HIPAA 2.5

Compliance Documents for Medical Practices

This is a list of the forms with their descriptions that are included in the Compliance Package. We recommend following the directions in the **Using These Materials** file found in the **Start Here** section. You may only need some of the documents, as this is a comprehensive package. The notations in **BOLD** at the end of some descriptions cite the part of the Rule to which the referenced document applies. **Standards** are explained in Sections II and III of the Privacy Policies and Procedures. **Addressable** versus **Required** per HHS website:

If an implementation specification is described as "required," the specification must be implemented. The concept of "addressable implementation specifications" was developed to provide covered entities additional flexibility with respect to compliance with the security standards. In meeting standards that contain addressable implementation specifications, a covered entity will do one of the following for each addressable specification: (a) implement the addressable implementation specifications; (b) implement one or more alternative security measures to accomplish the same purpose; (c) not implement either an addressable implementation specification or an alternative. The covered entity's choice must be documented. The covered entity must decide whether a given addressable implementation specification is a reasonable and appropriate security measure to apply within its particular security framework. For example, a covered entity must implement an addressable implementation specification if it is reasonable and appropriate to do so, and must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative. This decision will depend on a variety of factors, such as, among others, the entity's risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation. The decisions that a covered entity makes regarding addressable specifications must be documented in writing. The written documentation should include the factors considered as well as the results of the risk assessment on which the decision was based.

MEDICAL COMPLIANCE DOCUMENTS

Start Here

Using these Compliance Materials	**START HERE!**
Description of Compliance Documents	Lists all the forms in the document file with descriptions for their use.
Risk Assessment Tool	Walks you through the kind of risk assessment that you will need to demonstrate you've performed in order to assess potential risk exposure. **(A7 - §164.308(a)(1)(ii)(B) Required)**
Key HIPAA Terms	Glossary

Policies and Procedures

Privacy Policies and Procedures	Sample Policies and Procedures in Word format are a complete outline of what you should consider including in your practice's Policies and Procedures. Your Policies and Procedures should only include the sections of this document that are relevant for your practice. **(A1 - §164.308(a)(1)(i) Standard)**
Security Policies and Procedures	There are elements of security guidelines included in the Privacy Policies and Procedures, but these are more detailed and must be implemented separately. There are cross-references between the two. Start with these examples, then modify, add and delete to create a set of policies that match your situation. Your Policies and Procedures should only include the sections of this document that are relevant for your practice. (**PH1 - §164.310(a)(1) Standard)**
Staff Signature Page	Formatted to collect acknowledgement and signatures for the 4 key documents (Priv. & Sec. Policies & Procedures, Confidentiality Agreement, BYOD) in one document. Using this negates the need to have employees sign each document separately.
Staff Training Log on Your Policies and Procedures	Record staff training on your practice's Privacy and Security Policies and Procedures. Use the Staff Signature Page. **(A10 - §164.308(a)(1)(ii)(C) Required)**

Business Associate Agreement

Business Associate Agreements	Your practice may work with outside parties who can access PHI. They should sign a Business Associate Agreement in which they commit to protect all PHI. Remember, this contract should be modified to reflect the particular project and access to PHI each Business Associate may have or need. **(A64 - §164.308(b)(3) Required)**
Business Associate Agreement Cover Letter	Draft letter to accompany Business Associate Agreement so they understand why they have received a BAA
Business Associate Log	Use to keep track of all your Business Associates. **(A61 - §164.308(b)(1) Standard)**

Patient Rights Forms

Accounting of Disclosure Log	Helps document the disclosure of Protected Health Information about patients and prepares practice for any legal or regulatory action (including an audit) that may occur.
Authorization and Release to Use or Disclose PHI	Gives practice the right to appropriately disclose PHI about a patient, for instance, to a family member. The practice may use or disclose PHI for treatment, payment of healthcare operations without first seeking a patient’s authorization. This form also spells out the individual's rights to safeguard his or her health information.
Authorization to Use and Disclose PHI for Marketing Purposes	Use when patient agrees to allow marketing that includes his/her PHI
Request/Denial for Accounting of Disclosures	Patient uses to request that the practice or their BA inform the patient when they disclose their health information. The practice can deny this request.
Request Alternate Methods of Communication	Use when patient asks to be contacted at a different location than that on file
Request Limitations and Restrictions of PHI	The patient may want to limit who sees their PHI such as a family member. Practice can deny this request but has to specify the reason.
Request/Denial for Amendment of Records	Patient request to change or amend their own records. The practice can deny this request.
Request/Denial to Inspect and Copy	Allows access to health information in designated record. The practice can deny this request.

. . . More Patient Rights Forms

Do Not File Insurance Waiver	Patient can pay for services in cash and request that no claim be filed with the his/her insurance company. This request will only be honored if no other laws or regulations supersede this request.
Patient Complaint - Internal	Patient will complete when filing a complaint with the practice about the practice or care that they consider a HIPAA violation
Patient Complaint to HHS	If you have tried to mitigate a complaint and failed, the complainant could use this form to file a complaint with HHS.

Notice of Privacy Practices

Notice of Privacy Practices (NPP)	Describes how medical information about patients will be protected and how it may be disclosed. It also defines a contact if there is a question or concern. Provide to your patients to describe your privacy practices and post prominently in the waiting area and on your website. Remember, this is a draft and should be amended to reflect your particular practice's needs and approach to HIPAA implementation. **(PO1 -§164.316(a) Standard)**
Notice of Privacy Practices (NPP) - Simplified HHS Version	HHS has created a simplified version of the NPP that may be sufficient for your practice's needs. The same distribution rules apply as above. Remember, this is a draft and should be amended to reflect your particular practice's needs and approach to HIPAA implementation. **(PO1 -§164.316(a) Standard)**
Agreement To Receive NPP Electronically	It may be easier to reach your patients via email. By having them sign this form and filing it in their record, you can send them the NPP electronically.
Notice of Privacy Practices Log	A simple log that allows you to keep track of whom has received your Notice of Privacy Practices. Patients do not need to sign indicating they have received the NPP.

Internal Forms

Access Request Tracking Log	Used to keep track of whom has requested access to their PHI and in what stage of the process is the request
Bring Your Own Device Agreement (BYOD)	Provides policies, standards, and rules for the use of smartphones, tablets and/or other devices owned by the individual and used in your practice or for staff personal use. **(PH1 - §164.310(a)(1) Standard)**
Confidentiality Agreement with Staff	Model confidentiality language can be added to staff agreements to make them aware of their heightened responsibilities and the consequences of a breach. There is also language to make staff aware of the requirement to protect the practice's business information.
Chart Log	Log patient charts moved from and returned to the file room/stacks/cabinets
Exit Checklist	Assists with the questions and information you should make sure you cover with an exiting staff member **(A29 - §164.308(a)(3)(ii)(C) Addressable)**
Minimum Necessary Information Worksheet	Use to outline what information person/ staff member can access
Request to Amend PHI Tracking Log	Use to track in what stage of the process it is when patients ask to modify an entry in their medical record
Social Media Policy	Provides employees with policies and guidelines regarding conduct on various social media platforms.

Breach Forms

Incident & Breach Policy	Outlines what you should consider including in your practice's Incident and Breach Policy **(A29 - §164.308(a)(3)(ii)(C) Addressable)**
Incident and Breach Log	Document all Incidents and Breaches that occur within the practice
Breach Analysis Worksheet	Helps you organize your Breach response **(A47 - §164.308(a)(6)(ii) Required)**
HIPAA Complaint Form – Initial Complaint	Provides a documented record if a patient wishes to file a complaint with your practice. Your Policies and Procedures should outline your action(s) and response.
HIPAA Complaint Form – HHS	If you have tried to mitigate a complaint and failed, the complainant could use this form to file a complaint with HHS.

. . . More Breach Forms

Example of Press Treatment of Breach	The kind of article typically seen when there has been a Breach. It is included to help you understand what the negative press exposure can be.
Repairing Your Reputation Post Breach	Article with suggestions for how to deal with your patients and the press after a Breach
Sample Letter to Patients Affected by Breach	Provides a framework for the letter you are required to send to patient whose PHI, financial identity or other means of personal identification may have been compromised. If fewer that 500 people affected, a letter is sufficient. Remember, the US Department of Health and Human Services must be notified immediately if more than 500 patients are affected.
Sample Press Release when 500+ Affected by Release of PHI	When a breach affects 500 or more patients, a press release must be issued to a prominent media outlet serving those in the affected geographic area(s). HHS must also be notified immediately.

Security and Reference Documents

Back Up and Data Recover Plan	Establishes expectations for back up and restoration of data to share with your IT staff or Business Associate. It is also found in the Security Policies and Procedures, Addendum C. Use whichever is most convenient for you. **(T11 - §164.312(a)(2)(ii) Required)**
Disaster Recovery Plan	You will need to have a Disaster Recovery Plan as a part of your Security Plan - this document is a sample to use for that purpose. It is also found in the Security Policies and Procedures, Addendum D. Use whichever is most convenient for you. **(A50 - §164.308(a)(7)(i) Standard)**
Employee Access Request Form	Use to track requests for access to PHI-sensitive data storage. **(PH15 - §164.310(a)(2)(iii) Addressable)**
Encryption Guidelines	The HIPAA Omnibus ruling requires encryption. If there is a Breach of unencrypted PHI, the notification actions you must take are much more elaborate. This document outlines specific encryption tools and technologies for data stored in an electronic format or emailed. **(T20 - §164.312(a)(2)(iv) Addressable)**
Risk Management Policy	Provides structure for the organization's evaluation, prioritization and implementation of risk-reducing security measures
Risk Analysis Log	When there has been a breach, you need to document the event in order to determine if the company Policies and Procedures need to change.

Change Control Logs for Security

Annual Security Review	Document your annual review of the company's Security elements for possible audit with a personal reminder of the importance of the task. (**A4 - §164.308(a)(1)(ii)(A) Required)**
Application Change Control Log	Use for application or software changes to help ensure completeness and accuracy
Database Change Control Log	If you have a database, log all inserts, updates and deletes of database changes in order to verify what data was modified and who made the modifications. **(PH17 - §164.310(a)(2)(iv) Addressable)**
File Room Log	If your company still keeps paper files, track when they are moved from and returned to the file room
Incident Disaster Log	Use to record all incident disasters or situations at or within the practice
Inventory of Information Assets	Think of an information asset as any software, hardware, network or computing component that creates, receives, maintains or transmits ePHI. This includes removable devices, mobile devices and remote access points. **(PH1 - §164.310(a)(1) Standard)**
Maintenance Log	Track all repairs and modifications to the physical security of the facility. (**PH17 - §164.310(a)(2)(iv) Addressable)**
Media Sanitization	Use for recording the final disposition of media to ensure proper accountability of equipment and inventory control. (**PH35 - §164.310(d)(2)(ii) Required)**
Network Changes	Use to document all network changes, such as printer additions and deletions
Operating System Changes Audit	Use to log IT security programs and systems; helps monitor accountability, reconstruction, intrusion and problem detection **(T4 - §164.312(a)(1) Standard)**
Physical Entry Access	Track changes to access (lost keys, new keys) to your physical space. (**PH8 - §164.310(a)(2)(ii) Addressable)**
Removable & Mobile Device Management Log	Use to document all (company-owned or personal) removable and mobile devices, the users and what systems access are available for each device and/or user, including, but not limited to: iPads, flash drives, smartphones, etc. **(PH1 - §164.310(a)(1) Standard)**
Responsibility Change Log	Document changes to user rights access. **(A24 - §164.308(a)(3)(ii)(A) Addressable)**

. . . More Change Control Logs for Security

System Access	Use to identify software/programs attached to each department. **(A24 - §164.308(a)(3)(ii)(A) Addressable)**
Workstation Log	Identify and track your workstations and who has access to them. **(PH21 - §164.310(b) Standard)**

Training

HIPAA Quick-Guide	Review and overview of Privacy and HIPAA Omnibus Ruling of 2013
Policies & Procedures Quiz	Required in addition to the training on the Law and can be modified to assess staff understanding of your practice's Policies and Procedures
Training Log	Document which staff has completed training on your Policies and Procedures. This log is important if there is an audit of your practice.