – Implement procedures for granting access to ePHI that document access to ePHI or to services and systems that grant access to ePHI. Examples include: ○ Creating a process for how the authorization is granted and who has access to grant it. ○ Assuring that the minimum necessary standard in the HIPPA Privacy Rule is being followed.
☐	Security Reminders (addressable) – Periodically send updates and reminders to staff about security and privacy policies to employees. Ensure your email reminders reinforce the proper use of their workstation, computer, equipment, etc.
☐	Protection against Malware (addressable) – Create procedures for guarding against, detecting, and reporting malicious software. Follow below examples to develop procedures: ○ Assure anti-virus software is installed and regularly updated. ○ Develop procedures for staff to report suspected or confirmed malicious software. ○ Develop Plan for recovering from malicious attacks. ○ Create a process to examine electronic mail attachments and downloads.
☐	Login Monitoring (addressable) – Institute monitoring of logins to systems and reporting of discrepancies. Create a standard for an auto lock after a number of failed attempts. Review log in attempts to look for trends. Document each log review and set a timeline of when they will be reviewed next.
☐	Password Management (addressable) – Ensure that there are procedures for creating, changing, and protecting passwords. Examples include: ○ Regular password changes (every 30/60/90 days) ○ Standards for strong passwords (minimum length, combination of numeric, alphabetical characters, capital, lowercase letters, case sensitive) ○ Unique passwords ○ Prohibiting password sharing within the office staff

☐	Response and Reporting (required) – Identify, document, and respond to security incidents. Incorporate the below questions into your procedures: ○ Was reason for breach identified? Who to notify of potential incidents? ○ How to respond to suspected incidents? ○ How to mitigate the incident - What measures have been taken to prevent similar instances from occurring in the future? ○ How to document the incident?
☐	Contingency Plans (required) – Ensure that there are accessible backups of ePHI and that there are procedures to restore any lost data. Example includes consulting with computer and software vendors on implementing appropriate data backup routine, including use of off-site location for storage of data via daily tape, CD or DVD.
☐	Contingency Plans Updates and Analysis (addressable) – Have procedures for periodic testing and revision of contingency plans. Assess the relative criticality of specific applications and data in support of other contingency plan components.
☐	Emergency Mode (required) – Establish, and implement as needed, procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.
☐	Evaluations (required) – Perform periodic evaluations (technical and non-technical) to see if any changes in your business or the law require changes to your HIPAA compliance procedures. Think about receiving automated information regarding changes to HIPAA regulations.
☐	Business Associate Agreements (required) – Have special contracts with business partners who will have access to your PHI in order to ensure that they will be compliant. Choose partners that have similar agreements with any of their partners to which they are also extending access.
☐	Complaints (required) –Implement policies and procedure for patients to file HIPAA compliance complaints.

3. Physical Safeguards

☐	Contingency Operations (addressable) – Establish, and implement, procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
☐	Facility Security Plan (addressable) – Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
☐	Access Control and Validation Procedures (addressable) – Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
☐	Maintenance Records (addressable) – Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (e.g. hardware, walls, door, and locks).
☐	Data Backup and Storage (addressable) – Create retrievable, exact copies of ePHI, when need, before movement of equipment, and implement procedures for removal of ePHI from electronic media and personnel responsible for removal.
☐	Workstation Use (required) – Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be

	performed, and the physical attributes of the surrounding of a specific workstation or class of workstation that can access ePHI.
☐	Workstation Security (required) – Implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.
☐	Disposal (required) – Implement policies and procedures to address the final disposition of ePHI, and/or the hardware or electronic media on which it is stored. Remember that PHI must be rendered unreadable when it is destroyed.
☐	Media Re-Use (required) – Implement procedures for removal of ePHI from electronic media before the media are made available for re-use.
☐	Accountability (addressable) – Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

4. Technical Safeguards

☐	Unique User Identification (required) – Assign a unique name and/or number for identifying and tracking user identity.
☐	Emergency Access Procedure (required) – Establish, and implement as needed, procedures for obtaining necessary ePHI during an emergency.
☐	Automatic Logoff (addressable) – Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
☐	Encryption and Decryption (addressable) – Implement a mechanism to encrypt and decrypt ePHI.
☐	Audit Controls (required) – Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.
☐	Mechanism to Authenticate ePHI (addressable) – Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.
☐	Authentication (required) – Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.
☐	Integrity Controls (addressable) – Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.
☐	Encryption (addressable) – Implement a mechanism to encrypt ePHI whenever deemed appropriate.

5. Required Forms

☐	HIPPA Privacy Notice (required) – draft patient notice that informs patients of privacy practices, post it in a prominent location, and make it available to patients.
☐	HIPAA Consent Authorization form (required) – form for release of confidential PHI as required by HIPAA. Give a signed copy to the patient, and establish the patient's right to revoke consent.
☐	Other forms as required by either HIPAA or state law. Examples include notice of privacy practices acknowledgement, new patient authorization, statement of financial responsibility, health plan coverage information, etc.
☐	Note (required) – forms should be read and signed in languages appropriate for each individual patient.

6. Patient Access to Records

☐	Implement procedures (required) to review patient requests to access their records. In creating the procedure, ask yourself this question- does the practice have protocols for verifying that a patient contacting the practices is actually the patient in question?
☐	Implement policy and procedure (required) to review denials of patient requests to PHI records.
☐	Implement procedures (required) for processing of patient requests to amend information in their records.
☐	Implement policy and procedure (required) to determine HIPAA compliant access to third party patient records – friends, family, caretaker, or legal next of kin.

Here are some helpful links designed to better understand HIPAA and stay compliant with the law:
http://www.hhs.gov/ocr/privacy/hipaa/understanding/
http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/index.html
http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html
http://www.onlinetech.com/resources/references/what-is-hipaa-compliance
https://www.securitymetrics.com/hipaa
http://www.onr.com/secure-server-hosting/what-is-hipaa-compliance/

Sources

1) Erik Kangas, HIPAA Compliance Checklist: What You Need to Do, LuxSci (July, 2013). Available at: http://luxsci.com/blog/hipaa-compliance-checklist-what-you-need-to-do.html.
2) HIPAA Compliance Checklist for HIV Providers Covered by HIPAA's Privacy Rule, Legal Action Center (February, 2008). Available at: http://www.lac.org/doc_library/lac/publications/HIPAA_Checklist_for_HIV_Providers-08.pdf.
3) HIS HIPAA Security Checklist, Indian Health Service. Available at: http://www.ihs.gov/hipaa/documents/ihs_hipaa_security_checklist.pdf.
4) Jason Wang, How do I become HIPAA compliant? (a checklist), TRUEVAULT (October, 2013). Available at: https://www.truevault.com/blog/how-do-i-become-hipaa-compliant.html#.U-0v_-NdXUk
5) Protecting the Privacy of Personal Health Information, HIPAA News 2010. Available at: http://hipaanews.org/checklist.htm.