HIPAA Compliance Guide

HIPAA Compliance for Business Associates

Who Must Comply with HIPAA?

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.

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 – Process standard HIPAA transactions from one form or format into another form or format.

What Must a Business Associate Do to Comply with HIPAA?

Because most Business Associates (BAs) 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 Business Associates completely or in part. 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 penalties 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. BAs now have vastly increased responsibilities and liabilities under HIPAA since the Final Rule became effective. The Final Rule not only raised the penalties for HIPAA violations to a new high of $50,000 per violation and $1.5 Million annual maximum per violator. The Final Rule also makes these fines and penalties *applicable to BAs* in the same manner they apply to all Covered Entities. When we speak of HIPAA and HIPAA compliance today, HITECH and the 2013 Final Rule are automatically included, as both have now become integral parts of the HIPAA Regulations.

HIPAA requires Business Associates to comply with the "use and disclosure requirements" of the HIPAA Privacy Rule and to include those terms in their BA Agreements (contracts) with any Covered Entities. This carries on an earlier (pre-HITECH) HIPAA mandate that requires highly specific contracts to be signed and implemented between all Covered Entities and their Business Associates.

BAs must also comply in full with sections 164.308, 164.310, and 164.312 of HIPAA's Security Rule, which covers all electronic forms of patient health data, as well as the information systems where such data is received, transmitted, used, or stored. The Security Rule calls for the implementation of specific administrative, technical, and physical "data safeguards" to protect sensitive data. Compliance here means developing and implementing a set of Policies and Procedures (P&Ps) called for in the Regulations, as well as any applicable forms that may be needed for implementing or managing the requirements.

BAs are also required to provide appropriate training to all members of the workforce who may handle or be exposed to patient data. Training must be tailored to the nature of the workforce and their responsibilities under HIPAA.

BAs must also be prepared to handle Breach Notification, the mandatory requirement to notify patients whose health data has been lost, stolen, or compromised. BAs must coordinate with their CE partners to ensure that Breach Notification requirements are fulfilled in a timely manner.

Finally, BAs must be prepared for the documentation and record retention requirements that HIPAA imposes. For all these reasons, it is critically important that BAs learn and implement everything HIPAA requires, without delay.

What Does "Compliance" Specifically Require for Business Associates?

Compliance Requirements	First Steps
Privacy & Security Policies and Procedures – BAs must develop and implement written privacy policies and procedures that are consistent with the applicable portions of the Privacy & Security Rules. **(§164.316)**	Develop your entity's own Policies and Procedures. See the "Business Associates" category on the HIPAA Store.
Use & Disclosure Requirements of Privacy Rule – BAs must comply with the "Use and Disclosure" requirements of HIPAA's Privacy Rule. BAs must also include those requirements in their BA Agreements (contracts) with the Covered Entities they work with. **(§164.502)**	Learn about Use & Disclosure requirements and determine how they apply to you. Learn more about this from our HIPAA Advanced or HIPAA Masters courses.
Workforce Training and Management – BAs 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)) & §164.308(a)(5)** 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 online and DVD-based HIPAA training, including BA-specific courses.
Administrative Safeguards – These are "*administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the ... entity's workforce in relation to the protection of that information.*" **(§164.308)**	Be sure your I.T. professionals understand and implement Admin Safeguards. Our BA Policies cover all these HIPAA requirements. Our HIPAA Masters course is perfect for training I.T. leaders.
Physical Safeguards – These are defined in the HIPAA Regulations as: "*physical measures, policies, and procedures to protect an entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.*" Physical Safeguards are an additional layer of defense for protecting patient data. **(§164.310)**	Be sure your leadership team understands & implements Physical Safeguards. Our BA Policies cover all these HIPAA requirements. Our HIPAA Masters course is perfect for training I.T. professionals.
Technical Safeguards – These are: "*the technology and the policy and procedures for its use that protect electronic Protected Health Information and control access to it*." The Rule allows an entity to use any security measures that allows it reasonably and appropriately to implement the standards and implementation specifications. **(§164.312)**	Be sure your I.T. professionals understand & implement Technical Safeguards. Our BA 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 BA, the BA must promptly notify the Covered Entity who provided the PHI, and must provided detailed data about the breach, along with the names and contact information of all affected individuals. **(§164.410)**	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 BA "Forms" product in the HIPAA Store.
Documentation and Record Retention – BAs must maintain (until six years after the later of the creation-date or last effective-date) privacy and security policies and procedures, compliance documentation, dispositions of complaints, and other actions, activities, and designations that the Privacy Rule requires to be documented. **(§164.530(j))**	Train your I.T. professionals and your HIPAA leaders with our HIPAA Masters course to be sure you've addressed everything HIPAA requires of Business Associates.