HIPAA Compliance Work Plan

6 Critical Elements for Effective Security and Privacy Policies

Compliance Helper
HIPAA Compliance Work Plan
6 Security Elements for Effective Procedures

By Rebecca Herold and Jack Anderson

Version 1.00
Revised August, 2013

Limits of Liability & Disclaimer of Warranty

The author and publisher of this eBook and the associated materials have used their best efforts in preparing this material. The author and publisher make no representations or warranties with respect to the accuracy, applicability, fitness, or completeness of the contents of this material. They disclaim any warranties expressed or implied, merchantability, or fitness for any particular purpose. The author and publisher shall in no event be held liable for any loss or other damages, including but not limited to special, incidental, consequential, or other damages. If you have any doubts about anything, the advice of a professional should be sought.

This material contains elements protected under International and Federal Copyright laws and treaties. Any unauthorized reprint or use of this material is prohibited.
About HIPAA Compliance Tools

HIPAA Compliance Tools is a medical management consultant firm that has been involved with the health care industry for approximately 10 years. It has streamlined HIPAA Compliance procedures for thousands of doctors, dentists, hospitals and clinics.

HCT offers many products and programs that have assisted healthcare organizations and employers meet their compliance and operational needs. HCT has recently combined with Compliance Helper to deliver the most effective method for compliance in the industry.

**Jack Anderson** of Compliance Helper has teamed with **Rebecca Herold**, CIPP, CISSP, CISM, CISA, FLMI, “The Privacy Professor®”, to build a cloud based solution for HIPAA HITECH Information Security and Privacy compliance.

Our Internet-based service delivers customizable policies and procedures built around international information security and privacy standards and mapped to HIPAA/HITECH and other regulatory requirements, forms, a step-by-step process which includes gap analysis, and an expert human helper to assist business associates and covered entities in attaining and maintaining information security and privacy compliance.

If you have questions please [click here](#).
Contents

About HIPAA Compliance Tools .................................................................................... 3
Introduction .................................................................................................................. 5
Special Offer ............................................................................................................... 6
1. Information Security and Privacy Program Management ................................... 7
2. Training and Awareness ....................................................................................... 8
3. Human Resources (HR) Activities .................................................................... 9
4. Organization Management ............................................................................... 10
5. Information Technology (IT) .......................................................................... 11
6. Legal ............................................................................................................... 12
7. Facilities Management and Physical Security and Safety ............................ 13
8. Audit .............................................................................................................. 14
6 Critical Elements of Information Security and Privacy Policies ..................... 15
   1. People must be aware of information security and privacy policies .......... 15
   2. Create a committee to develop information security and privacy policies .. 15
   3. Information security and privacy policies must be specific to your organization ................................................................. 16
   4. Information security and privacy policies must be readable and understandable .............................................................. 16
   5. Information security and privacy policies must be fair, reasonable, and legal. ................................................................. 16
   6. Information security and privacy policies must be enforced. .................... 16
HIPAA Program Highlights ...................................................................................... 18
**Introduction**

The following is a high-level work plan to create an information security and privacy program to meet compliance with HIPAA, HITECH and other regulatory and contractual requirements. The areas listed will vary depending upon the organization's business model, size, number of geographic locations, other applicable legal requirements, and any other unique factors. Each organization should use this as a starting point and change appropriately for its own unique business situation.

Do you realize the average HIPAA Violation is over $50,000 and can include up to a year in prison? Violations are becoming more prevalent and the chance of a random audit is increasing monthly as we approach the new health care laws passed under the current administration.

Today is a perfect time to get your facility compliant and stay ahead of the ever changing laws regarding HIPAA and HITECH Act. Our goal is to keep you informed with monthly law changes, form updates and new violations.
Special Offer

“Are you prepared to spend hundreds of hours filtering through all the changing HIPAA/HITECH Omnibus rules about to come into effect? Do you have all the needed forms? Is your office out of Compliance? Do you know if it is or not? We have the solution.”

www.hipaacompliance.org

We have turned HIPAA LAW into a cloud based OFFICE PROCEDURE. Within 30 days, your facility will be a 100% compliant and stay compliant with the help of our trademarked "Compliance Meter".

Due to drastically changing health care laws and Omnibus laws coming in September we have designed an incredible membership offer. Get our entire HIPAA Office System and all the cost and time saving features for as low as $497.00 and $47.00 per month. Please check our plans to find the one that's right for your facility.

Special Offer: Enter "HIPAA13" in the coupon code box at checkout and receive an additional 5% off the initiation price.
1. Information Security and Privacy Program Management

a. Obtain Executive Management Support: An information security and privacy compliance program cannot be successful without the clear and strong support of executive management. Make sure your CEO, or equivalent, position is willing to provide strong support for the information security and privacy program.


c. Enterprise Wide Responsibilities. Document the responsibilities for key information security and privacy responsibilities throughout the organization.

d. Identify and Inventory Personal Information. Document where personal information, including Protected Health Information (PHI) is located and maintain this inventory.


f. Information Security and Privacy Risk Assessment. Perform an information security and privacy risk assessment, including gap analysis for HIPAA and HITECH compliance requirements.

g. Information Security and Privacy Policies. Formally document information security and privacy policies to address the identified risks, in addition for those necessary to meet HIPAA, HITECH and other applicable legal requirements.

h. Information Security and Privacy Procedures and Processes. Formally document the types of procedures and processes necessary throughout the organization to support the policies.

i. Access, Authorization, Process, and Technical Controls. Establish and maintain technical controls and settings to support the procedures and compliance.

j. Passwords. One of the most common vulnerabilities in an information security and privacy program is allowing the use of bad passwords. Make sure your program establishes requirements for strong passwords that cannot be easily discovered, and that must be changed under appropriate conditions.

k. Information Security and Privacy Education. People are the weakest link for security and privacy protections. HIPAA, HITECH and dozens of other legal requirements exist for providing regular training and ongoing awareness communications. Assign information security and privacy education responsibilities, and ensure strong executive support for the activities.
2. Training and Awareness

a. Training and Awareness Plan. Document a formal plan for providing regular training and ongoing awareness communications for information security and privacy.

b. Training Content. Identify and contract, purchase or create the training content to support the plan.

c. Awareness Content. Identify and contract, purchase or create the awareness content, and any associated activities materials, to support the plan.
3. Human Resources (HR) Activities

a. HR Security & Privacy Responsibility. Formally assign responsibilities to a position or team within HR for ensuring information security and privacy compliance activities in that area.

b. HR Information Security and Privacy Procedures. Create procedures for HR staff to follow, based upon their assigned work responsibilities and activities, to support compliance with the organization’s information security and privacy policies.

c. HR Information Security and Privacy Training. Ensure HR staff receive training and awareness specific to their unique work activities and job responsibilities to support compliance with the policies, procedures and the types of information, of all forms, that they handle.
4. Organization Management

a. Organization Management Security & Privacy Responsibility. Formally assign responsibilities to the Organization Management within each of the business units for ensuring information security and privacy compliance activities in those areas.

b. Organization Management Information Security and Privacy Procedures. Create procedures for the Organization Management and staff within each of the business units to follow, based upon their assigned work responsibilities and activities, to support compliance with the organization’s information security and privacy policies.

c. Organization Management Information Security and Privacy Training. Ensure Organization Management and their staff receive training and awareness specific to their unique work activities and job responsibilities to support compliance with the policies, procedures and the types of information, of all forms, that they handle.
5. Information Technology (IT)

a. IT Security & Privacy Responsibility. Formally assign responsibilities to a position or team within IT for ensuring information security and privacy compliance activities in that area.

b. IT Information Security and Privacy Procedures. Create procedures for IT staff to follow, based upon their assigned work responsibilities and activities, to support compliance with the organization’s information security and privacy policies.

c. IT Information Security and Privacy Training. Ensure IT staff receive training and awareness specific to their unique work activities and job responsibilities to support compliance with the policies, procedures and the types of information, of all forms, that they handle.
6. Legal

a. Legal Counsel Security & Privacy Responsibility. Formally assign responsibilities to a position or team within the Legal Department (or equivalent) for ensuring information security and privacy compliance activities in that area.

b. Legal Counsel Information Security and Privacy Procedures. Create procedures for the Legal Department (or equivalent) staff to follow, based upon their assigned work responsibilities and activities, to support compliance with the organization’s information security and privacy policies.

c. Legal Counsel Information Security and Privacy Training. Ensure the Legal Department (or equivalent) staff receive training and awareness specific to their unique work activities and job responsibilities to support compliance with the policies, procedures and the types of information, of all forms, that they handle.
7. Facilities Management and Physical Security and Safety

a. Facilities Management Information Security & Privacy Responsibility. Formally assign responsibilities to a position or team within the Facilities Management (or equivalent) department for ensuring information security and privacy compliance activities in that area.

b. Facilities Management Information Security and Privacy Procedures. Create procedures for the Facilities Management (or equivalent) department staff to follow, based upon their assigned work responsibilities and activities, to support compliance with the organizations information security and privacy policies.

c. Facilities Management Information Security and Privacy Training. Ensure the Facilities Management (or equivalent) department staff receive training and awareness specific to their unique work activities and job responsibilities to support compliance with the policies, procedures and the types of information, of all forms, that they handle.
8. Audit

a. Audit Security & Privacy Responsibility. Formally assign responsibilities to a position or team within the Audit department for ensuring information security and privacy compliance activities in that area.

b. Audit Information Security and Privacy Procedures. Create procedures for the Audit department staff to follow, based upon their assigned work responsibilities and activities, to support compliance with the organizations information security and privacy policies.

c. Audit Information Security and Privacy Training. Ensure the Audit department staff receive training and awareness specific to their unique work activities and job responsibilities to support compliance with the policies, procedures and the types of information, of all forms, that they handle.
6 Critical Elements of Information Security and Privacy Policies

Too commonly, information security and privacy policies either do not exist or are not enforced in today's healthcare environments. The first major hurdle that must be addressed to ensure information security and privacy policies are implemented and managed properly is that of upper management support. Even though HIPAA compliance is federal law, healthcare organizations still need buy-in from their upper management if policies are to be successfully developed and embraced. If you have reached the point of communicating the value and requirements of HIPAA to upper management and are already working toward compliance, this should not be a major issue for you as it is in other nonregulated environments.

Beyond upper management buy-in, there are six other critical factors that will determine whether or not security policies are effective. In no particular order, these factors are as follows:

1. People must be aware of information security and privacy policies.

Perhaps the greatest mistake in information security and privacy policies management is that organizations create them and then put them on a shelf without making anyone aware of them. The organization would be just as well off without information security and privacy policies in this case. Refer to Chapter 24 for details on the best ways to get the word on your security policies out to everyone involved.

2. Create a committee to develop information security and privacy policies.

You do not want to develop information security and privacy policies all by yourself. This could be misconstrued as one-sided or biased, and this is certainly not the position any one individual wants to be in. Additionally, you must consider the expertise of your business leaders to ensure the policies you create are feasible. Get other people involved. It is preferable to get HR, Legal, facilities management, IT and applicable business unit representatives to help with this.
3. **Information security and privacy policies must be specific to your organization.**

You cannot simply buy an information security and privacy policies book or download sample policies off the Internet and apply them verbatim to your immediate needs. Do not get us wrong; these policies are a *great* place to start -- they can definitely save you a lot of time, money, and effort. Plus they help you to ensure you are covering all the topics you need to cover. Just remember to tailor these policies to your organization's specific needs and requirements. In fact, try to relate your information security policies to your privacy policies whenever possible. Tailoring these policies should not take a lot of work, and it is absolutely necessary to make sure your information systems and protected health information (PHI) are properly protected in your particular environment.

4. **Information security and privacy policies must be readable and understandable.**

Make sure you know your intended audience before you start writing your policies. Regardless of who will be reading them, use the legal and technical jargon sparingly. All of your employees, independent of their knowledge and intellect, need to be able to read any and all of your organization's information security and privacy policies and completely understand them. This is not just an education or awareness issue. It also depends on how well written the policies are in the first place.

5. **Information security and privacy policies must be fair, reasonable, and legal.**

Put yourself in your end users' position. Do the policies seem fair and reasonable in order to get the job done? If security policies are not fair and reasonable, people will break them, and that is the last thing anyone needs to have happen with their HIPAA policies. It really is possible to balance security, HIPAA compliance, and convenience. Make sure your organization is doing that. Also, do not forget to run your security policies by your legal counsel before you publish them to make sure they are legal from an HR and employees' rights perspective.

6. **Information security and privacy policies must be enforced.**

It is not enough for information security and privacy policies to be fair, reasonable, in compliance with applicable laws and regulations, and legal. They must also be enforced within the organization for all users, including upper management. Sure, HIPAA mandates information security and privacy policies, but similar to the awareness issue discussed previously, if policies are not enforced by the policies committee (if you have one), HIPAA Officer(s), or upper management, then it is probably not worth the time, money, and effort to develop
them in the first place. Not only this, but HIPAA, and many other laws and regulations, also mandates sanction policies and requires documentation that you are actually enforcing the policies.
HIPAA Program Highlights

Features Included:

- 54 policies of which 23 are Privacy
- 76 procedures of which 23 are Privacy
- 73 customized forms, with PDF, Word Doc and Excel format
- Personal Helper to assist in all compliance projects and forms
- Simple step-by-step process monitored by helper
- Compliance Meter™ to insure compliance is maintained
- Monthly task lists and documentation

Monthly Membership Benefits:

- Automatic Law Upgrades including form revisions at no extra cost
- Customer Support including access to a Helper to answer questions
- Monthly newsletter reporting new legislation and recent violations
- Continuous updates on Obama Care sent via cloud as they occur
- No renewal fees, simply pay the membership and never lose benefits
- Customer support in the event of a HIPAA or HITECH Audit

Why you need this program:

- Saves research hours trying to keep up with law and form updates
- Saves money purchasing forms and upgrading laws and procedures
- Provides staff with super quick and easy reference materials & forms
- Removes all uncertainty and allows staff and Drs. to spend time on patients
- Protects clients data and provides insurance coverage for violations

100% Money back Guarantee if not totally satisfied

Take me there www.hipaacompliance.org