HIPAA 2.5

Compliance Documents for Employers

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.

EMPLOYER COMPLIANCE DOCUMENTS

Start Here

Using These Compliance Materials	START HERE!
Description of Compliance Documents	List of all the forms in the Document file with descriptions for their use.
Risk Assessment Tool	Walks you through the kind of risk analysis that you will need to demonstrate you've performed in order to assess your employer's 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 might want to consider including in your company's Policies and Procedures. However, for your purposes, you may only need a small portion of these. Your Policies and Procedures should only include the sections of this document that are relevant for your company. **(A1 - §164.308(a)(1)(i) Standard)**
Security Policies and Procedures	There are elements of these 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 company. **(PH1 - §164.310(a)(1) Standard)**
Policies and Procedures Updates	Document when you update P&P
Employee 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 company'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 company may work with outside parties who can access employee 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 track the status of your BA Agreements **(A61 - §164.308(b)(1) Standard)**

Forms for Employees

Confidentiality Agreement with Company's Employees	This model confidentiality language can be added to employee agreements to make them aware of their heightened responsibilities and the consequences of Privacy and Security Breaches. There is also language to make employees aware of the requirement to protect company business information. **(A9 - §164.308(a)(1)(ii)(C) Required)**
Social Media Policy	Provides employees with policies and guidelines regarding conduct on various social media platforms.
Bring Your Own Device Agreement (BYOD)	Provides policies, standards and rules of behavior for the use of smartphones, tablets and/or other devices owned by company employees personally **(PH1 - §164.310(a)(1) Standard)**
Authorization and Release Form to Disclose Health Information/Revocation	Gives employer the right to appropriately disclose PHI in order to file health claims. It spells out the individual's rights to safeguard his or her health information. This document also can be used to revoke permission to disclose health information. Note: You do not have to have this form completed every time, but only when it will be necessary to share with a third party when they require an authorization.
Employee Complaint Form	Employees have the right to file a complaint with the company as well as with the Office of Civil Rights when they feel their rights under the HIPAA Privacy Rule have been violated. It is in your best interest to take all complaints seriously and document all employee complaints.

. . . More Forms for Employees

Exit Checklist	Assists with the questions and information you should make sure to cover with an exiting employee. **(A29 - §164.308(a)(3)(ii)(C) Addressable)**
Request for Alternative Methods of Communication	Employees may designate where they want to be contacted about anything relating to their PHI.
Request/Denial Limitations and Restrictions of PHI	Employee may want to limit who sees their PHI. Employer can deny this request.
Request and Response to Inspect and Copy PHI	Employees now have the right to request access to their records and inspect and copy those records. They must provide those requests in writing. Employer can accept, or deny with good reason, employee access to inspect and copy records.

Notice of Privacy Practices

Notice of Privacy Practices (NPP)	A copy must be provided to each employee if you haven't already done so, at enrollment and then send a reminder at least every three years that the Notice is available on request, or when there is a change in your Privacy Policies and Procedures. Remember, this is a draft and should be amended to reflect your particular company'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 employer's needs. The same distribution rules apply as above. Remember, this is a draft and should be amended to reflect your particular employer's needs and approach to HIPAA implementation. **(PO1 -§164.316(a) Standard)**
Agreement To Receive NPP Electronically	It may be easier to reach your employees 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.

Internal Forms

Access Request Tracking Log	Use to keep track of whom has requested access to their PHI and in what stage of the process is the request

. . . More Internal Forms

Accounting of Disclosure Log	Helps you document the disclosure of Protected Health Information and prepares your company for any legal or regulatory action (including an audit) that may occur
Minimum Necessary Information Letter	Send to anyone who may be providing your company with PHI about an employee. It specifically requests that your company only be provided the information necessary to deal with a specific situation, rather than providing you with the employee's entire record.
Minimum Necessary Information Worksheet	Used to identify what management roles have access to specific information. Individuals should not receive access to more PHI than is necessary to do their jobs.
Notice to Others of Amendment	Everyone on the requestor's list of persons or entities to be notified of an amendment of PHI should receive the same notification.
Request for Amendment of PHI	Employee request to change or amend their own records
Request to Amend PHI Tracking Log	Track when and who requests amendment to PHI
Requestor's List of Persons to be Notified	When an amendment is made to an employee's PHI, anyone who has prior records will need to update them. The employee making the request should provide you with a written list of persons to be notified of the amendment.
Responsibility Change Log	Document changes to user rights access. **(A24 - §164.308(a)(3)(ii)(A) Addressable)**

Breach Forms

Incident and Breach Policy	Outlines what you should consider including in your company's policy. **(A29 - §164.308(a)(3)(ii)(C) Addressable)**
Incident and Breach Log	Document all Incidents and Breaches that occur within the company
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 an individual wishes to file a complaint with your office. 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.
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.

. . . More Breach Forms

Repairing Your Reputation Post Breach	Article with suggestions for how to deal with your employees and the press after a Breach
Sample Letter to Person Affected by Breach	Provides a framework for the letter you are required to send to someone whose PHI, financial identity or other means of personal identification may have been compromised. If fewer that 500 people are affect by the release of information, a letter is sufficient. Remember, the United States Department of Health and Human Services must be notified immediately if more than 500 individuals are affected.
Sample Press Release when 500+ Affected by Release of PHI	When a breach affects 500 or more employees, a press release must be issued to a prominent media outlet serving those in the affected geographic area(s). HHS must be notified immediately.

Security and Reference Documents

Back Up and Data Recovery 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	Sample policy related to incident tracking and handling for your company to adopt. **(A5 - §164.308(a)(1)(ii)(B) Required)**
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 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 company
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 and Mobile Device	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)
Workstations Log	Identify and track your workstations and who has access to them. (PH21 - §164.310(b) Standard)