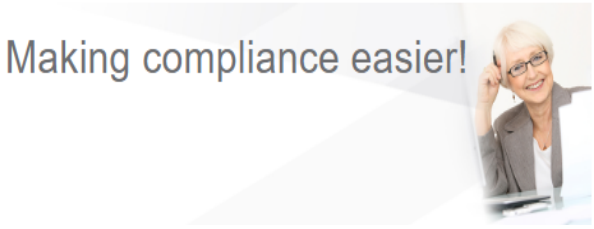
HIPAA Survival Guide



HSG Subscription Plan Checklist & Frameworks Datasheet

Table of Contents

Introduction

Our HIPAA checklists and Frameworks provide you with step-by-step guidance regarding the "big concepts" contained within the Rules. For example, our Privacy Rule and Security Rule checklists provide for each requirement of the respective Rules: (1) a policy; (2) a suggested set of processes that underpin each policy; and (3) suggested tracking mechanisms that capture process results.

Our Frameworks do the same in a slightly different fashion. For example, our Breach Notification Framework walks you through the process of determining when Breach Notification is triggered, and the content required to notify. It also provides the time of notification.

Checklists

As discussed below our Subscription Plan delivers the following Checklists: (1) Privacy Rule; Security Rule; and (3) Cloud, Social Media & Mobile.

Overview

 This begs the question, what do we mean by a checklist, and more specifically in this context, a legal/compliance checklist? The short answer is that it is a way to "attack" problems or issues. Checklists have been widely adopted across industries (e.g. aviation) and are now becoming acclaimed in the practice of medicine. Our Checklists combine reusable solutions with analysis patterns, research, useful organizational techniques, and specific examples of successful approaches; it is like having your own personal library, which can be tailored specifically for your experience and organization.

Our Checklists are intended to provide guidance, including suggested ***policies, processes, and tracking mechanisms*** that enable you to make sense out of this new terrain. They are intended as a knowledge transfer vehicle to allow you to derive the HIPAA compliance solution that works best within your organization. Our Checklists will "walk you through" the relevant statutory/regulatory sections of the HIPAA Rules, highlighting the policies, processes and tracking mechanisms required at a granular level.

What is a Policy

The word "policy" can be used in so many ways that it bears some exploration, especially regarding HIPAA regulatory compliance. We often talk of "developing a policy," or of "implementing a policy" or "carrying out a policy." For example, 45 CFR §164.530 (i)(1)[3] states as follows:

> **Standard: Policies and procedures**. A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this subpart and subpart D of this part.

Notice that the standard above makes a distinction between policies versus procedures. In general, think of a "policy" as a purposeful set of decisions or actions usually in response to a problem that has arisen. From a compliance perspective, a policy is a set of statements, including decisions and actions regarding what an organization intends to do in order to meet its regulatory requirements (e.g. see our Breach Notification Policy). A policy indicates ***what*** an organization intends to do and is often used as a communications vehicle of that intent.

What is a Process?

A process is a repeatable series of steps that are accomplished over time. From a HIPAA regulatory compliance perspective, processes are how policies get implemented. Policies without processes are nothing more than empty promises and will not prevent serious compliance liability. HHS will require evidence of policies and processes. For example, the Privacy Rule in section 45 CFR §164.530 (b)(1) states the training requirement as follows:

> **Standard: Training.** A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart

and subpart D of this part, as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity.

The requirement expressly states that the training must cover both your organization's policies with respect to the Privacy Rule and your underlying processes. Notice that nothing in the standard indicates how the required training should be carried out. The training standard has a corresponding implementation specification that reads as follows:

> (2) **Implementation specification: Training.**
>
> (i) A covered entity must provide training that meets the requirements of paragraph (b)(1) of this section, as follows:
>
> (A) To each member of the covered entity's workforce by no later than the compliance date for the covered entity;
>
> (B) Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and
>
> (C) To each member of the covered entity's workforce whose functions are affected by a material change in the policies or procedures required by this subpart or subpart D of this part, within a reasonable period of time after the material change becomes effective in accordance with paragraph (i) of this section.
>
> (ii) A covered entity must document that the training as described in paragraph (b)(2)(i) of this section has been provided, as required by paragraph (j) of this section.

Again, although the implementation specification speaks to when training is required and the fact that it must be documented, it does not prescribe how your training should be conducted. Your *training process* is the vehicle used to specify, with a degree of detail and rigor, how your training will be carried out (e.g. formal classroom training, audited video training, self-help training, etc.).

What is a Tracking Mechanism?

 A tracking mechanism is a way to keep track of process results. For example, QuickBooks is a tracking mechanism for accounting data and processes. You must be able to track the results of your compliance processes if you hope to provide ***Visible Demonstrable Evidence*** ("VDE") that you are meeting regulatory requirements. Your HIPAA training policy indicates your compliance training intentions; your training process is how you go about fulfilling those intentions; and your tracking mechanism must capture the results of your training process (i.e. how well you did in meeting your intentions). HHS will likely want to see evidence of all three components, ***but if you cannot show process results, then your entire training initiative is likely to be suspect***.

There are many compliance processes that require tracking within the Privacy rule including, but not limited to the following:

1. patient privacy notice provisioning process;
2. patient authorization process;
3. patient restriction request process;
4. patient complaint process;
5. patient record access request process; and
6. workforce training process.

This "short list" of processes is not exhaustive but rather illustrative of the scope and magnitude of what needs to be tracked in order to move your organization along the compliance continuum toward full compliance.

How should your compliance processes be tracked? It is no longer reasonable to track compliance processes on paper (if it ever was). You are going to need a suitable Intranet, spreadsheets, and/or HIPAA compliance software in order to track and report effectively. We recommend the latter because it is the most economically viable option, even for small covered entities and business associates

Privacy Rule Checklist

Our Privacy Rule Checklist covers all the requirements of the Privacy Rule allowing you to create ***Visible, Demonstrable, Evidence*** ("VDE") of compliance for requirements of the Rule. We also deliver a scorecard wherein you can grade your organization on its Privacy Rule Compliance.

Security Rule Checklist

Our Security Rule Checklist covers all the requirements of the Security Rule allowing you to create ***Visible, Demonstrable, Evidence*** ("VDE") of compliance for each requirement of the Rule. Like the Privacy Rule Checklist, we also provide a scorecard where you can grade your organization on its Security Rule Compliance.

Cloud, Social Media & Mobile Checklist ("CSMM")

This Cloud Social Media & Mobile Checklist ("CSMM") offers a Compliance Officer CSMM HIPAA best practices in this rapidly evolving technological and regulatory landscape. The Checklist should be viewed as an addendum to your existing HIPAA compliance program. It is a different kind of Checklist because it is derived from "first order" requirements contained in the Privacy Rule

and the Security Rule. Again, we provide a scorecard wherein you can grade your organization on its CSMM Compliance.

Frameworks

The term "Framework" means a mechanism for "attacking" a compliance problem or issue by providing direction regarding how to think through and solve a problem, based upon the experience of others. Our Compliance Frameworks differ from our Checklists in that the former take a set of requirements holistically providing the necessary guidance. For example, our Breach Notification Framework addresses the requirements of the Breach Notification Rule as a conceptual whole. This is true of our Breach Response Framework and our Contingency Framework as well. All of our Frameworks come with tools and templates that help you comply with the respective requirements.

Breach Notification Framework

Our Breach Notification Framework addresses the requirements of notification that were introduced under the HITECH Act, specifically section 13402. These requirements did not *originally* exist under HIPAA. HHS subsequently (i.e. after the promulgation of the HITECH Act) issued regulations pertaining to Breach Notification in 45 CFR 164 (Subpart D). In general, this is the universe of controlling legal authority, to be supplemented by Federal common law, as Breach Notification cases are heard by the Federal Courts. Our Breach Notification Framework addresses every requirement in 45 CFR 164 (Subpart D).

Breach Response Framework

Our Breach Response Framework provides organizations of all sizes who experience a breach, the tools to meet the requirements of various federal, state and private regulatory regimes. HIPAA is simply one regulatory regime example. After disasters that result from high profile breaches, organizations are starting to realize that it's not a question of "if" they will experience an attack that leads to a breach, but simply "when." Despite this realization most, C-Suite participants are at a loss as to how to proceed, given their lack of subject matter expertise, and the myriad of options available—from enhancing their cybersecurity fortifications to transferring the risk via insurance.

Contingency Framework

Our Contingency Framework provides HIPAA stakeholders with the tools to meet requirements of HIPAA's Administrative Safeguards standard §164.308(a)(7)(i) ("Contingency Standard") and its five implementation specifications ("Controls"). All five Controls fall under §164.308(a)(7)(i)(ii) as follows:

(A) **Data Backup Plan** (**Required**). Establish and implement procedures to create, retrieve and maintain exact copies of electronic protected health information ("ePHI").
(B) **Disaster Recovery Plan** (**Required**). Establish (and implement as needed) procedures to restore any loss of data.
(C) **Emergency Mode Operation Plan** (**Required**). Establish (and implement as needed) procedures to enable continuation of critical business processes for protecting the security of ePHI while operating in emergency mode.
(D) **Testing and revision procedures** (**Addressable**). Implement procedures for periodic testing and revision of contingency plans.
(E) **Applications and data criticality analysis** (**Addressable**). Assess the relative criticality of specific applications and data in support of other Contingency Plan components.

These Controls are now generally referred to as "Business Continuity" across industries and encompass much more that a mere Data Backup Plan.

Summary

The HIPAA Survival Guide provides all HIPAA requirements covered in our Checklists and Frameworks, ready for your use.