



HIPAA Compliance Manual



This Manual is provided to assist your efforts to comply with the federal privacy and security rules mandated under HIPAA and HITECH, specifically as said rules relate to services provided by TASC (HRA, FSA, etc.). TASC strongly recommends that all TASC Clients become familiar with these laws and take the time to set up and document compliance, if applicable. Compliance for the typical employer is not difficult.

This Manual is provided with the understanding that neither TASC, nor its employees or owners are engaged in rendering legal or accounting services, and no such services or advice are being offered in this Manual. When necessary, such legal advice or other expert assistance should be sought from a competent professional.

What is HIPAA? What is HITECH?	3
What are the risks of non-compliance?	3
Do the privacy and security rules apply to my company?	3
What records are subject to these laws?	4
What must we do to comply with the privacy rule?	4
When may we share PHI?	5
Who may access PHI?	6
What training is required?	6
What ongoing records must be maintained?	6
What steps are required if an unauthorized disclosure of PHI occurs?	7
What security measures are required for compliance?	7
Where do I obtain additional information?	8

What is HIPAA? What is HITECH?

HIPAA is a federal law that governs entities that handle “Protected Health Information” (PHI) in relation to “Group Health Plans,” health treatment, and claims payment. Called The Health Insurance Portability & Accountability Act of 1996 (“HIPAA”), this federal law was amended by the Health Information Technology for Economic & Clinical Health Act of 2009 (“HITECH”). HIPAA covers several other key aspects of health Plan compliance, including but not limited to special enrollment rights, pre-existing conditions, portability of plans, administrative simplification, discrimination, and more. Administered by Health & Human Services (“HHS”) and the Centers for Medicare & Medicaid Services (CMS), HIPAA mandates are enforced by the Office of Civil Rights (“OCR”). In addition HITECH granted authority to state attorneys general to enforce HIPAA violations.

What are the risks of non-compliance?

Non-compliance can be costly. During the HITECH Act debates, Congress specifically noted a need for increased penalties and increased enforcement. Subsequently, the penalties were augmented dramatically and are now based on a finding of non-compliance and a determination of the efforts to comply as shown below.

- If the entity did not know and by exercising reasonable diligence would not have known of the violation, the penalty for each violation will be an amount not less than \$100 and not more than \$50,000;
- For a violation due to reasonable cause and not willful neglect, the penalty for each violation will be an amount not less than \$1000 and not more than \$50,000;
- For a violation due to willful neglect that was corrected in a timely fashion, the penalty for each violation will be an amount not less than \$10,000 and not more than \$50,000;
- For a violation due to willful neglect that was not corrected in a timely fashion, the penalty for each violation will be an amount not less than \$50,000; and,

- A penalty for violations of the same requirement or prohibition under any of these categories may not exceed \$1,500,000 in a calendar year.

The news has reported penalties that have exceeded a million dollars.

Do the privacy and security rules apply to my company?

Not all employers who sponsor Group Health Plans are subject to these rules, and in many cases only a subset of the rules apply. In general, HIPAA applies to Protected Health Information that is produced, maintained, or transmitted in connection with your Group Health Plan.

- **Protected Health Information (PHI)** is a broad term that denotes individually identifiable health information that is maintained or transmitted in any form or medium, including, without limitation, all information (including demographic, medical, and financial information), data, documentation, and materials which are created or received, and relate to: (a) the past, present, or future physical or mental health or condition of an individual; (b) the provision of healthcare to an individual; and/or (c) the past, present, or future payment for the provision of healthcare to an individual that identifies or could reasonably be used to identify an individual.
- **Group Health Plan** indicates an employer-sponsored arrangement that includes indemnity and self-funded health plans that offer the following: medical benefits including HMO coverage, long-term care plans, dental plans, vision plans, flexible spending accounts (FSAs), health reimbursement accounts (HRAs), and other plans that may offer medical care such as some EAP plans and wellness plans.

Employers are allowed two exceptions under which the privacy and security rules are not imposed:

1. **Fully insured hands off employers.** Employers who sponsor fully insured health plans (indemnity or HMO Contracts) are not

subject to the privacy or security rules if they have access to summary health data for limited purposes only (names and items that identify the person are redacted), with only paper access to enrollment and disenrollment information. (Note: The federal security rule applies to the storage, transmission, and destruction of the enrollment and disenrollment data maintained or transmitted in an electronic format when a business office is maintaining or sending enrollment data electronically. If employees are enrolling online through a TPA or carrier then that entity must comply with the security rules.)

2. **Self-funded self-administered small plans.** Employers who self-administer a self-funded health Plan (including FSA or HRA) with fewer than 50 covered employees are not subject to the privacy or security rules.

Employers who offer Group Health Plans and do not meet the two exceptions above are subject to some or all of the privacy and security rules explained in this Manual.

What records are subject to these laws?

The following three categories of records do not come under the federal privacy or security rules. Note: the enrollment and disenrollment data requirements depend on whether the employer meets one of the exceptions above.

1. **Employment records are not PHI.** This test is not concerned with actual content of the record. Instead, it relates to the purpose for which the record was obtained. For example, records related to a benefit claim for medical treatment in a hospital are considered PHI. Conversely, a physician's note provided to an employer providing the reason for time off (documentation of the same hospital stay) and an opinion that the employee is ready to return to work, are not PHI. Further, physical examinations to determine an employee's ability to perform a job function are considered "employment records," not PHI. To be considered PHI, the records must be created, maintained, or transmitted for the administration of the employer's Group Health Plan.

Employment records are outside of the privacy and security rules.

2. **Enrollment and disenrollment data is PHI.** The definition of PHI includes any data that shows enrollment or disenrollment in a Group Health Plan. Any organization that takes the "hands off" approach, noted above, is not required to comply with the privacy rule related to enrollment or disenrollment data, and need not comply with the security rule unless said organization creates, maintains or transmits electronic enrollment or disenrollment data. Any organization otherwise subject to HIPAA must comply with both the privacy and security measures dictated by these laws.
3. **De-identified information.** De-identified information is data that does not identify any employee. Employers must show a reasonable basis to believe that said information cannot be linked back to any specific employee. It is the type of data that is used for underwriting, managing the overall Plan costs, setting COBRA premiums for self-funded plans, and so on.

All other PHI, including enrollment and disenrollment data, that is received, stored, or transmitted for the administration of a Group Health Plan is subject to the HIPAA privacy and HITECH security rules.

What must we do to comply with the privacy rule?

There are some general rules that you will need to know to get started.

- You will need to appoint a Privacy Officer. This individual will be responsible for developing and implementing policies and procedures relating to privacy. The Privacy Officer will also serve as the contact person for Participants who have questions, concerns, or any complaints about PHI. Typically, this person keeps the documentation for compliance and trains any staff with access to PHI.
- You will need to appoint a Security Officer. This individual will be responsible for developing and implementing policies and procedures relating to how the PHI is electronically stored, transmitted and destroyed. Typically, the Security Officer maintains the documentation for system compliance.

- You cannot use or disclose PHI for any reason other than the administration of your Group Health Plan. It is illegal to use or disclose PHI for any other purpose, including any employment purpose such as a promotion or termination. Remember, employment records obtained for other purposes not related to your Group Health Plan are not PHI; as such that information may be used for other legitimate employment reasons.
 - Under no circumstances are you allowed to sell PHI.
 - HIPAA Privacy Rights may not be waived by any person or entity. These rules are enforced regardless of any waivers that are obtained.
 - The extent of your compliance efforts can be linked to the PHI that is created, maintained and transmitted. For instance, consider a psychiatric hospital with personal data that could be used to harm someone's reputation; this hospital's burden to secure that data is far greater than that of an employer whose sole PHI is related to who enrolled in a plan, or terminated coverage in a plan. (In many cases, enrollment data includes a Social Security Number that could be used to harm an employee.)
2. You may disclose the minimum necessary PHI without an authorization to a Business Associate for Plan administration purposes.
 3. You may disclose PHI to a government agency as a result of a legal request such as a subpoena.
 - **Authorizations.** PHI may be disclosed by Participant authorization to the Participant or as directed by the Participant. All uses and disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization. An authorization must be a separate form that includes the following: (a) a note that the authorization may be revoked at any time, (b) identification of the person who is the subject of the PHI, (c) identification of the person(s) who may receive the PHI, (d) the purpose of the request, (e) an expiration date, and (f) a statement that the Plan will not condition claims payment on the signing of the authorization.
 - **Business Associates.** PHI may be disclosed without Participant authorizations to a Business Associate only when the disclosure is for Plan administration and the minimum necessary information is sent to complete the intended function. All Business Associates must enter a written Privacy Agreement with you, as Plan Sponsor. We recommend using the sample agreements published at "HHS.gov." (search the site for "business associate contract"). A Business Associate is an entity or person who: (a) performs or assists in performing a Plan function or activity involving the use and disclosure of PHI (including claims processing or administration; data analysis, underwriting, etc.); or (b) provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to PHI.
 - **Plan Sponsor Certification** is needed when obtaining PHI regarding a claim, an appeal, or other legitimate Plan reason. This information is outside of the routine disclosures allowed under a Business Associate Contract. The Plan Sponsor must certify that the Plan Documents have been amended

When may we share PHI?

The "Minimum Necessary" rule dictates that when making disclosures of PHI for health plan administration, only PHI necessary for the intended purpose may be disclosed. You must tailor all transmissions of PHI to the "minimum necessary" needed to complete the transaction. For instance, when sending data for enrollment neither the employee's health screening data nor any benefit usage information may be included.

The Minimum Necessary standard does not apply to uses or disclosures made to the Participant upon request; uses or disclosures made pursuant to a valid authorization; or, required disclosures made to the Department of Labor ("DOL").

Three levels of authorized disclosures exist.

1. You may disclose PHI for an employee who signs and authorizes said disclosure.

to comply with the privacy rule and that the Plan Sponsor agrees to comply with said rule.

As the Plan Sponsor, your office must certify the following items and list them in your Plan Document:

1. certify that you will not use or further disclose protected health information (“PHI”) other than as permitted or required by this Plan Document, or as required by law,
2. ensure that any subcontractors or agents to whom the Plan Sponsor provides PHI agree to the same restrictions,
3. promise that you will not use or disclose PHI for employment related actions,
4. report to the Health Plan any use or disclosure that is inconsistent with this Plan Document or the federal privacy rule,
5. make the PHI information accessible to the Participants upon request,
6. allow Participants to request an amendment to their PHI,
7. provide an accounting of its disclosures of PHI discussed below,
8. make your practices available to the Secretary of HHS for determining compliance,
9. return and destroy all PHI when no longer needed, if feasible, and
10. establish adequate firewalls.

Who may access PHI?

You must limit access to PHI to only those persons who are trained regarding your Privacy Policy. Your Privacy Policy must document the personnel who are allowed access to PHI.

What training is required?

Training is a federal requirement. It usually takes around ½ hour and is easy to document. All employees with access to PHI must undergo training within 30 days of their date of hire or by the date upon which they may first access PHI. We recommend that the trained personnel sign a short form confirming that the person received said training and that said employee—as a condition of employment—agrees to comply with your Privacy Policy. The actual training

must include a statement explaining that sanctions for using or disclosing PHI in violation of your HIPAA Privacy Policy will be imposed in accordance with your discipline policy, up to and including termination.

What ongoing records must be maintained?

The Plan Document. The Plan Document must be amended when your office first commences to receive PHI, see the “Plan Sponsor Certification” above. The Plan and the Plan Sponsor are two separate entities under the federal law. The employer who sponsors the Plan is the Plan Sponsor, and the Plan provides benefits to participating employees, as set up by the Plan Document. The Plan Document must spell out what PHI the employer-Plan Sponsor will receive. For instance, a fully insured Plan in which the employer is taking the “hands off” approach may be silent on PHI. When the insurance company requires the employer-Plan Sponsor to decide appeals, the document will address that process. The items that are typically addressed in the Plan Document amendment are the same 10 items listed under the Plan Sponsor Certification term above. There is no requirement to amend your Summary Plan Description for these rules.

HIPAA Privacy and Security Policy. We advise our Clients to maintain a written HIPAA Privacy and Security Policy. Besides helping with training and when responding to inquiries, said policy will also evidence your attempt to comply. (Consider accessing online programs; for a fee you can access pertinent documents after answering questions on your involvement and use of PHI.) The policy must include a term/descriptor for any personnel with access to PHI, what PHI is created for Plan administration, where the PHI is stored with security measures described, how PHI is transmitted including encryption detail, and how it is destroyed. To determine security measures, examine all e-locations in which PHI is maintained electronically, and ensure that your fire wall efforts are included and monitored.

Training documentation. Retain a copy of training materials used and each employee’s signed agreement that acknowledges he/she has undergone training regarding the privacy rule and the Privacy Policy, and that by signing said employee promises compliance with this HFS Privacy Policy. Training must include a note explaining that sanctions may be imposed for violations up to and including termination of employment.

Disclosures. For six (6) years from the date of the disclosure, you must document PHI disclosures, including those made by authorization EXCEPT for the following (need not document disclosures of):

- Summary Health Information as defined above, and
- Routine Disclosures described above that are made under a Business Associate Agreement.

The record will include name and address of all who received the PHI, a brief description of information forwarded, statement of the purpose of the disclosure, and signed authorization, if required.

Authorizations. For six (6) years from the date of an authorized disclosure the Privacy Officer must maintain a copy of each authorization and the particular PHI disclosed in response to the authorization.

Participant rights. Participant rights are typically an issue for a healthcare practitioner or hospital; as such, they rarely arise in the office setting. The Privacy Officer will document the following requests and the outcome of each. The request's outcome is not driven by the law. For instance, if a Participant requests that you amend his/her medical records (a possible scenario when an appeal is being reviewed), you could direct the member back to the medical practitioner who created the record.

- **Request to restrict the use of the PHI and request confidential communications.** The Privacy Officer will document all requests for restrictions, and/or confidential communications, whether granted or not, for six (6) years following the last day of the applicable Plan Year.
- **Request for alternative communication means or locations.** The Privacy Officer will keep a copy of the request and any action taken, if any, for six (6) years after the end of the Participant's last Plan Year.
- **Request to inspect and copy PHI.** The Privacy Officer will keep a copy of the request and any action taken, if any, for six (6) years after the request was received.
- **Request to amend PHI.** The Privacy Officer will keep a copy of the request and any action taken, if any, for six (6) years after the end of the Participant's last Plan Year.

Complaints. The Privacy Officer must document any complaint made regarding the use or disclosure of PHI and any resolution of a complaint.

What steps are required if an unauthorized disclosure of PHI occurs?

An Incident Response Policy must be established; it should describe actions to be taken in the instance of an unauthorized disclosure of PHI by an employee or a Business Associate (a disclosure that does not otherwise comply with the disclosure rules provided above). All such unauthorized disclosures must be reported as soon as reasonably possible to the Privacy Officer. The incident must be documented, including mitigation described below and whether follow-up breach letters are required (see below).

You are required to mitigate, to the extent possible, any harmful effects of an unauthorized disclosure. The typical recourse is to request that the unauthorized PHI recipient immediately destroy the data and confirm that they have done so. Email or other confirmation that the data was destroyed is acceptable. Mitigation may include additional options as determined, including required notices described below and ID theft monitoring services.

A "Breach" under the HITECH Act is where there is an impermissible acquisition, access, use or disclosure of PHI, a breach is presumed unless the Covered Entity or Business Associate demonstrates, through a risk assessment, that there is a low probability that PHI has been compromised. The risk assessment must consider at least the following factors:

- 1) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- 2) the unauthorized person who used the PHI or to whom the disclosure was made;
- 3) whether the PHI was actually acquired or viewed; and
- 4) the extent to which the risk to the PHI has been mitigated. Entities may consider other factors, but the analysis must be thorough and in good faith, and it must reach a reasonable conclusion. In addition, covered entities and business associates can provide breach notifications following any impermissible use or disclosure without performing a risk assessment, if they choose to do so.

As mandated, any breach that affects 500 or more Participants must be reported to Health and Human Services. Employers so affected should seek professional counsel prior to making a final determination regarding extent of notices required. In general, the Breach Notice is required only when the unauthorized disclosure is determined to be an actual breach.

There is a requirement that a Covered Entity send HHS a report of all of its breaches that occurred that were under 500 persons at the close of each Plan Year, starting for plan years that end in 2014.

What security measures are required for compliance?

The security rules under the HITECH Act address how you store, send and destroy electronic PHI. The measure of security depends on the data. Enrollment data usually includes social security numbers and must be stored in a manner that is either encrypted or inaccessible to persons who are not HIPAA trained. This manual does not attempt to recommend or describe computer security methods. The HITECH Act incorporated the recommendations of the National Institute of Standards and Technology (NIST). The NIST standards include, but are not limited to the following items that store PHI:

- **End user device policies**

 - Workstation use and security

 - Laptop use and security

 - Writeable media

- **Data destruction**

 - Data destruction and a data destruction log

 - Personal computer and laptop destruction

 - PDA and writeable media

 - Shredding all paper records with PHI

- **Electronic transmissions** – we recommend using email security programs that meet NIST Standards; these are available online.

 - Secure email sending (This is key to avoiding breach incidents.)

Where do I obtain additional information?

Health and Human Services at <http://www.hhs.gov/ocr/privacy/> has a great deal of information on the privacy and security rules under HIPAA and HITECH, with compliance manuals.

You can subscribe to free newsletters (EBIA or Benefitlinks) that will keep you updated with any new regulatory requirement under these rules.

COBRAToday COBRA Administration
DirectPay Health Reimbursement Arrangements (HRA)
FlexSystem Flexible Spending Accounts (FSA)
ERISAEdge ERISA Compliance
FMLAMatters FMLA Administration
PayPath Payroll Services
TASC Health Savings Accounts (HSA)