



HIPAA Implementation

Jeffrey P. Back

What is HIPAA?

In our instant, electronic age, sensitive information about a person's physical and mental health will almost certainly be found in electronic data files. Medical records may be seen by strangers who work in health care, the insurance industry, and a host of businesses associated with healthcare organizations. HIPAA--perhaps one of the most feared acronyms in the healthcare industry today sets the standard for privacy in this electronic age.

HIPAA is the United States **H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct of 1996, also referred to as Public Law 104-191 and the Kennedy-Kassebaum Bill. The legislation was passed by Congress and signed into law in August 1996.

There are five sections to the act; however we will only concern ourselves with: HIPAA Title II, which includes an administrative simplification section that is designed to provide standardization of healthcare-related information systems. Specifically, we will explore the Administrative Simplification section (Subtitle F).

The Administrative Simplification section has the following purposes:

- To protect and enhance consumer rights by providing adequate access to their health information and requiring those entities who are in possession of that information to ensure that it is protected from inappropriate use.
- To improve the efficiency and effectiveness of healthcare delivery by creating a standard for privacy protection

Within the Administrative Simplification section, there are four sub-sections that mandate the privacy and security of personal and confidential healthcare information. Going forward, use of the term HIPAA in this book will focus on this specific section.

Who must comply with HIPAA?

The HIPAA Privacy Rule pertains to three categories of Covered Entities (CEs) - healthcare providers, health plans, and health care clearinghouses. Essentially the entire healthcare industry is affected by the law, from the one-physician practice to the largest health insurer.

Covered Entities

1. *Healthcare providers*: Can be an individual, a group or an organization and includes doctors, hospitals, staff involved in patient treatment, laboratories, pharmacists, dentists, and many others that provide medical, dental, and mental health care or treatment. In short, a provider is almost any individual, group or organization in the business of providing health care that is licensed or regulated by the states.

2. *Health plans:* Can be any organization that pays for the cost of medical care. Including: health insurance companies, HMOs (health maintenance organizations), group health plans sponsored by employers, Medicare and Medicaid, and virtually any other company or arrangement that pays for health care. Note: Health plans do not include workers' compensation programs, property and casualty insurance or disability insurance programs.
3. *Healthcare clearinghouses:* Can be any number of organizations that work as a go-between for health care providers and health plans. Examples include: medical billing services, value-added networks, and consulting companies.

Are You a Covered Healthcare Provider?

It is important to determine if the activities and functions that are performed within your organization are covered healthcare functions under the HIPAA regulations. Therefore, you must first determine whether your organization performs activities or functions that meet the definition of a covered entity (CE). Use Exhibit 1 to make that determination.

Note: A covered transaction is a transmission of information between two parties to carry out a financial or administrative activity related to health care. It includes information transmissions such as: healthcare claims/encounters, healthcare payment/remittance advice, coordination of benefits, healthcare claim status, enrollment/disenrollment in a health plan, eligibility for a health plan, health plan premium payments, referral certification and authorization, first report of injury, health claims attachments, and any other transactions that the federal HHS Secretary may prescribe by regulation.

Minimally, the functions performed at the lowest levels of your organization should be considered when answering questions asked in Exhibit 1.

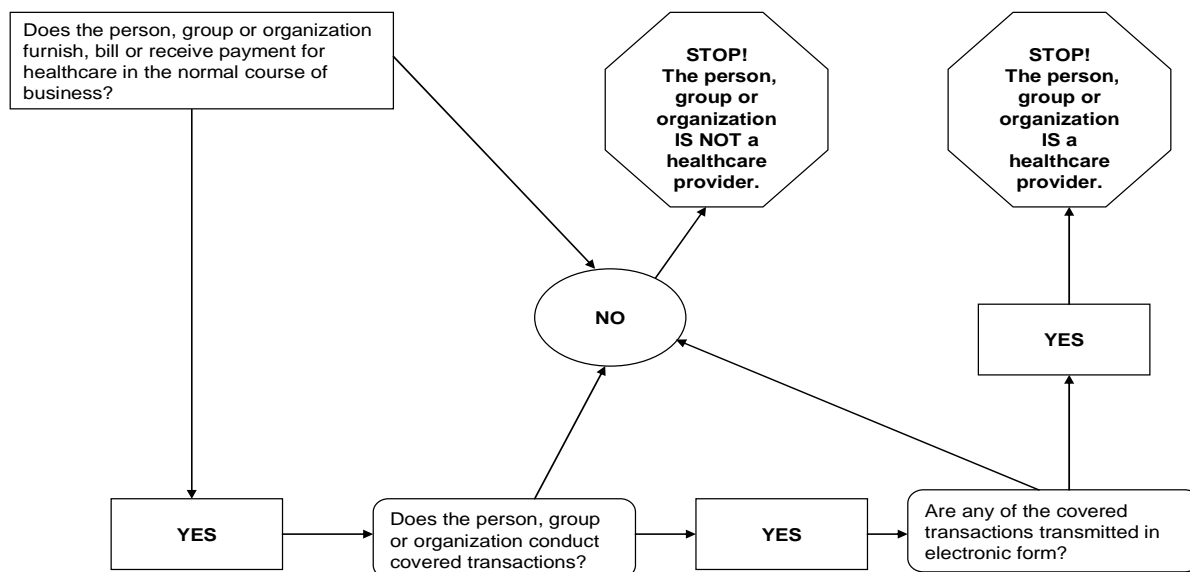


Exhibit 1. Covered Entity-Healthcare Provider Decision Flowchart

If you determine from Exhibit 1 that no part of your organization performs an activity or function that is covered by the HIPAA regulations, please note that there could still be an indirect impact to your organization if it performs any healthcare functions or activities on behalf of another covered entity.

OK, so you're a covered entity, now what?

You will now need to determine potential gaps between how you currently operate and how you will be required to operate to comply with HIPAA.

HIPAA Implementation

Implementation Concerns

Most organizations don't realize the scope of HIPAA and the steps that are required in order to comply with the law. In fact, many healthcare providers erroneously believe their organizations are HIPAA compliant just by providing each patient with a NPP (Notice of Privacy Practices).

The Compliance Model

The Compliance Model is an overall approach for addressing HIPAA as an organizational initiative. This approach can be used to track and manage all aspects of the detailed implementation of HIPAA Privacy Compliance.

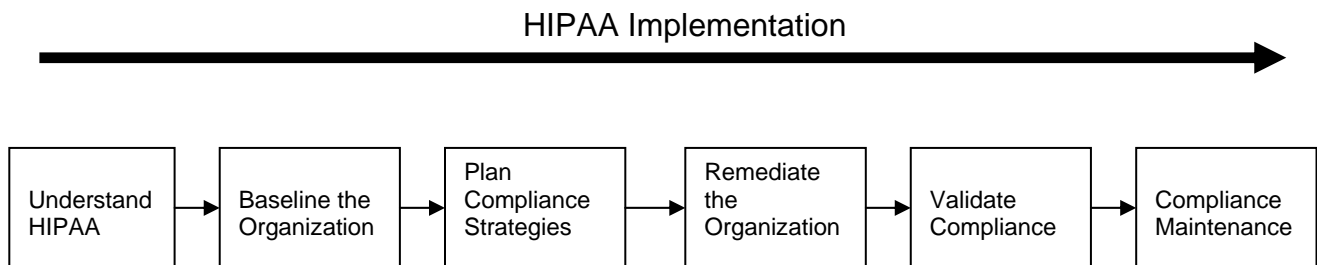


Exhibit 2. Compliance Model

Exhibit 2 is a visual representation of the 6 steps in compliance leading to successful implementation of HIPAA.

Step 1: Understand HIPAA

Activities

1. Read, understand and interpret the HIPAA regulations
2. Familiarize yourself with the compliance timelines and penalties
3. Conduct awareness training for pertinent employees
4. Develop a budgetary estimate to address HIPAA and seek commitment of funding
5. Determine who will manage the implementation
6. Establish a steering committee to oversee and guide the HIPAA effort
7. Organize a team of people to track and manage the HIPAA activities
8. Develop a strategic plan so that everyone in the organization understands the mission, goals, and objectives of the effort
9. Confirm your scope and establish your due diligence documentation method and repository
10. Develop initiative-level roles and responsibilities so that each major component of the organization knows who is doing what in the effort
11. Develop detailed work plans for at least the next phase of your effort and a master plan for the implementation
12. Analyze the HIPAA regulations against existing organization specific rules, directives, enterprise policies, etc.
13. Analyze the HIPAA regulations against potentially preemptive, or conflicting State and Federal law

Step 2: Baseline the Organization

Activities

1. Identify privacy and security officers
2. Develop an assessment method (may be a different method for each regulation area)
3. Conduct assessment activities
4. Identify your business associates and electronic trading partners
5. Document potential impacts (gap analysis)
6. Refine your budget estimates

Step 3: Plan Compliance Strategies

Activities

1. Determine what needs to be done to close the gaps
2. Document your business compliance strategy
3. Document your technical compliance strategy
4. Refine your budget estimates as necessary
5. Organize and/or recruit the staff necessary to close the gaps

Step 4: Remediate the Organization

Activities

1. Conduct appropriate levels of training for implementation staff as well as designated privacy and security officers
2. Establish/amend formal trading partner agreements and business associate contracts as necessary
3. Modify (remediate) business processes, business application systems, and technical infrastructure as necessary to comply
4. Test and/or pilot modifications
5. Conduct training relating to modifications or compliance issues
6. Implement/install changes
7. Transition the maintenance of new processes and/or products to the responsible parties

Step 5: Validate Compliance

Activities

1. Develop and deploy self-verification tools and/or techniques that can be used by sub-sections of the organization to verify that they have met the requirements of HIPAA
2. Determine whether independent validation and verification techniques will be used in any of the regulation areas
3. Solicit external validation and verification assistance as necessary

Step 6: Compliance Maintenance

Activities

1. Develop and implement an ongoing compliance training programs for privacy officers, security officers, new employees, etc.
2. Determine whether an ongoing HIPAA compliance office is necessary and establish one if necessary
3. Develop and implement an audit program to ensure ongoing compliance
4. Establish change management processes so that you are prepared to deal with future changes in the HIPAA law or to individual regulation areas

Conclusion

As you can see, your work just begins once you have determined that you are a covered entity under HIPAA. There is a great deal of effort required in both implementing HIPAA as well as maintaining compliance. In addition, HIPAA requirements do not have a termination date and noncompliance with the regulations at any time will result in strict penalties.