HIPAA Compliance Guide

HIPAA Compliance for Covered Entities

Who Must Comply with HIPAA?

Covered Entities (CEs)

Covered Entities must comply with *all* of HIPAA's requirements. CEs include:

- ❑ Health Care Providers – Medical practices, doctors, clinics, hospitals, nursing homes, dentists, psychologists, psychiatrists, chiropractors, pharmacies, etc.
- ❑ Health Plans – Health insurance companies, HMOs, company health plans, some government health programs.
- ❑ Clearinghouses – Entities that process HIPAA-related transactions from non-standard formats into standard formats, and vice versa.

Business Associates (BAs)

BAs must comply with *most* of HIPAA's requirements. BAs are people or companies (not members of a CEs workforce) who provide services to CEs involving the use or disclosure of individually identifiable health data.

- ❑ BA Activities Include: claims processing, data analysis, utilization review, and billing.
- ❑ BA Services Include: legal, actuarial, accounting, courier, consulting, data aggregation, management, administrative, accreditation, or financial services, storage, and shredding.

What Must a Covered Entity Do to Comply with HIPAA?

Since most Covered Entities (CEs) don't have a HIPAA expert in-house, HIPAA compliance begins with education. Before making any compliance efforts, you must first learn what HIPAA is all about, and what is required of your entity. HIPAA contains several sections, called "Rules", which apply to Covered Entities. Our focus here is on HIPAA's Privacy and Security Rules, as these are the two areas that require the most work. These are also the two areas where the risks of fines and other damages are highest.

In February, 2010, HIPAA was amended and expanded by the HITECH Act. In 2013, HIPAA was expanded once again with the HIPAA Final Rule. With that expansion, CEs have much to do in order to be fully compliant. When we speak of HIPAA and HIPAA compliance today, HITECH and the Final Rule are both included, as both are now an integral part of the HIPAA Regulations.

HIPAA compliance requires a Risk Analysis, designed to determine what sorts of "Protected Health Information" (PHI) are received, stored, used and transmitted by an entity. The Risk Analysis analyzes and quantifies the degree of risk posed by each category of PHI. It also looks at the degree of 'attractiveness' various types of PHI have to criminals, who seek patient data to commit identity theft, fraud, and other crimes. The Risk Analysis also helps guide several other compliance steps.

Covered Entities must develop a set of Policies and Procedures (P&Ps) required by HIPAA's Privacy and Security Rules. These P&Ps then govern the entity's operations regarding the privacy and security of patient data, and inform the workforce of the rules and boundaries related to the safe handling and protection of PHI. A complete set of HIPAA-related Forms should be developed as well, to assist in implementing HIPAA requirements such as PHI uses and disclosures, patients' rights, complaints, etc.

The next major compliance step required of all Covered Entities is providing appropriate training to the workforce. All workforce members must be trained, including full-time, part-time, non-paid workers, and volunteers. HIPAA requires evidence of training to be retained for a minimum of six (6) years from the last training date.

Every Covered Entity's I.T. staff will have to implement a variety of Data Safeguards (Administrative, Technical, and Physical), that coordinate with the various Policies, Procedures, and other requirements in HIPAA's Privacy and Security Rules.

Covered Entities will also have to assign someone to be their "HIPAA Officer", sometimes called the "Privacy Officer" or "Compliance Officer". This person should be highly trained on HIPAA, as they will be responsible for overall HIPAA compliance, managing the entity's Business Associates, handling and resolving complaints, and responding to any enforcement actions raised against the entity.

HITECH and the Final Rule dramatically raised the penalties for HIPAA violations to a new high of $50,000 per violation and $1.5 Million annual maximum per violator. And Breach Notification requires patients to be notified in most situations when their records have been lost, stolen or otherwise compromised. For all these reasons, it's more important than ever to learn what must be learned, and do what must be done, to be fully compliant with HIPAA.

What Does "Compliance" Specifically Require for Covered Entities?

Compliance Requirements	First Steps
Risk Analysis – CEs are requited to "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the Covered Entity." **(§164.308(a)(1)(ii)(A))**	Learn what a Risk Analysis is, and how to conduct one. See the (free) NIST guides on Risk Analysis at **www.NIST.gov**.
Privacy & Security Policies, Procedures, and Forms – CEs must implement written privacy & security policies, procedures, and forms that are consistent with the Privacy and Security Rules. **(§164.316)** and **(§164.530(i))**	Develop your entity's own Policies, Procedures, and Forms. See the "HIPAA Compliance" category on the HIPAA Store.
Privacy Personnel – CEs must designate a privacy official responsible for developing and implementing privacy policies and procedures, and a contact person or contact office responsible for receiving complaints and providing individuals with information on the entity's privacy practices. **(§164.530(a))**	Assign primary HIPAA responsibility to a senior employee. Train them thoroughly. HIPAA Officers should take our HIPAA Masters online course.
Workforce Training and Management – CEs must train all workforce members on their privacy policies and procedures, as necessary and appropriate for them to carry out their functions. **(§164.530(b))** Workforce members include employees, volunteers, trainees, and may also include other persons whose conduct is under the direct control of the entity (whether or not they are paid by the entity). **(§160.103)**	Train all workforce members to a level appropriate for their work: Basic, Advanced, or Masters. See "HIPAA Training" on the HIPAA Store for both online and DVD-based HIPAA training.
Mitigation – Covered Entities must mitigate, to the extent practicable, any harmful effects caused by the use or disclosure of protected health information by their workforce or their BAs in violation of privacy policies and procedures or the Privacy Rule. **(§164.530(f))**	Have a Mitigation Plan and Policy in place. Learn more about Mitigation from our HIPAA Masters course.
Data Safeguards – CEs must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information in violation of the Privacy Rule and to limit its incidental use and disclosure pursuant to otherwise permitted or required use or disclosure. **(§164.530(c))**	Be sure your I.T. team understands and implements Data Safeguards. Our CE Policies cover all these HIPAA requirements. Our HIPAA Masters course is perfect for training I.T. professionals.
Breach Notification – When a breach of unsecured protected health information (PHI) is discovered by a Covered Entity, the CE must notify each individual whose PHI has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach. **(§164.400-164.414)**	Have a Breach response Plan in place, with all needed forms prepared in advance. Prepare for Breaches with our HIPAA Advanced or Masters courses. Also see our "Forms" product in the HIPAA Store.
Complaints – Covered Entities must have procedures for individuals to complain about violations of their privacy policies and procedures and the Privacy Rule. **(§164.530(d))** Covered Entities must explain those procedures in their Privacy Practices Notice. **(§164.520(b)(1)(vi))**	Implement your Complaints handling process in advance. Learn more about handling Complaints from our HIPAA Advanced or Masters courses.
No Retaliation – Covered Entities may not retaliate against a person for exercising rights provided by the Privacy Rule, for assisting in an investigation by HHS or other appropriate authority, or for opposing an act or practice that the person believes in good faith violates the Privacy Rule. **(§164.530(g))**	Understand these and other important HIPAA prohibitions to avoid serious violations. Learn more about Retaliation from our HIPAA Masters course.
Documentation and Record Retention – CEs must maintain (until six years after the later of the date of their creation or last effective date) privacy policies and procedures, privacy practice Notices, dispositions of complaints, and other actions, activities, and designations that the Privacy Rule requires to be documented. **(§164.530(j))**	See our convenient "HIPAA Final Rule Compliance Checklist" on the HIPAA Store to be sure you've addressed everything HIPAA requires.