HIPAA Compliance Reference Guide

Welcome to TASC HIPAA Compliance service.

This Reference Guide is intended to assist you in establishing and documenting compliance with federal privacy and security rules as mandated by HIPAA and HITECH. TASC is not engaged in rendering legal or accounting services, and no such service or advice is being offered in this product. When seeking such legal advice or other expert assistance, a competent professional should be engaged.

This Reference Guide provides general information to inform you about compliance issues, along with details regarding how to use the innovative compliance tools that are part of the TASC HIPAA Compliance service offering.

Here's what you'll find inside:

HIPAA

HI-5134-080320

What are HIPAA and HITECH?

The federal law is the Health Insurance Portability & Accountability Act of 1996 (HIPAA), amended by the Health Information Technology for Economic & Clinical Health Act of 2009 (HITECH). HIPAA covers several other key aspects concerning compliance of Group Health Plans (GHPs), including but not limited to special enrollment rights, pre-existing conditions, portability of GHPs, administrative simplification, discrimination and more. Administered by the U.S. Department of Health & Human Services (HHS) and the Centers for Medicare & Medicaid Services (CMS), these laws are enforced by the Office of Civil Rights (OCR). In addition, HITECH grants authority to state attorneys general to enforce HIPAA violations.

HIPAA and HITECH apply to Protected Health Information (PHI) that is produced, maintained, and transmitted in connection with your Group Health Plan.

- Protected Health Information is a broad term that means individually identifiable health information maintained and 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, which identifies or could reasonably be used to identify an individual, and which relates to: (a) the past, present, or future physical or mental health or condition of an individual; (b) the provision of healthcare to an individual; or (c) the past, present, or future payment for the provision of healthcare to an individual.
- Group Health Plan means 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, vision, Flexible Spending Accounts (FSAs), Health Reimbursement Accounts (HRAs), and other plans that provide or pay for medical care, such as some Employee Assistance Program (EAP) plans and wellness plans.

What employers need TASC's HIPAA Compliance service?

TASC's HIPAA Compliance service offering is for employers who sponsor a self-funded GHP that is administered by a third party administrator or service provider. The self-funded GHP can be an HRA or health FSA. It can be a standalone self-funded benefit program such as a prescription drug plan, dental plan, or vision plan. The key is that the benefits are paid from the general assets of the employer, or a trust, and not paid by an insurance company. Consult your benefit advisors or benefits counsel if you are unsure whether your GHPs are self-funded TASC will make that determination ONLY for the tax advantaged account plans we administer (DirectPay and FlexSystem).

If you self-administer your self-funded plan(s) and maintain medical records for claims purposes then this product will not bring you into compliance with the HITECH Security requirements.

If all of your benefits are insured, and you sponsor no self-funded plans, then you need not be concerned about compliance with HIPAA or HITECH.

The extent of your compliance efforts can be linked to the PHI that is created, maintained and transmitted. For instance, a psychiatric record can affect an individual's reputation, and as such requires vigilant security, while PHI related to enrollment or terminated coverage in a GHP requires less burden to secure.

What records are not subject to these laws?

The following categories of records that employers maintain are not subject to HIPAA or HITECH.

1. Employment Records. The determination is not in regards to the contents of the record. It is based on the purpose for which the record was obtained.
    - Records related to a benefits claim for medical treatment in a hospital are PHI.
    - 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.
    - Physical examinations to determine an employee's ability to perform his/her job function are not PHI.

    To be considered PHI, the records must be created, maintained, or transmitted for the administration of your GHP. Other employment records are outside of these federal privacy and security rules. (Meanwhile, state privacy laws generally protect personal information related to ID theft, and focus on employment records that can be used to access an employee's accounts, including Social Security numbers.)

2. De-Identified Information. De-identified information is data that does not identify an individual. Required is show of the employer's reasonable effort to ensure that said information cannot be linked back to any specific employee. This type of data is used for underwriting, managing the overall GHP costs, etc. A list of items to be removed is provided in the HIPAA Policy provided with this service.

All other PHI, including enrollment and disenrollment data, that is received, stored, or transmitted for the administration of your GHP is subject to HIPAA and HITECH.

What must you do to comply with HIPAA and HITECH?

This TASC Product provides you with the tools to have a compliant HIPAA HITECH policy. By using this Product and following the TASC recommendations you will be well on your way to compliance with HIPAA and HITECH.

Some general recommendations will help you begin.

- Appoint a Privacy/Security Officer. This Officer will be responsible for developing and implementing policies and procedures relating to privacy and security. This Officer will also serve as the contact person for Participants who have questions, concerns, or any complaints about how you manage their PHI. Typically, this Officer maintains all documentation related to compliance and trains staff who have access to PHI.
- You may not use or disclose PHI for any reason other than the administration of your GHP. 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 GHP are not PHI, and as such may be used for other legitimate employment reasons.
- You may not sell PHI for any reason. (TASC follows this approach to avoid the complex regulatory scheme in place for receiving any compensation for PHI.)
- HIPAA Privacy Rights cannot be waived by any person or entity. These rules are enforced regardless of any waivers that are obtained.
- All employees with access to PHI must complete HIPAA and HITECH Training within 30 days of their first access to PHI.

All Clients are obliged to maintain up-to-date contact information in MyTASC; this includes email and mailing addresses, and phone numbers. TASC periodically sends important Plan notifications (regarding balances, deadlines, and/or Plan changes). We are not responsible for any consequences resulting from communications not received due to inaccurate contact information.

When can we access and share PHI?

TASC recommends that you limit your access to PHI to enrollment and termination data, and to limited medical information in instances where you are called upon to resolve an appeal or dispute with your third-party administrator

or service provider. This is a key to this TASC service.

All access and sharing of PHI must respect the "Minimum Necessary" rule, which dictates that only PHI necessary for the intended purpose be obtained or disclosed. You must tailor all transmissions of PHI to the minimum necessary needed to complete the transaction. For instance, when sending data for enrollment you need not send the employee's health screening data or any benefits usage information. The minimum necessary standard does not apply to (a) uses or disclosures made to the Participant upon request; (b) uses or disclosures made pursuant to a valid authorization; or (c) required disclosures made to the U.S. Department of Labor (DOL).

TASC recommends shortening the Social Security Numbers to the last 4 digits whenever possible.

Three levels of authorized disclosures apply, as follows:

1. for an employee who signs an authorization allowing disclosure;
2. to a Business Associate for GHP administration purposes (minimum necessary PHI only); and
3. 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 and should provide the following:
  - clarify that the authorization may be revoked at any time;
  - identify the individual who is the subject of the PHI;
  - identify the individual(s) who may receive the PHI;
  - clarify the purpose of the request for the PHI;
  - include an expiration date;
  - include a statement that the GHP will not condition claims payment pursuant to the signing of the authorization.

TASC provides an Authorization at the end of this Manual for your use.

- Business Associates. PHI can be disclosed without Participant authorization to a business associate (a) only when the disclosure is for GHP administration and (b) the minimum necessary is sent to complete the intended function. Your third-party administrator and/or service provider is/are your business associates. TASC provides you with the information and contracts you need to share data with your business associates.
- Plan Sponsor Certification is needed for your office to obtain PHI regarding a claim, an appeal, or other legitimate GHP reason. This information is outside of the routine disclosures allowed under a Business Associate Contract. TASC provides the items needed to provide this Certification.

Who may be allowed access to PHI?

Access to PHI must be limited to persons who are trained regarding your Privacy Policy and who complete a legitimate function for your GHP. TASC provides a training program and an easy way to document which personnel are trained and allowed access.

What training is required of those with access to PHI?

Training usually takes less than one hour and is easy to document. All employees with access to PHI must be trained within 30 days of their date of hire or date upon which access to PHI is granted. TASC provides a training PowerPoint and short "training confirmation" form for the employee's signature stating that the signatory has received training and as a condition of employment agrees to comply with your Policy. The training material includes a statement 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 kept?
All required documentation is retained for 6 years from the date of the event as described below, or when appropriate for 6 years after the end of the Plan Year in which the document was created.

The Plan Document. Your Plan Document must be amended when your office receives PHI. This is a part of the Plan Sponsor Certification noted above. Considered two separate entities under federal law, the Plan Sponsor is the employer who sponsors the GHP, and the Plan is an entity established by the Plan Document to provide benefits to employees. The Plan Document must spell out what PHI the employer-Plan Sponsor will receive. TASC provides you with a Plan Document Amendment to be executed and retained with your records.

HIPAA Privacy and Security Policy. TASC provides a written HIPAA Privacy and Security Policy. It will help in training and is a resource for responding to inquiries.

Training Documentation. Keep a copy of training materials used and the employee's signed confirmation that acknowledges he/she has received training regarding the Privacy and Security Policy, and confirms that he/she will comply with this Policy. TASC provides a worksheet to capture the trained personnel and the training material used.

Disclosures. Document all disclosures, including those made by authorization. You do not need to document disclosures of the following:

- Summary Health Information as defined above, or
- Routine disclosures described above that are made under a Business Associate Contract

The record will include names and addresses of those who received the PHI; a brief description of information forwarded; statement of the purpose of the disclosure; and a signed authorization, if required. The HIPAA Policy provided with this Product presents more detail for your use.

Participant Rights. Typically Participant rights are an issue for healthcare practitioners and hospitals but rarely come up in the office setting. For instance, the right to copy medical records is key for patients who transfer providers. In the past patients frequently were told that their records were the work product of the provider, and as such were not released.

The Privacy Officer will document the following requests and the outcome of each. The outcome of the request is not driven by the law. For example, a Participant requests that you amend the medical records you received to review an appeal. You could direct the member back to the practitioner who created the record. You can use the HIPAA Policy provided by TASC when you get a request from a Participant—under one of the HIPAA rights noted below—to review the specific right and required response.

- 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 6 years following the last day of the applicable Plan Year.
- Request for Alternative Communication Means or Locations. The Privacy Officer will retain a copy of the request and any action taken.
- Request to Inspect and Copy PHI. The Privacy Officer will retain a copy of the request and action taken, if any, for 6 years after the request was received.
- Request to Amend PHI. The Privacy Officer will retain a copy of the request and action taken, if any, for 6 years after the end of the Participant's last Plan Year.
- Request for an Accounting of Disclosures. A Participant may want to know to whom you have released PHI. You will not have to account for minimum necessary transmissions to a business associate, or disclosures pursuant to an authorization. If you follow the TASC recommendations in most cases

the response will be that no PHI has been disclosed.
- Right to receive a Privacy Notice. This service provides you with a HIPAA Privacy Notice to meet this requirement.

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

What do we do if we have an unauthorized disclosure of PHI?

Contact your Benefits Advisor or Counsel. The determinations explained below can impact the resolution. TASC employees cannot answer legal questions based on factual events, such as whether an unauthorized disclosure is a "breach" as defined by state or federal law.

An Incident Response Policy is provided that describes actions for an unauthorized disclosure of PHI—defined as a disclosure that does not otherwise comply with the Disclosure Rules—either by an employee or a business associate.

You are required to mitigate, to the extent possible, any harmful effects of an unauthorized disclosure. The ideal course is to request that the unauthorized recipient of the PHI confirm that they have immediately destroyed the data and that no further disclosures were made. Email or other confirmation is acceptable. Mitigation may include additional options such as ID Theft monitoring services.

A breach under the HITECH Act is defined as the impermissible acquisition, access, use or disclosure of PHI. A breach is presumed unless it is determined, through a risk assessment, that it is highly unlikely that PHI has been compromised. The risk assessment must consider at least the following factors:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the PHI or to whom the disclosure was made;
- Whether the PHI was actually acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated.

Entities may consider other factors. The analysis must be thorough and in good faith, and it must reach a reasonable conclusion.

Any breach that includes 500 or more Participants must be reported to Health & Human Services. We recommend obtaining advice from professional counsel prior to making a final determination regarding extent of notices required. Posted on the HSS website is an online form along with instructions to be used by covered entities in reporting breaches to the agency. The notice must be submitted electronically by completing the online Breach Notification Form.

At the close of each Plan Year, a covered entity must send HHS a report of all occurring breaches that included that year, starting with Plan Years that end in 2014.

What security measures are required?

The security rules under the HITECH Act address manner of storing, sending, and destroying 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 in a secure system accessible only to persons who are HIPAA trained. TASC recommends removing any other detailed medical records—especially records sent for an appeal of an adverse determination—from your electronic media and retaining them in a secure locked place where trained employees only have access. 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 HIPAA Policy provided with this product includes items for the following:

- Security Incident Response Plan and Procedures,
- Hard Copy Storage Requirements,
- Workstation Protection,
- Laptop Use and Security,
- Electronic Data Retention and Storage Requirements, and
- PHI Destruction Requirements.

Where can 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, including compliance manuals.

Annual Plan Renewal

Near the end of the Plan Year, you will have the opportunity to re-enroll for the upcoming Plan Year.

TASC Invoicing Practices

TASC's Invoicing Practices aim to communicate expectations to all Clients and Providers, ensuring compliance to TASC Plans and services, creating consistency between all of TASC's divisions, and ensuring the continuation of services.

Philosophy

To ensure that TASC operations continue to run smoothly, various actions need to occur in a timely manner, including the payment of TASC administrative fees. Paying in advance demonstrates that the Plan is for the benefit of employees and provides further evidence that the Plan has been established on a pre-thought basis. TASC invoices in advance for two additional reasons:

1. TASC requires a commitment in advance of the business being processed, and
2. TASC requires a payment history for its Clients, so as to determine the Clients' status of good standing.

Administrative Fees

Because your TASC service begins before the Plan start date, TASC invoices forty-five (45) calendar days prior to the Plan start date. For example, for Plans with a January 1 start date, the first invoice is mailed on November 15 and is due seven (7) calendar days from the invoice date. TASC fees are calculated on the number of known employees at the time the invoice is generated, and Clients are charged a minimum administrative fee.

Types of Payments for Administrative Fees

- Check
  - Clients may pay by check.
- E-Pay
  - Clients may pay electronically as long as they use E-Pay, and as long as these fees are debited no later than seven (7) calendar days prior to the Service Period start date. Therefore, if a Service Period begins January 1, Clients will be debited on December 23.
- ACH Credit
  - Clients may pay administrative fees via an electronic ACH Credit transfer. A $40 per transaction Service Charge will be assessed. Clients should contact their Provider for details.
- ACH Debit
  - Clients may pay administrative fees via an electronic ACH Debit transfer. There is no Service Charge for this method.

Types of Invoices

- Administrative Fee
  - Generated annually for TASC Services that are provided during the Service Period.
- Premium Services Fee
  - Generated when a Client has elected a Premium Service.

Standard Invoicing Procedures

- Invoice
  - Generated and sent forty-five (45) calendar days prior to the Service Period start.
- Due Date
  - Seven (7) calendar days from the date the invoice was generated (invoice date).
- Service Charge Date
  - An additional $20 fee will be assessed sixty (60) calendar days from the original invoice date if the invoice is not paid by the Service Charge due date, and the account will be placed on hold.
- Statement
  - A Statement (second notice) of unpaid invoices will be mailed fifteen (15) calendar days prior to the start of the Service Period.
- Past Due Email Notification
  - On the first day of the Service Period or forty-five (45) calendar days after the

original invoice date (whichever comes first), an email will be sent to any account with unpaid invoices older than forty (40) calendar days. This email will inform the Client that the account will be put on hold and that a $20 service fee will be charged if the invoice is not paid within sixty (60) calendar days of the original invoice issue date.

- Final Notice Statement
  - A Final Notice Statement (third notice) will be mailed fifteen (15) calendar days into the Service Period, with a Service Charge of $20.00, a notice of "default" status, and an additional notice that all account services have been placed on hold.
- Collections
  - The account will be placed in Collections forty-five (45) calendar days into the Service Period start, or ninety (90) calendar days after the original invoice date, whichever comes first.
- Plan Termination
  - The account will be terminated one hundred four (104) calendar days into the Service Period start. Letters will be sent to each Client being terminated.

Client Responsibilities

- Please make your checks payable to TASC Administration. Checks incorrectly payable to TASC IRS Form 5500 Preparation can cause some confusion and may delay the administration of your Plan.
- Mail invoices and payments in the envelope provided (goldenrod color) to: TASC, 2302 International Lane, Madison, WI 53704-7098.
  - All invoice payments must be submitted separately from all other payments and transactions.
  - All invoice payments must be made separately (i.e. one check with one invoice).
- Notify TASC of any disputes or any changes.

Contacting TASC

Technical and Customer Service Support - TASC has a team of employee benefit experts to assist you with your Plan. Our experts can give you guidance and expertise to help ensure you remain compliant with all regulations. You may call toll-free (from 8am-5 pm weekdays except Wednesdays 9am-5pm) to address questions regarding compliance, technical issues, or other questions relevant to TASC.

For Your Benefit

TASC distributes For Your Benefit, a bi-annual newsletter that includes Plan updates and a calendar of important dates, along with information about other TASC Plans and guidance for managing and developing your business.

News Updates

Stay informed about important news regarding your Plan. Visit the TASC Client news site at www.tasctracker.com and subscribe to receive news updates via email.

HIPAA

The HIPAA Compliance Service

The HIPAA Compliance Service includes the following materials:

The HIPAA Privacy and Security Policy
This Policy covers the issues and processes that will be used in your compliance efforts. The topics include items that will be used daily to maintain compliance as well as items that are rare for employers who do not administer the GHP. For instance, the Policy includes Workstation Security that will be trained and used daily, as well as detail on Participant rights and responses to requests that are rare outside of a medical provider's office.

The Business Associate Agreement
TASC provides a Business Associate Contract for your use. You must obtain written assurances from all business associates regarding their HIPAA and HITECH compliance. The format for this assurance is a Business Associate Contract. TASC provides and recommends the latest model from the U.S. Department of Health & Human Services, without adding promises or obligations. Many third-party administrators and service providers must establish a compliant program for thousands of clients and cannot entertain unique or special conditions that are not required by the law.

The HIPAA Privacy Notice
The HIPAA Privacy Rule requires the distribution of a notice that provides a clear, user friendly explanation of the following:

- The uses and disclosures of PHI,
- The individual's HIPAA rights, and
- The GHPs' legal duties with respect to the PHI.

The HIPAA Notice must be provided to ALL persons who requests a copy, whether they are or are not current Participants. The Notice must be prominently posted and available on any website it maintains that provides information about its GHP or benefits.

The HIPAA Policy provided has detail on the distribution and documentation of the HIPAA Notice.

Plan Document Amendment
TASC provides a Plan Document Amendment that can be executed and retained with your Plan records. It is intended to be attached to and become incorporated with any Plan Document. It must be distributed to employees who request Plan Documents. It is not a part of the Summary Plan Description and must be distributed to employees only when requested.

Training
TASC provides a voiced-over slide presentation that provides necessary training to employees with access to PHI. It takes less than 1 hour. TASC has provided a sign off sheet for the employee to confirm receipt of the training and to assert their agreement to follow your HIPAA and HITECH Policy. In addition the Worksheet included in this Manual is useful for tracking staff training.

HIPAA

HIPAA and HITECH Compliance Worksheet

List each Group Health Plan that you sponsor for employees, and whether it is provided through an insurance contract or self-funded. Note: a signed Business Associate Contract is required of each third-party administrator and/or service provider.

Plan Name	Insured or or Self-Funded	Entity Contracted	Business Associate Agreement Required	Date Business Associate Agreement Signed
Example Dental Plan	Self-Funded	TPA – Dental USA	Yes	1/1/11
Example Health Plan	Insured	Insurer- CareFree BCBS	No	

List all employees with access to PHI. Provide HIPAA HITECH training date for each, as well as publication date of HIPAA materials.

Employee Name	Date of Training	Publication Date of HIPAA Material (updated periodically)	GHP Functions Assigned
Example John Doe	1/1/14	1/1/14	Routine enrollment administration
Example Jane Doe	1/1/14	1/1/14	Privacy Officer

HIPAA

Acknowledgement of the HIPAA and HITECH Privacy and Security Policy

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations ("the Privacy Rule") amended by the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH or Security Rule) restrict the ability to use and disclose Personal Health Information (PHI).

Various states have passed similar laws related to personal information we gather and the risk of identity theft.

The HIPAA and HITECH Privacy and Security Policy is intended to comply with the requirements mandated by law. Compliance with this Policy is important.

_____

I have undergone training regarding (a) the basic concepts of the Federal Privacy and Security Rule, (b) state laws that protect data that can be used for identity theft, and (c) the HIPAA and HITECH Privacy and Security Policy. This training addressed (d) how these items affect my job.

I agree to comply with the Privacy and Security Policy and will disclose Participant data solely in compliance with that Policy.

I have read, understand, and agree to comply with the Privacy and Security Policy.

_____ _____

Employee Signature Date

_____

First and Last Name Printed

HIPAA

Employee Authorization to Allow Disclosure of Protected Health Information (PHI)

Employer: _____

Employee Name: _____

- Date of Birth _____
- Daytime Phone: _____
- Email Address:_____

I hereby authorize my employer to allow _____ (Identify the person or organization in detail) access to my Personal Health Information for the following purpose:

_____

_____

_____

The following PHI may be released per this Authorization (describe the PHI that may be released):

_____

_____

_____

Access to my Personal Health Information is limited as follows (describe any PHI that may not be released):

_____

_____

_____

I understand I may revoke this Authorization in writing at any time.

This Authorization is to remain in full force and effect until my employer receives written notification from me of its revocation, or it will expire on _____. If left blank the Authorization will remain in effect for 10 days from date of signature below.

Failure to allow this or any other Authorization will in no way affect the Plan benefits I receive.

Employee Signature: _____ Date: _____

First and Last Name Printed: _____