

# HIPAA Privacy Compliance Manual



**TOTAL ADMINISTRATIVE SERVICES CORPORATION**

AgriPlan  
BizPlan  
COBRAToday  
DirectPay  
FlexSystem  
MAPP  
PHiEd

## Purpose of this Manual

*This publication provides authoritative and accurate information regarding requirements of the Health Insurance Portability and Accountability Act (HIPAA) and its implementing regulations. It is provided with the understanding that neither Total Administrative Services Corporation, its employees, or its owners are engaged in rendering legal, accounting, or other professional services, and that no such service or advice is being offered herein. When necessary, such legal advice or other expert assistance should be sought from a competent professional. If you use the sample documents contained herein as a starting point for your own documents, you should seek the advice of legal counsel prior to the reliance thereon.*

# Contents

Purpose of this Manual ..... 2

HIPAA – General Overview ..... 4

Privacy ..... 4

Electronic Data Interchange ..... 7

Security ..... 7

Document Instructions ..... 7

HIPAA Resources ..... 9

Identifier Worksheet ..... 10

HIPAA Privacy Policy ..... 11

HIPAA Notice Of Privacy Practices ..... 19

HIPAA Internal Privacy Use and Disclosure Procedures ..... 24

HIPAA Firewall Protections ..... 36

BUSINESS ASSOCIATE AGREEMENT ..... 37

HIPAA Implementation List ..... 41

## Purpose of this Manual

This manual provides you with the tools necessary for compliance with the Health Insurance Portability and Accountability Act. This guide applies only to the Privacy requirements under HIPAA and only to the services offered by TASC (HRA, FSA, etc.).

This guide is broken down into several different components. The first, a general outlook of the rules, is not meant to be all inclusive. Employers are strongly encouraged to research the privacy rules and to seek legal advice regarding their compliance efforts. Secondly, we have included various forms that have been created for your use, but should be used as a guide only. These documents, are required under the Privacy Rules and are included along with concise instructions for their use.

## HIPAA – General Overview

In 1997 the Health Insurance Portability and Accountability Act (HIPAA) was enacted. It includes administrative simplification regulations or mandates that are applicable to various health plans and medical reimbursement plans, including Cafeteria Plans. These regulations were designed to ensure the privacy and confidentiality of client health information, otherwise known as Protected Health Information (PHI).

The requirements under HIPAA are broken down into three different categories:

1. The Privacy of health information.
2. The Electronic Data Interchange of health information.
3. The Security of health information.

## Privacy

HIPAA defines those who may be authorized for access to health information created or maintained by certain covered entities. It focuses on the right of individuals to determine how their information is to be used or disclosed to others and promotes the protection of privacy of certain health care information. Large plans must comply by April 14, 2003; small plans have until April 2004 to comply.

The Protected Health Information (PHI) that the HIPAA rules intend to protect includes:

- Information that relates to an individual's medical condition, the provision of medical care for the individual, or the payment for that individual's health care.

## HIPAA Privacy Compliance Manual

- Health coverage option or category, along with enrollment and premium payment information as well as information relating to a health condition and treatment.
- Information that identifies the individual to whom it relates and that is created or received by a covered entity or employer, with the exception of education records and employment records created or maintained by the employer.

As an example, enrollment or dis-enrollment claims status and payment information relating to an employee is health information that is subject to the HIPAA rules.

Employers should understand why their Plan is subject to these rules. According to HIPAA, three entities are subject to these rules. First is a *health care provider*, broadly defined as a provider of medical or other services or one that furnishes medical or health care services or supplies, or any other entity that furnishes, bills, or is paid for health care in the normal course of business.

The second entity is a *health care clearinghouse*. This public or private entity processes, or facilitates the processing of, health information received from another entity. The third entity is a *health plan*. The definition of a health plan includes a long list of commonly known health plans, such as HMO's, Medicare supplement policies, Medicaid, health insurance issuers, ERISA plans, etc. The health care flexible spending account offered under a Cafeteria Plan and a Health Reimbursement Arrangement are technically defined as ERISA plans, and are therefore subject to these rules.

The regulations indicate that technically the "Plan" is the covered entity responsible for compliance. As the "Plan" has no workforce, indirectly, the sponsor of the Plan will be responsible for the compliance efforts. Employers are defined as the Plan sponsor and therefore, are ultimately responsible for compliance.

The HIPAA rules recognize that many covered entities hire other entities to perform functions relating to their health plans. Pursuant to HIPAA, these entities -- called Business Associates -- need to access and use individually-identifiable health information in connection with their Plan administrative duties. Although business associates are not covered entities, the information that is disclosed and/or used by them must be protected. A Business Associate is defined as a person, or entity who:

- Performs or assists in performing a function or activity involving the use and disclosure of individually-identifiable health information (including claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; or repricing) or involving any other function or activity regulated by HIPAA's administrative simplification rules.
- Provides legal, accounting, actuarial, consulting, data aggregations, management, accreditation, or financial services, where the performance of such services involves forwarding individually-identifiable information to the service provider.

Generally, a Third Party Administrator offering administrative services associated with a health flexible spending account or a Health Reimbursement Arrangement is deemed a business associate. A covered entity that discloses PHI to a business associate must enter into a contract with its business associates. In other words, TASC must enter into a business associates agreement with all employers who utilize an of TASC's administrative services that are subject to HIPAA. We have created this Agreement and it is included in this manual.

*It should be stressed that if an employer/Plan sponsor utilizes outside vendors who may meet one of the two items above, the employer should execute a business associate agreement with that vendor. For example, if an employer utilizes an outside accountant to audit their medical reimbursement account, and this vendor has access to PHI, then the employer must establish an official business associate agreement with that accountant. Such business associate agreements are separate and apart from the agreement you have with TASC; therefore TASC is not responsible for creating that agreement.*

### **Privacy Rules**

The below serves as a general overview. It is meant to give employers an idea of actions to take in their compliance efforts. Pursuant to these rules, the enclosed Notice of Privacy Practices allows for the inclusion of certain disclosures that are part of the Plan's administrative function. This includes an employer's inquiries regarding the status of an employee's claim or its payment, enrollment information, etc. It allows for sharing information with a family member who is inquiring about the same information.

The privacy rules include three core requirements. Some highlights follow:

#### **1. Use and Disclosure Rules**

All covered entities must obtain specific authorizations for most types of uses or disclosures of health information, other than uses and disclosures for treatment, payment, and health care operations. Authorizations must be informed and voluntary, and must meet specific technical requirements. Some Public Policy exceptions apply. Special rules apply when a group health plan shares information with a plan sponsor.

#### **2. Individual Rights, Including Privacy Notices**

Individuals, including Plan Participants, must be able to access their records and to request changes; they may also receive an accounting of disclosures other than those disclosures for treatment, payment, and health care operations or disclosures made to the individuals themselves or pursuant to an authorization. Providers and health plans must provide individuals with a notice of the entity's Privacy Practices.

### **3. Administrative Safeguards**

Covered entities must implement written privacy procedures and appropriate safeguards. Specific requirements include designating a privacy official, training employees, establishing a process by which employees can lodge complaints, and developing a system of sanctions for those who violate the rules.

## **Electronic Data Interchange**

Covered entities and their business associates that engage in particular specified transactions must comply with rules designed to standardize their format and content. They also must use uniform codes to identify medical conditions and procedures. Due date for compliance is October 2003.

## **Security**

Covered entities that conduct electronic transactions must maintain reasonable and appropriate safeguards to ensure the integrity and confidentiality of health information. These precautions aim to protect against threats to security or unauthorized uses or disclosures of information, and to otherwise ensure compliance by officers and employees alike. A due date for compliance for large Plans is April 2005 and for small Plans is April 2006.

TASC Plans and/or transactions are exempt from the Electronic Data Interchange (EDI) rules. With no due date in the immediate future, we will revisit the Security Rules at a later time. All enclosed information applies to the Privacy Rules only.

## **Document Instructions**

As mentioned earlier, this Manual provides you with the tools necessary to implement the items mentioned in the Privacy Rules Section. All included communications reflect the requirements listed earlier in this document. The following list of these communications includes instructions for their use.

### **Identifier Worksheet (Refer to page 10)**

The Identifier Worksheet identifies several important items under the Privacy Rules, and is related to the Plan offered by the employer.

Most fields have been completed. The Plan's contact person must complete the name of the Plan, the first field. The first person listed should be the contact person for the Plan. Also list any others who may have access, such as others from the benefits or Human Resources Department, any managers, any employees from the Information Systems Department, etc.

You must also identify any external vendors with access to employees' health information. This includes any external CPA who may review your Plan's books or any third party who may assist the employer or the employees with administrative functions for the Plan. A thorough list of all such vendors is important, as the employer may need to enter into a Business Associates Agreement with these individuals.

### **Privacy Policy (Refer to page 11)**

This sample HIPAA Privacy Policy addresses the requirements that must be satisfied by the Plan and by the employer/plan sponsor in order for the Plan to provide PHI to the sponsor for any administrative functions associated with the Plan.

It is necessary that the employer elect a Privacy Official. While in most cases this will be the contact person for the Plan, the employer may elect a different individual.

This notice must be maintained with the Plan (or employer) and may reference other procedures that must be implemented. We have not provided sample documents for these procedures because their magnitude is so minuscule. Employer/Plan Sponsors are responsible for their implementation.

### **Notice of Privacy Practices (Refer to page 19)**

This sample Notice of Privacy Practices satisfies the Privacy rule that require the Plan to provide this notice to employees whose health information will be used or maintained by the employer. It describes the use and disclosures of the health information as well as the employee's rights, and outlines the employer's legal duties with respect to the health information.

This notice must be distributed to all employees who are currently eligible to participate in the Plan, including eligible employees who elect not to participate. This notice also should be distributed to any new employees who become eligible to participate in the Plan.

Finally, while the employer should contact the Plan's contact person with any questions, employees should contact the employer with any questions.

### **Internal Policy and Procedures (Refer to page 24)**

This sample form may be altered to serve a specific situation and may be used as a guide for creating your own document. These internal procedures address the steps that employees must take when asked to provide PHI to an individual or external entity (such as a group of employees performing Plan administrative functions). These procedures should be reviewed by all employees identified in the worksheet. It is a document that is maintained by the employer.

### **Firewall Protections and Safeguards (Refer to page 36)**

Employers/Plan Sponsors are required to implement "firewalls" in order to prevent PHI from being used impermissibly. The term "firewall" is defined here differently than when used in the computer world. For our purpose, firewall includes the creation of an internal procedure to identify who has access to PHI. This will likely be the same individuals as those identified on the "Identification Worksheet."

To assure compliance with HIPAA requirements, those employees identified are required to review the employer's Privacy Policy as well as the Procedures outlined herein. Once complete, the employer will maintain a file of these forms.

### **Business Associate Agreement (Refer to page 37)**

A Business Associate is an outside entity or person who assists the employer with certain administrative functions relating to their Plan. Business associates often need to access and use PHI on behalf of the covered entity for which they are providing services. Generally, Third Party Administrators are considered Business Associates.

Although business associates are not covered entities, the information disclosed to them and/or used by them must be protected. The Privacy Rules require that covered entities enter into a Business Associates Agreement with those vendors that are performing functions related to their Plan. We have created and included a Business Associates Agreement that specifically details TASC's services provided to you as the Plan sponsor. **Unlike the other forms in this manual, the Business Associates Agreement should be used as is. Please remove the Agreement, sign it and maintain it for your files.** TASC has already signed the Agreement, signifying execution of the Agreement. All that is needed to finalize the Agreement is for you to add your signature.

## **HIPAA Resources**

As we stated early in this document, this publication is designed to provide authoritative and accurate information regarding requirements of the Health Insurance Portability and Accountability Act (HIPAA) and its implementing regulations. For legal advice and/or other expert assistance, seek the services of a competent professional.

For resources available on the Internet, try the following sites:

- Centers for Medicare and Medicaid <http://cms.hhs.gov/hipaa/>
- Employee Benefit Institute of America (EBIA) <http://www.ebia.com/index.jsp>
- Thompson's Publishing Group <http://www.thompson.com/index.html>

### **Contacting TASC**

If required, Client support is available from TASC Monday through Friday CST 8am – 5pm. Please contact TASC at 1-800-422-4661, and press 1 for Client Services. E-mail TASC at [service@tasconline.com](mailto:service@tasconline.com).



## Identifier Worksheet

### HIPAA Privacy Rules

1. **Identify the name of the Plan:** \_\_\_\_\_
  
2. **Identify health information received or created by the Plan:** (Check all that apply.)
  - Enrollment and dis-enrollment by employee.
  - Claims adjudication.
  - Claims payment.
  
3. **List internal personnel with access to the above health information:**
  - a. \_\_\_\_\_
  - b. \_\_\_\_\_
  - c. \_\_\_\_\_
  - d. \_\_\_\_\_
  
4. **List external vendors with access to the above health information:**
  - a. TASC
  - b. \_\_\_\_\_
  - c. \_\_\_\_\_
  - d. \_\_\_\_\_

**Describe known uses for the health information:**

Plan enrollment.  
Claim review.  
Claims payment.



## HIPAA Privacy Policy

\_\_\_\_\_ (insert company name) sponsors a Plan subject to the HIPAA Privacy Rules. Certain employees may have access to the individually-identifiable health information of Plan Participants as it relates to the administrative functions of the Plan.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations restrict the company's ability to use and disclose protected health information:

Protected health information means information that is created or received by the Plan and (a) relates to the past, present, or future physical or mental health or condition of a participant; (b) relates to the provision of health care to a participant; (c) relates to the past, present, or future payment for the provision of health care to a participant; or (d) identifies the participant and suggests a reasonable likelihood that the information might be used to identify the participant. Protected health information includes information of persons living or deceased.

The Plan intends to fully comply with HIPAA's requirements. Those with access to PHI must comply with this policy. The Plan reserves the right to amend or change this policy at any time without notice. To the extent that this policy establishes requirements and obligations above and beyond those required by HIPAA, the policy shall not be binding upon the company. This policy does not address requirements under other federal or state laws.

## Plan Responsibilities

### 1. Privacy Official and Contact Person

\_\_\_\_\_ (name of employee appointed as the Privacy Official) will be the Privacy Official for the Plan and as such will be responsible for the development and implementation of policies and procedures relating to privacy, including but not limited to this Policy and the Company's HIPAA policies and procedures. The Privacy Official will also serve as contact person for Participants who have questions, concerns, or complaints about the privacy of their PHI.

### 2. Education and Training

This company will inform and educate all employees with access to PHI about its various privacy policies and procedures.

### 3. Safeguards and Firewall

The company will establish, on behalf of the Plan appropriate safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's Privacy rules. Safeguards include limiting access to information by creating computer firewalls. Other safeguards include locking doors on filing cabinets. Firewalls will ensure that only authorized employees may access PHI, that they may access only the minimum amount of PHI necessary for plan administrative functions, and that they may not further use or disclose PHI.

### 4. Privacy Notice

The Privacy Official is responsible for developing and maintaining a notice of the Plan's privacy practices that describes the use and disclosure of PHI, the individual's rights, and the Plan's legal duties with respect to PHI. This notice will inform Participants that the company will have access to PHI in connection with Plan administrative functions. The privacy notice will also provide a description of the company's complaint procedures, along with the name of the contact person to whom complaints may be voiced.

The Notice of Privacy Practice must be provided to any new employee at the time of Plan enrollment and within 60 days after a material change has been made to the notice. The employer should also provide notice of availability of the privacy notice at least every three years.

### 5. Complaints

The Privacy Official will be the Plan's contact person for receiving complaints and concerns. This person will be responsible for creating a process for individuals to lodge complaints and for creating a system for handling such complaints.

### 6. **Violations**

Sanctions for using or disclosing PHI in violation of this HIPAA Privacy Policy will be imposed in accordance with the employer's discipline policy, up to and including termination.

### 7. **Mitigation of Inadvertent Disclosure of PHI**

To the extent possible the employer shall mitigate any harmful effects from use or disclosure of an individual's PHI in violation of the set policies and procedures. As a result, if an employee becomes aware of a disclosure of protected health information, the Participant should immediately contact the Privacy Official so that steps can be taken to expeditiously mitigate any harm to the Participant.

### 8. **No Intimidating or Retaliatory Acts; No waiver of HIPAA Privacy**

No employee may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA. No individual shall be required to waive his or her privacy rights under HIPAA as a condition of treatment, payment, enrollment, or eligibility.

### 9. **Plan Document**

The Plan Document shall include provisions for describing both permitted and required company uses and disclosures of PHI for Plan administrative purposes. Specifically the Plan Document shall require that the employer:

- Not use or further disclose PHI other than as permitted by the document or required by law.
- Ensure that any agents or subcontractors to whom it provides PHI agree to the same restrictions and conditions that apply to the Company.
- Not use or disclose PHI for employment-related actions or in connection with any other employee benefit plan.
- Report to the Privacy Official any use or disclosure of the information that is inconsistent with the permitted uses or disclosures.
- Make PHI available to Plan Participants, consider their amendments and, upon request, provide them with an accounting of PHI disclosures.
- Upon request, make available to DHHS the company's internal practices and records relating to the use and disclosure of PHI received from the Plan.
- If feasible, return or destroy all PHI received from the Plan and retain no copies of such information when no longer needed for their original purpose, unless such return or destruction is not feasible, or would limit subsequent uses and disclosures.

The Plan Document must also require the Company to certify to the Privacy Official that the Plan Documents have been amended to include the above restrictions and that the Company agrees to those restrictions and provides adequate firewalls.

### **10. Documentation**

The Plan's and the Company's Privacy Policies and procedures shall be documented and maintained for at least six years. Policies and procedures must be changed as necessary or appropriate to comply with changes in the law, standards, requirements, and implementation specifications (including changes and modifications in regulations). Any changes to policies or procedures must be promptly documented.

If a change in law impacts the privacy notice, the Privacy Policy must be revised promptly and made available. Such a change is effective only with respect to PHI created or received after the effective date of the notice.

The Plan and the Company shall document certain events and actions relating to an individual's privacy rights.

The documentation of any policies and procedures, actions, activities, and designations may be maintained in either written or electronic form. Covered entities must maintain such documentation for at least six years.

**Policies on Use and Disclosure of PHI**

**1. Use and Disclosure Defined**

The Company and the Plan will use and disclose PHI only as permitted under HIPAA. The terms are defined as follows:

Use: The sharing, employment, application, utilization, examination, and/or analysis of individually-identifiable health information by any person working for or within the benefits department of the Company, or by a Business Associate of the Plan.

Disclosure: For information that is PHI, disclosure means any release, transfer, provision of access to, or divulging in any other manner of individually-identifiable health information to a person or persons not employed by or working within the Company’s Benefits Department.

**2. Workforce Must Comply with Company’s Policy and Procedures**

All members of the Company’s workforce with access to PHI (described at the beginning of the Policy and referred to herein as “employees”) must comply with this Policy and with the Company’s more detailed use and disclosure procedures, which are set forth in a separate document.

**3. Who has Access to PHI**

The following employees have access to PHI: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**4. Permitted Uses and Disclosures – Payment and Health Care Operations**

PHI may be disclosed for the Plan’s own payment purposes, and PHI may be disclosed to another entity for the covered entity’s payment purposes.

Payment includes activities undertaken to obtain Plan contributions or to determine or fulfill the Plan’s responsibility for providing benefits under the Plan or activities to obtain or provide reimbursement for health care. Payment also includes:

- Eligibility and coverage determinations, including coordination of benefits and adjudication of health benefit claims.
- Risk adjusting based on enrollee status and/or demographic characteristics.
- Billing, claims management, collection activities and/or obtaining payment under a contract for reinsurance and related health care data processing.

PHI may be disclosed for purposes of the Plan's own health care operations. PHI may be disclosed to another covered entity for quality assessment and improvement, for case management, or for health care fraud and abuse detection programs, if the covered entity has a relationship with the Participant and the PHI requested pertains to that relationship.

Health care operations means any of the following activities to the extent that they relate to Plan administration:

- Conducting quality assessment and improvement activities.
- Reviewing health care performance.
- Underwriting and premium rating.
- Conducting or arranging for medical review, legal services, and auditing functions.
- Business planning and development.
- Business management and general administrative activities.

### **5. PHI Disclosures that are Permitted**

While PHI may be disclosed in various situations without a Participant's authorization, the employer's policy and procedure on use and disclosure should describe any specific requirements that must be met

before these types of disclosures may be made. The requirements include prior approval of the Company's Privacy Official. Disclosures are permitted under the following circumstances:

- Victims of abuse, neglect or domestic violence.
- Judicial and administrative proceedings.
- Law enforcement purposes.
- Public health activities.
- Health oversight activities.
- Decedents.
- Cadaveric organ, eye, or tissue donation purposes.
- Certain limited research purposes.
- Serious threats to health and/or safety.
- Specialized government functions.
- Workers' compensation programs.

PHI may be disclosed for any purpose if the Participant provides an authorization that satisfies all of HIPAA's requirements. All uses and disclosures made pursuant to a signed authorization must be consistent with the organization's terms and conditions.

### 6. "Minimum" Necessary Requirements

When PHI is used or disclosed, HIPAA requires that the information disclosed must be limited to the "minimum necessary" to accomplish the purpose of the use or disclosure. The minimum necessary standard does not apply to any of the following:

- Uses or disclosures made to the individual.
- Uses or disclosures made pursuant to a valid authorization.
- Disclosures made to the DOL.
- Uses or disclosures required by law.
- Uses or disclosures required to comply with HIPAA.

Employees may disclose PHI to the Plan's business associates and allow the Plan's business associates to create or receive PHI on its behalf. However, prior to doing so, the Plan must first obtain assurances from the business associate that it will appropriately safeguard the information. Before sharing PHI with outside consultants or contractors who meet the definition of a business associate, employees must contact the Privacy Official and verify that a business associate agreement is in place.

## Individual Rights

### 1. Access to PHI and Requests for Amendment

HIPAA gives Participants (or defined business associates) the right to access and obtain copies of their PHI (or its business associates) which should be maintained in a designated records set. HIPAA also permits Participants to amend their PHI. The Plan will provide access to PHI and will consider requests for amendments that Participants submit in writing.

A designated record set is a group of records maintained by or for the Company and includes an individual's enrollment, payment, and claims adjudication record. Or if other PHI is used, in whole or in part, by or for the Plan to make coverage decisions about an individual.

### 2. Accounting

An individual may request an accounting of certain disclosures of his or her own PHI. This right extends to disclosures made in the last six years, and to other disclosures, such as:

- To carry out treatment, payment, or health care operations.
- To individuals about their own PHI.
- Incidental to an otherwise permitted use or disclosure.
- Pursuant to an authorization.
- For creating a facility directory, for disseminating to persons involved in the patient's care, or other notification purposes.
- As part of a limited data set.
- For national security or law enforcement purposes.

The Plan shall respond within 60 days to an accounting request. If the Plan is unable to comply, it may extend the period by 30 days, as long as it provides the Participant notice of such a delay within the original 60-day period.

The accounting must include the date of the disclosure, the name of the receiving party, a brief description of the information disclosed, and a brief statement of the purpose of the disclosure. The first accounting in any 12 month period shall be provided free of charge. The Privacy Official may impose reasonable production and mailing reimbursement requests for subsequent accounting.



## HIPAA Notice Of Privacy Practices

### The Privacy of Your Health Information

Your employer understands that your health information is personal. We are committed to protecting this information. We created a record of the health care claims reimbursed under the Plan, along with other related items that are used for administrative purposes. This notice applies to all health records that are maintained and informs you about the ways in which we may use and disclose your medical information. It also describes our obligations and your rights regarding the use and disclosure of medical information.

By law, your employer is required to:

1. Make sure that your medical information is kept private.
2. Give you this notice of our legal duties and Privacy Practices with respect to your medical information.

### Use and Disclosure of Your Medical Information

The following identifies the different ways that we use and disclose your medical information.

**Payment.** We may use and disclose your medical information to determine eligibility for Plan benefits, to facilitate payment for treatment and services, to determine benefit responsibility under the Plan, or to coordinate Plan coverage.

**As required by law.** We will disclose your medical information when required to do so by federal, state or local law.

**To avert a serious threat to health or safety.** We may use and disclose your medical information when necessary to prevent a serious threat to your health and safety or that of the public.

### Special Situations

**Discloser to other health plan sponsors.** Your information may be disclosed to another health Plan maintained by the employer for purposes of facilitating claims payments under that Plan. In addition, your medical information may be disclosed solely for purposes of administering benefits under the Plan.

**Organ and tissue donation.** If you are an organ donor, we may release your medical information to organizations that handle or procure organ, eye, or tissue transplants or to an organ donation bank, as necessary to facilitate organ or tissue donation and transplant.

**Military and veterans.** If you are a member of the armed forces, we may release your medical information as required by military command authorities. We may also release medical information about foreign military personnel to the appropriate foreign military authority.

**Workers' compensation.** We may release your medical information for workers' compensation or similar programs. These programs provide benefits for work-related injuries or illness.

**Public health risks.** We may disclose medical information about you for public health activities. These activities generally include the following:

- To prevent or control disease, injury, or disability.
- To report births and deaths.
- To report child abuse or neglect.
- To report reactions to medications or problems with products.
- To notify people of recalls of products they may be using.
- To notify a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition.
- To notify the appropriate government authority if we believe a patient has been the victim of abuse, neglect, or domestic violence. We will make this disclosure only with your permission or when required or authorized by law.

**Health oversight activities.** We may disclose your medical information to a health oversight agency for activities authorized by law. These oversight activities include audits, investigations, inspections, and licensure. These activities are necessary for the government to monitor the health care system and government programs, and for compliance with civil rights laws.

**Lawsuits and disputes.** If you are involved in a lawsuit or a dispute, we may disclose your medical information in response to a court or administrative order. We may also disclose your medical information in response to a subpoena, discovery request, or other lawful process, but only if efforts have been made to tell you about the request and only if you have not sought a prior order protecting the information requested.

**Law enforcement.** We may release your medical information if asked to do so by a law enforcement official under the following circumstances:

- In response to a court order, subpoena, warrant, summons, or similar process.
- To identify or locate a suspect, fugitive, material witness, or missing person.
- About the victim of a crime if, under certain limited circumstances, we are unable to obtain the person's agreement.
- If the information is about a death that may be the result of criminal conduct.
- If the information is about criminal conduct at the hospital.
- In emergency circumstances to report a crime; the location of the crime or victims; or the identity, description, or location of the person who committed the crime.

**Coroners, medical examiners and funeral directors.** We may release your medical information to a coroner or medical examiner. We may also release medical information about hospital patients to funeral directors as necessary for them to carry out their duties.

**National security and intelligence activities.** We may release your medical information to authorized federal officials for intelligence, counterintelligence, and other national security activities authorized by law.

**Inmates.** If you are an inmate of a correctional institution or under the custody of a law enforcement official, we may release your medical information to the correctional institution or law enforcement official. This release would be necessary (1) for the institution to provide you with health care; (2) to protect the health and safety of you and others; or (3) for the safety and security of the correctional institution.

### Employee Rights

**Right to inspect and copy.** You have the right to inspect and copy medical information that may be used to make decisions about your plan benefits. To do so, you must first submit your request in writing to your employer. If you request a copy of the information, we may charge a fee for the costs of copying, mailing, or other supplies associated with your request. We may deny your request to inspect and copy in certain very limited circumstances. If you are denied access to medical information, you may request that the denial be reviewed.

**Right to amend.** If you feel that the medical information we have about you is incorrect or incomplete, you may ask us to amend it. You have the right to request an amendment for as long as the information is kept by or for the Plan. Your request in writing must detail reasons for the request and be submitted to the Plan's contact person.

We may deny any request for an amendment that is not in writing or does not include a reason for the request. In addition, we may deny your request if you ask us to amend information that:

- Is not part of the medical information kept by or for the Plan.
- Was not created by us, unless the person or entity that created the information is no longer available to make the amendment.
- Is not part of the information which you would be permitted to inspect and copy.
- Is accurate and complete.

**Right to account disclosures.** You have the right to request an “accounting of disclosures” where such disclosure was made for any purpose other than treatment, payment, or health care operations.

To request this list of accounting disclosures, you must submit your request in writing to the Plan’s contact person. Your request must state a time period no longer than six years and not prior to April, 2004. Your request should indicate in what form you want the list (example – paper or electronically). The first list you request within a 12 month period will be free. For additional lists, we may charge you for the costs of providing the lists. We will notify you of the cost involved and you may choose to withdraw or modify your request at that time, before any costs are incurred.

**Right to request restrictions.** You have the right to restrict or limit the medical information we use or disclose about you for treatment, payment, or health care operations. You also have the right to limit the medical information we disclose about you to someone who is involved in your care or in the payment for your care, such as a family member or friend. We are not required to comply with your request.

All restrictions requests must be made in writing. In your request, you must tell us: (1) what information you want to limit; (2) whether you want to limit our use, disclosure, or both; and (3) to whom you want the limits to apply.

**Right to request confidential communication.** You have the right to request that we communicate with you about medical matters in a certain way or at a certain location. To request confidential communication, you must submit your written request to the Plan’s contact person. We will not ask you the reason for your request, and we will accommodate all reasonable requests. Your request must specify how or where you wish to be contacted.

**Right to a paper copy of this notice.** You have the right to a paper copy of this notice. Even if you have agreed to receive this notice electronically, you are still entitled to a paper copy of this notice. You may ask the Plan’s contact person for a copy of this notice at any time.

### **Changes to This Notice**

The employer reserves the right to change this notice. We reserve the right to make the revised or changed notice effective regarding medical information we already have about you as well as regarding any information we receive in the future. The Plan is required to abide by the terms of the notice currently in effect. If a revision is made, it will be provided to the Participant by mail or other specific means.

### **Complaints**

If you believe your privacy rights in respect to this Plan have been violated you may file a complaint with the Plan. To file a complaint, contact the Plan's contact person. All complaints must be submitted in writing.

### **Other**

Other uses and disclosures of medical information not covered by this notice or the laws that apply to us will be made only with your written permission. If you provide us permission to use or disclose your medical information, you may revoke that permission, in writing, at any time in the future. If you revoke your permission, we will no longer use or disclose your medical information for the reasons covered by your written authorization. You must understand that we are unable to take back any disclosures we have already made with your permission, and that we are required by law to retain our records of the care that we provided you. The effective date of this notice is April 14, 2003.



## HIPAA Internal Privacy Use and Disclosure Procedures

### Introduction

\_\_\_\_\_ (the employer) sponsors a Group Health Plan. Employees may have access to the individually-identifiable health information of Plan Participants, on behalf of the Plan itself, on behalf of the employer, or for administrative functions related to the Plan.

Protected health information included under the Act is defined as the following:

Protected health information means information that is created or received by the Plan and (a) relates to the past, present, or future physical or mental health or condition of a participant; (b) relates to the provision of health care to a participant; (c) relates to the past, present or future payment for the provision of health care to a participant; or (d) identifies the participant and suggests a reasonable likelihood that the information might be used to identify the participant. Protected health information includes information of persons living or deceased.

We at \_\_\_\_\_ intend to fully comply with HIPAA's requirements. Those with access PHI must comply with this policy. The company reserves the right to amend or change this policy at any time without notice. To the extent that this policy establishes requirements and obligations above and beyond those required by HIPAA, the policy shall not be binding upon the company. This policy does not address requirements under other federal or state laws.

### Procedures for Use and Disclosure of PHI

#### I. How Use and Disclosure are Defined

The employer and the Plan will use and disclose PHI only as permitted under HIPAA. Use means the sharing, employment, application, utilization, examination, or analysis of individually-identifiable health information by any person working for or with the employer's Benefits Department or by a Business Associate of the Plan.

Disclosures of information that is PHI, means any release, transfer, provision or access to, or divulging in any other manner any individually-identifiable health information to persons not employed by or working within the company's Benefits Department.

All employees of the employer who have access to PHI must comply with these procedures.

The employees with access to PHI as identified in the identifier worksheet, may use and disclose PHI for Plan administrative functions, and may disclose PHI to other employees with access to this information for Plan administrative functions. Employees with access may disclose PHI to employees with access in accordance with these procedures only.

### **II. Procedures on the use and disclosure of PHI: Payment and health care operations**

Payment records include activities undertaken to obtain Plan contributions, to determine or fulfill the Plan's responsibility for provision of benefits under the Plan, or to obtain or provide reimbursement for health care. Payment also includes:

- Eligibility and coverage determinations, including coordination of benefits and adjudication or subrogation of health benefit claims.
- Risk adjusting based on enrollee status and demographic characteristics.
- Billing, claim management, collection activities, obtaining payment under a contract for reinsurance, and related health care data processing.

Health care operations means any of the following activities to the extent that they are related to Plan administration:

- Conducting quality assessment and improvement activities.
- Reviewing health plan performance.
- Underwriting and premium rating.
- Conducting or arranging for medical review, legal services, and auditing functions.
- Business planning and development.
- Business management and general administrative activities.

### Procedure

- An employee may use and disclose a Plan Participant's PHI to facilitate the Plan's own payment activities or health care operations.
  - Disclosures must comply with the minimum necessary standard.
  - Disclosures must be documented in accordance with the appropriate procedure.
- An employee may disclose a Plan participant's PHI to another covered entity or health care provider so as to perform the other entity's payment activities. Disclosures may be made under the following circumstances:
  - Disclosures must comply with the minimum necessary standard.
  - Disclosures must be documented in accordance with the appropriate procedure.
- An employee may disclose PHI for purposes of the other covered entity's quality assessment and improvement, for case management or health care fraud and abuse detection programs, and/or if the other covered entity has a relationship with the individual and the PHI requested pertains to that relationship. Such disclosures are subject to the following:
  - The Privacy Official must approve the disclosure.
  - Disclosures must comply with the "minimum-necessary standard" (see page 14).
  - Disclosures must be documented in accordance with the appropriate procedure.
- Unless an authorization from the individual has been received, an employee may not use a Participant's PHI for the payment or operations of the company's non-health benefits (disability, workers' compensation, and life insurance). If an employee requires Participant's PHI for payment or health care operations of non-plan benefits, follow these steps:
  - Obtain an authorization.
  - Have the disclosure approved by the Privacy Official.
  - Ensure that the disclosure complies with the minimum-necessary standard.
  - Document the disclosure in accordance with the appropriate procedure.

### III. PHI Disclosures to Individuals and the Department of Health and Human Services

#### Procedure

There must be a request from the individual, who must follow the procedure for "Disclosures to Individuals Under Right to Access Own PHI." If there is a request from the DHHS, the employee must follow the procedure set forth in "Verification of Identity of Those Requesting Protected Health Information." The disclosure must be documented in accordance with the appropriate procedure.

## IV. Legal Disclosures of PHI

### Procedure

When an employee receives a request for disclosure of an individual's PHI and said request appears to fall within the aforementioned categories, the Privacy Official must be contacted. The disclosure must be approved by the Privacy Official and must comply with the minimum necessary standard. All disclosures must be documented in accordance with the appropriate procedure.

Disclosures about victims of abuse, neglect, or domestic violence can be met only if (a) the individual agrees with the disclosure; (b) if the disclosure is expressly authorized by statute or regulation (and the disclosure prevents harm to the individual); or (c) the individual is incapacitated and unable to consent, the information will not be used against the individual, and the information is necessary for an imminent enforcement activity.

Disclosures for judicial and administrative proceedings are covered if they are in response to an order of a court or administrative tribunal, or are a subpoena, discovery request, or other lawful process not accompanied by a court order or administrative tribunal. The individual must first have been given notice of the request, or the party seeking the information must have made reasonable efforts to receive a qualified protective order.

Disclosures to a law enforcement official for law enforcement purposes are permitted under the following conditions:

- Pursuant to a process and as otherwise required by law, but only if the information sought is relevant, the request is specific and limited to reasonable amounts, and it is not possible to use de-identified information.
- Information requested is limited information used to identify or locate a suspect, fugitive, material witness, or missing person.
- Information is about a suspected victim of a crime if the individual consents to the disclosure, or without the individual agreement, if the information is not to be used against the victim, if the need for the information is urgent, and if disclosure is in the individual's best interest.
- Information is about a deceased individual arising upon suspicion that the individual's death resulted from criminal conduct.
- Information sought constitutes evidence of criminal conduct that occurred on the Company's premises.

Disclosures are allowed to the appropriate public health authorities, to a health oversight agency, to a coroner or medical examiner about decedents, for cadaveric organ, eye or tissue donation purposes, and for certain limited research purposes. Disclosures also may be made to avert a serious threat to health or safety, for specialized government functions, and for worker's compensation programs.

### **V. Disclosures Pursuant to an Authorization**

#### **Procedure**

Any requested disclosure to a third party (not the individual to whom the PHI pertains) that does not fall within one of the categories for which disclosure is permitted or required (under the Use and Disclosure Procedures) may be made pursuant to an individual's authorization. When there is a disclosure via an authorization, the following procedures apply:

- Verify the individual's identity in accordance with the appropriate procedure.
  - Determine that the authorization is valid. It should be signed properly and dated, and must not be expired.
  - Include a description of the information to be used or disclosed, along with the name of the entity or person authorized to use or disclose the PHI.
  - Include the name of the recipient.
  - Include a statement regarding the individual's right to revoke the authorization and the procedure for such, along with a statement regarding the possibility for any subsequent re-disclosure of the information.
- A use or disclosure made pursuant to an authorization must be consistent with the terms of the authorization itself. And the disclosures must be documented in accordance with the appropriate procedure.

### **VI. Disclosures of PHI to Business Associate**

A Business Associate is an entity or person who performs or assists in performing a Plan function or activity involving the use and disclosure of PHI. A Business Associate is also one who provides legal, accounting, actuarial, consulting, data aggregations management, accreditation, or financial services, where the performance of such services involves giving the service provider access to PHI.

## **Procedure**

All uses and disclosures must be consistent with the Business Associate agreement. The disclosures must comply with the minimum necessary standards and must be documented in accordance with the appropriate procedure.

## **VII. Disclosures of PHI from spouses, family members and friends**

The Plan and employer will not disclose PHI to an individual's family and friends except as permitted by HIPAA.

## **Procedure**

If an employee receives a request for disclosure of an individual's PHI from an individual's spouse, family member, or personal friend, and the spouse, family member, or personal friend is either (1) the parent of the individual and the individual is a minor child; or (2) the personal representative of the individual, then their identity must be verified. The verification should comply with the appropriate procedure for individual access.

## **XIII. Disclosures of De-Identified Information**

De-identified information is health information that does not identify an individual and is not reasonably expected to be used to identify an individual. A covered entity can determine whether the information is de-identified in two ways: either by professional statistical analysis, or by removing 18 specific identifiers.

## **Procedure**

Obtain approval for the disclosure from the Privacy Official. The Privacy Official will verify that the information is de-identified. The Plan may freely use and disclose de-identified information, and de-identified information is not PHI.

### **IX. Verification of Identity of Those Requesting Protected Health Information**

Employees must take steps to verify the identity of individuals who request access to PHI. They must also verify the authority of any person who is to have access to PHI, if the identity or authority of said person is not known. Separate procedures are set forth below for verifying the identity and authority, depending on whether the request is made by the individual, by a parent seeking access to the PHI of his or her minor child, by a personal representative, or by a public official seeking access.

- When an individual requests access to his or her own PHI, the following steps should be followed:
  - Request a form of identification from the individual.
  - Verify that the identification matches the identity of the individual requesting access to the PHI.
  - Make a copy of the identification provided by the individual and file it with the individual's designated record set.
  - Disclosures must be documented in accordance with the appropriate procedure.
- When a parent requests access to the PHI of the parent's minor child, the following steps should be followed:
  - Seek verification of the person's relationship with the child and document the disclosure in accordance with the appropriate procedure.
  - When a personal representative requests access to an individual's PHI, the employee should require a valid power of attorney. A copy of this documentation should be made and filed with the individual's designated record set. And the disclosure must be documented in accordance with the appropriate procedure.
- If a public official requests access to PHI, and if the request is for one of the purposes set forth above in "Mandatory Disclosures of PHI" or "Permissive Disclosures of PHI," then the steps below should be followed to verify the official's identity and authority:
  - If the request is made in person, request presentation of an agency identification badge, other official credentials, or other proof of government status. Make a copy of the identification provided and file it with the individual's designated record set.
  - If the request is in writing, verify that the request is on the appropriate government letterhead.
  - If the request is by a person purporting to act on behalf of a public official, request a written statement (on appropriate government letterhead) that the person is acting under the government's authority, or other evidence or documentation of agency (such as a contract for services, memorandum of understanding, or purchase order), that establishes that the person is acting on behalf of the public official.

- Request a written statement of the legal authority under which the information is requested, or, if a written statement would be impractical, an oral statement of such legal authority. If the individual's request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or judicial or administrative tribunal, contact the Legal Department.
- Obtain approval for the disclosure from the Privacy Official.
- Document disclosures in accordance with the appropriate procedure.

### **X. Complying with the “Minimum-Necessary” Standard**

#### **Procedure for Disclosures**

- Identify recurring disclosures. For each recurring disclosure, identify the types of PHI to be disclosed, the types of person who may receive the PHI, the conditions that would apply to such access, and the standards for disclosures to routinely-hired types of Business Associates. Create a policy for each specific recurring disclosure that limits the amount disclosed to the minimum amount necessary.
- For all other requests for disclosures of PHI, contact the Privacy Official, who will ensure that the amount of information disclosed is the minimum necessary.

#### **Procedure for Requests**

- Identify recurring requests. For each recurring request, identify the information that is necessary for the purpose of the requested disclosure and create a policy that limits each request to the minimum amount necessary.
- For all other requests, the PO should be contacted, and should ensure that the amount of information requested is the minimum necessary.

A few exceptions do apply. The minimum necessary standard does not apply to use or disclosures made to the individual, made pursuant to an individual authorization, or made to DHHS, nor does it apply to use or disclosures required by law or those required to comply with HIPAA.

## **XI. Documentation**

### **Procedure**

Employees shall maintain certain items for a period of six years from the date the documents were created or were last in effect, whichever is later. These documents include the Notice of Privacy Practice, Individual Authorization, and all information relating to the specifics of a disclosure.

## **XII. Unknown Disclosures of PHI**

A covered entity must mitigate, to the extent possible, any harmful effects that become known of disclosing an individual PHI in violation of the policies and procedures set forth in this manual. The Privacy Official must be contacted immediately of any incorrect use or disclosure of PHI.

### **Procedures for Complying with Individual Rights**

#### **I. Request for Access**

A Designated Record set is a group of records maintained by or for the employer, and includes the enrollment, payment and claims adjudication record of an individual maintained by the Plan. It also includes other protected health information used, in whole or in part, by or for the Plan when making coverage decisions about an individual.

### **Procedure**

For disclosure of an individual's PHI, the employee must take the following steps:

- Verify the individual's identity.
- Determine whether the PHI is held in the designated record set.
- Determine whether an exception to the disclosure requirement might exist. See the PO as to whether any exception exists.

- Provide or deny the request within 30 days. If the PHI cannot comply with such a deadline, the deadline may be extended for 30 days by providing written notice to the individual within the original 30 day period.
  - A denial notice must contain the basis for the denial, a statement of the individual's right to request a review, and directions to the individual for filing a complaint concerning the denial.
  - Provide the information in a readable format. Or provide in a format agreed to by the employee.
- At the discretion of the employer, additional fees may be charged for copying, postage and preparation.
- Disclosures must be documented in accordance with the Documentation Requirements procedure.

## II. Request for Amendment

### Procedure

Upon Receipt of a request from an individual, from a parent of a minor child, or from a personal representative for an amendment to an employee's PHI in a designated record set, the employee must take the following steps:

- Verify the individual's identity.
- Determine whether the PHI at issue is held in the employee's designated record set. See the Privacy Official if the information does not seem to be held in designated record set.
- Determine whether the amendment is allowable under HIPAA's right to access.
- Determine whether the request for the amendment is appropriate.
- Respond to the request in 60 days by informing the individual whether the request has been accepted or denied. If a decision cannot be made within 60 days, the deadline may be extended for 30 more days.
- Upon acceptance of the amendment, make the change in the designated record set.
- Denied requests must do the following:
  - The PO must review the denial. The denial must include the reason for the denial, information about the individual's right to disagree, an explanation that the individual may ask that the request for amendment and its denial be included in future disclosures of the information, and directions for filing a complaint concerning the denial.
  - Under circumstances where the individual provides a statement of disagreement, include all specifics relating to the denial.

## III. Processing Request for an Accounting of PHI

### Procedure

Upon the receipt of a request for an account of disclosures the following procedures must be followed:

- Verify the identity of the individual procedure.
- Inform the individual that there may be a fee charged if the employees have requested this information more than once in the last twelve months.
- Respond to the request within 60 days by providing the accounting, or by informing the individual that there have been no disclosures that must be included in an accounting. The 60 day deadline may be extended for an additional 30 days by written notice.
- The accounting must include any disclosures made by the Plan or by a Business Associate for up to six years prior to the request. Disclosures not included are:
  - To carry out treatment, payment and health care operations.
  - To the individual about his/her own PHI.
  - Incidental to an otherwise permitted use or disclosure.
  - Pursuant to an individual authorization.
  - For specific national security or intelligence purposes.
  - To correctional institution or law enforcement when the disclosure was permitted without an authorization.
  - As part of a limited data set.
- The accounting must include the date of disclosure, the name of the entity or person to whom the information was disclosed, a brief description of the PHI disclosed, and a brief statement explaining the purpose for the disclosure.
- If the Plan has received a temporary suspension statement from a health oversight agency or a law enforcement official indicating that notice to the individual of disclosures of PHI would likely impede the agency's activities, then disclosure may not be required. The employee must contact the PO under these circumstances for more guidance.
- Accountings must be documented in accordance with the appropriate procedure.

## **IV. Processing Request for Confidential Communications**

### **Procedure**

In order for an individual to receive communications in an alternate format or location, the following steps must be followed:

- Verify the individual's identity as set forth in the appropriate procedures.
- Determine whether the request could endanger the individual.
- The employee should take steps to honor the request.
- If the request cannot be accommodated, the employees must contact the individual explaining why.
- All confidential requests will be maintained by the Privacy Officer.
- Requests and their dispositions must be documented in accordance with the appropriate procedure.

## **V. Processing Requests for Restriction on Use and Disclosures of PHI**

### **Procedure**

Upon the permission for access employees must adhere to the following steps regarding an individual's PHI:

- Verify the individual's identity in accordance with the appropriate procedure.
- Take steps to honor the request.
- If the request cannot be accommodated, the employee must contact the individual explaining why.
- Track all requests on use or disclosures.
- Notify all Business Associates that may have access to the individual's PHI of any agreed-upon restrictions.
- Document requests and their dispositions in accordance with the appropriate procedure.



## HIPAA Firewall Protections

\_\_\_\_\_  
**Name of Plan Sponsor**

\_\_\_\_\_  
**Date**

List employees who are involved in the administration of the Plan

_____	_____
_____	_____
_____	_____
_____	_____

The above employees are involved in the administration of the employer's Plan. They understand that their access will be limited to the minimum information necessary for them to perform their duties associated with the Plan.

These individuals are required to review and understand the employer's Privacy Policy as well as the outlined procedures the employer has adopted to comply with the HIPAA Privacy Requirements.



**TASC**

TOTAL ADMINISTRATIVE SERVICES CORPORATION

## **BUSINESS ASSOCIATE AGREEMENT**

**This Agreement**, is made this \_\_\_\_\_ day of \_\_\_\_\_, 200\_\_\_\_, by and between \_\_\_\_\_, (the “Covered Entity”), \_\_\_\_\_ sponsor of the Covered Entity (“Employer”), and Total Administrative Service Corporation (TASC), a Wisconsin corporation, hereinafter referred to as the “Business Associate.”

**Whereas**, The Employer sponsors a health plan and wishes to engage the services of the Business Associate with respect to the administration of said plan, and the Business Associate desires to provide said services;

### **I. Definitions**

- (a) *Business Associate*. Business Associate shall mean Total Administrative Services Corporation.
- (b) *Covered Entity*. Covered Entity shall be the party identified above.
- (c) *Individual*. Individual shall have the same meaning as the term “individual” in 45 CFR 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).
- (d) *Privacy Rule*. Privacy Rule shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, subparts A and E.
- (e) *Protected Health Information*. Protected Health Information shall have the same meaning as the term protected health information in 45 CFR 164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity.
- (f) *Required by Law*. Require by Law shall have the same meaning as the term require by law in 45 CFR 164.501.
- (g) *Secretary*. Secretary shall mean the Secretary of the Department of Health and Human Services or his designee.

## **Business Associate Agreement - Page 2**

**It is hereby agreed:**

### **II. Obligations and Activities of Business Associate.**

- (a) Business Associate agrees not to use or disclose Protected Health Information (PHI) other than as permitted by law.
- (b) Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the PHI other than as provided by this Agreement.
- (c) Business Associate agrees to report to Covered Entity any use or disclosure of the PHI of which it becomes aware that is not provided for by this Agreement.
- (d) Business Associate agrees to require any agent (including a subcontractor, to whom it provides PHI received from, or created or received by Business Associate on behalf of Covered Entity), to agree to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.
- (e) Business Associate agrees to provide access, at the request of Covered Entity, within thirty days (30) of a written request, to PHI in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an individual in order to meet the requirements under 45 CFR 164.524.
- (f) Business Associate agrees to make within a reasonable time any amendment(s) to PHI in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR 164.526 at the request of Covered Entity or of an individual.
- (g) Business Associate agrees to make internal practices, books, and records, including policies and procedures and PHI relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of Covered Entity if available to the Secretary; as designated by the Secretary, for Secretary's judgement of Covered Entity's compliance with the Privacy Rule.
- (h) Business Associate agrees to document such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to an individual's request for accounting of disclosures of PHI in accordance with 45 CFR 164.528.
- (i) Business Associate agrees to provide to Covered Entity or to an individual, in reasonable time and manner, information collected in accordance with Section (h) above, so as to permit Covered Entity to respond to an individual's request for an accounting of disclosures of PHI in accordance with 45 CFR 164.528.
- (j) Business Associate will implement administrative, physical, and technical safeguards (including written policies and procedures) that reasonably and appropriately protect the confidentiality, integrity, and availability of electronic PHI that it creates, receives, maintains, or transmits on behalf of a Covered Entity as required by the Security Rule.

### **III. Permitted Uses and Disclosures by Business Associate**

Business Associate may use PHI for its management, administration, data aggregation and legal obligations to the extent not prohibited by law. Business Associate may also use PHI to report violations of law to appropriate federal and state authorities, consistent with 164.502(j)(1), and to provide data aggregation services to Covered Entity as permitted by 45 CFR 164.504(e)(2)(i)(B).

**IV. General Uses and Disclosure Provisions**

Except as otherwise limited in this Agreement, Business Associate may use or disclose PHI on behalf of, or to provide services to, Covered Entity for purposes of fulfilling its service obligations to Covered Entity and Employer, if such use or disclosure of PHI would not violate the Privacy Rule or the minimum necessary policies and procedures.

**V. Obligations of Covered Entity**

- (a) Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.
- (b) Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.
- (c) Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

**VI. Permissible Requests by Covered Entity**

Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule unless otherwise provided for in this agreement.

**VII. Term and Termination**

- (a) Term. The Term of this Agreement shall be effective as of the date first written above, and shall terminate when all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy PHI, protections are extended to such information, in accordance with the termination provisions in this Section.
- (b) Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall provide an opportunity for Business Associate to cure the breach or end the violation. If Business Associate does not cure the breach or end the violation within a reasonable time, the Covered Entity may terminate this Agreement.
- (c) Effect of Termination.
  - (1) Except as provided in paragraph (2) of this section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to any PHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI.

**Business Associate Agreement - Page 4**

(2) In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction of PHI infeasible. Upon receipt of such written notice from Business Associate, the protections of this Agreement shall be extended to such PHI and shall limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

**VIII. Miscellaneous**

- (a) Regulatory Reference. A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended.
- (b) Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.
- (c) Survival. The respective rights and obligations of Business Associate under Section VI.C.2 of this Agreement shall survive the termination of this Agreement.
- (d) Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule.
- (e) Definitions. Terms used in this Agreement, but not otherwise defined shall have the same meaning as those terms in the Privacy Rule.

**In witness whereof**, each of the parties has hereunto signed their name or if acting as a business entity has caused its duly authorized officers or agents to execute this Agreement on its behalf on the date first written above.

**Covered Entity/Employer**

**Total Administrative Services Corporation:**

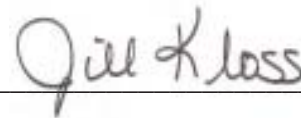
\_\_\_\_\_  
(Name)

\_\_\_\_\_  
(Name)

Jill Kloss

\_\_\_\_\_  
(Signature)

\_\_\_\_\_  
(Signature)





## HIPAA Implementation List

**Date Completed**

Complete Identification Work Sheet	_____
Review Educational Materials	_____
Distribute Privacy Practices	_____
Review Privacy Notice	_____
Review and File Policies and Procedures	_____
Sign Business Associate Agreement	_____
Review and Complete Firewall Protection Communication	_____



**TOTAL ADMINISTRATIVE SERVICES CORPORATION**

The information contained in this communication is confidential and is to be used by TASC employees and representatives for its intended purpose only.

© **Total Administrative Services Corporation**

2302 International Lane • Madison, WI 53704-3140 • 800-422-4661 • [www.tasconline.com](http://www.tasconline.com)