BASIC Full - Service
Employer HIPAA Privacy & Security Compliance Programs

How our Full - Service Compliance Program Works…

Web based consultation, training and compliance - BASIC conducts a web based business conference call with employer representative(s) to complete the due diligence review, discuss what safe guards the employer has in place, conducts web based HIPAA compliance training, develops the employer’s HIPAA Privacy and Security policy and procedure documents for implementation and provides the final compliance program to the employer for implementation.

All HIPAA Privacy & Security requirements are evaluated through a “due diligence” process with policies, procedures and practices developed for the employer. The HIPAA Privacy & Security compliance program is certified by BASIC as meeting HIPAA Privacy and Security Regulatory Requirements.

We Evaluate How HIPAA Affects You

The first step is a meeting and a review of the organization’s current activities and practices to create a “Gap Analysis”. Then we proceed with HIPAA compliance for the organization. The following key elements are included as a part of the compliance program:

HIPAA Policy/Procedure Development and Compliance Activities/Action Items

- Evaluate current practices (HIPAA Privacy and Security Due Diligence Review)
  - Current use of PHI/IHI
  - Access to PHI
  - Security Controls in place
    - Administrative controls
    - Electronic/Technology Security Controls
- Create HIPAA Policy and Procedure documents
  - Use specific HIPAA compliance language in policy.
- Create Confidentiality Agreements
 Benefits Administrator
 o Accounting Administrator
 o Managers/Supervisors who may become knowledgeable of PHI
 o Others

- Develop HIPAA Notice Form in New Employee Orientation
  o Employee Notification - HIPAA Policy and Practice
  o HIPAA Acknowledgement Form (signature required)

- Confirm - Separate Medical files (PHI/IHI) from other personnel & Administration records.

- Appoint HIPAA Privacy and Security Officer(s)

- Create and Post HIPAA Privacy Notice (includes)
  o Posting notice of individual rights under HIPAA in Public Area
    - Covers all aspects of HIPAA and how employees can initiate HIPAA complaint activities (Internally & Externally)
  o Provide a HIPAA Privacy Notice to distribute to employees
    - Summary of rights under HIPAA

HIPAA Compliance Training
- HIPAA Compliance Training
  o Privacy / Security Officer & Benefit Administration Personnel

Business Associate Agreements
- Agents & Insurance Companies
- TPA’s
- Vendors
- Others

Certification and Group Health Plan Amendment
- Create an Amendment to the Group Health Plan stipulating HIPAA Compliance.
- Certifying HIPAA compliance

General Compliance Forms
The following forms are created and included with our HIPAA Privacy Compliance Programs. Other forms and documents may be added based as determined during the due diligence review.
Company Policy and Procedure document (REQUIRED) - This document is “extremely” important. It identifies your organization’s policy and practice with regard to HIPAA compliance and your daily activities to “protect” the privacy and rights employees have under HIPAA. This document becomes the foundation of your HIPAA compliance program.

HIPAA Posting (REQUIRED) - Make sure that your HIPAA policy and practice documents are the same as what is referenced in the HIPAA posting. This document is to be posted in a common area and visible to your employees.

HIPAA NOTICE OF PRIVACY (REQUIRED) - This document provides employee with information with regard to the use, disclosure and security requirements as it pertains to Employee Protected Health Information maintained or transacted by the employer.

Orientation New Employee Notice – It is the Company’s notice to new hires that they comply with HIPAA Privacy and Security requirements directs them to the posted notice or to the Company’s designated HIPAA Privacy and Security Officer.

New Employee / Employee Medical Information Conditional Release Authorization – The reason why this document is executed is to ensure that the Group Benefit Plan does not obtain, use or disclose legally protected health or medical information about an employee without their permission or for purposes other than those permitted by law. This document should be given to new employees when they hire in, be signed and returned. All employees should sign this document when the employer is requesting their insurance agent, broker or business associate to obtain alternative price quotes for group health programs. This is a specific use document which identifies the reason why PHI may be disclosed and to whom.

This Medical Information Release Authorization is for the duration of employment. This release is not intended to be a “catch all” release allowing the plan to use protected health information for any and all purposes. A second release authorization is used for specific use, like the benefit administrator assisting an employee with medical benefit claim issues.
Authorization to Disclose Protected Health Information – This is one of the most important documents that an employer will use. Whenever an employee asks for help resolving a claim or guidance regarding a medical condition, the employee “must” complete this form. The purpose of the form is to obtain a release from the employee to share protected health information to resolve claims issues or for other reasons that will involve the Group Benefit Plan representative coming in contact with protected health information and to release the representatives and business associates to release information to others. Other occasions where there will be a need for this form is when the employer may require an employee to submit to a drug/alcohol test.

Often times, the Company doctor will have a Release Authorization Form, which they will have the employee sign, allowing them (the doctor) to release the results of the test to the employer. Protected health information as a result of a Workers’ Compensation claim is “exempt” and you do not have to have an authorization from the employee before reviewing or disclosing Protected Health Information resulting from the Workers’ Compensation claim.

Confidentiality Agreement – This is a “due diligence” document. Everyone that comes in contact with protected health information requires the highest level of training as compared to the remainder of your staff. These individuals are performing services on behalf of your Group Benefit Plan and should understand the need to maintain confidentiality with regard to protected health information. This document is not mandatory but it serves a purpose “if or when” as the employer, you are asked how you enforce PHI privacy issue. You can reference your HIPAA compliance policy binder and refer to the signed Confidentiality Agreements.

E-mail Confidentiality Statement – Required statement; needs to be added to the signature block when sending e-mails containing protected health information as an attachment or imbedded in the e-mail. This is a safeguard statement informing the recipient that the e-mail may contain confidential information and should be handled appropriately.

Fax Transmission Confidentiality Statement – Similar to the e-mail confidentiality statement. When sending faxes containing PHI it is imperative that this statement be included. This statement informs the recipient that the fax contains confidential and privileged information intended solely for the use of the recipient. Faxes containing PHI should be sent from fax machines in a secure location and attended during the transmission. A delivery confirmation should be attached to the original faxed documents prior to filing.

Employment Application Insert – This document may or may not be necessary. If your organization requires satisfactory completion of employment physicals and or drug tests, then you are required to obtain a medical release from the employee prior to reviewing the results of the physical or drug test. In many cases, the company doctor will have the employee sign the release prior to completing the physical or drug test and release the information to the employer. However, it is a good practice to have the applicant/employee sign the release prior to seeing the company doctor. No release is necessary if the employee’s physical condition is the result of a work-related incident, i.e. Workers’ Compensation claim.