

PIERCE COUNTY
HIPAA PRIVACY POLICIES
AND PROCEDURES

CMS Health Plans Guide to HIPAA Privacy Policy

The HIPAA Privacy Policy that follows is for use by a County health care plan if it is a self-funded group health plan with 50 or more participants. For County governments, this may mean either a self-funded group health plan for County employees, or a self-funded group health plan offered as a Social or Human Services program to County residents, such as a General Assistance-Medical.

If the County purchases an insurance plan for its employees or for county beneficiaries of a county social or human services program, the County is a County as defined by HIPAA and not a covered entity. Counties have some HIPAA responsibilities, but the County or HMO that provides the insurance product has the responsibility for seeing to it that the County has put in place the necessary forms and other requirements.

As a covered entity, a self-insured plan makes County government responsible for the Plan's compliance with HIPAA's privacy requirements. The guide envisions that the plan will be administered by certain County employees who will have access to protected health information (PHI) in connection with their duties, regardless of the use of outside third party administrator (TPA) to perform most or even virtually all administrative functions related to the group health plan.

It is assumed that most Counties will elect to declare themselves a hybrid entity, with the establishment of a clear separation between the employees ("workforce" under HIPAA) who will have the use of and access to PHI as a part of their duties in regards to the administration of the group health plan (the covered component) and those whose job do not involve PHI; i.e., those who perform all the other tasks within the County.

This policy addresses (1) the requirements that must be satisfied by the Plan as a covered entity; and (2) the requirements that must be satisfied by the Plan and the County in order for the Plan to provide PHI to the County for Plan administrative functions. Furthermore, this policy addresses privacy requirements under applicable state and other federal laws.

CMS Health Plans Guide to HIPAA Privacy Policy

Table of Contents

	Page
Introduction.....	3
The Plan’s Responsibilities as Covered Entity	4
Privacy Official and Contact Person.....	4
Workforce Training	4
Technical, Physical and Firewall Safeguards	4
Privacy Notice.....	4
Complaints	5
Sanctions for Violations of Privacy Policy.....	5
Mitigation of Inadvertent Disclosures of Protected Health Information	5
No Intimidating or Retaliatory Arts; No Waiver of HIPAA Privacy	5
Plan Document.....	5
Documentation and Retention.....	6
Policies on Use and Disclosure of PHI.....	7
Use and Disclosure Defined.....	7
Workforce Must Comply With County’s Policy and Procedures.....	7
Access to PHI Is Limited to Certain Employees	7
Permitted Uses and Disclosures: Payment and Health Care Operations	7
No Disclosure of PHI for Non-Health Plan Purposes.....	8
Mandatory Disclosures of PHI: to Individual and DHHS	8
Permissive Disclosures of PHI: for Legal and Public Policy Purposes	8
Disclosures of PHI Pursuant to an Authorization	9
Complying With the “Minimum Necessary” Standard	9
Disclosures of PHI to Business Associates.....	9
Disclosures of De-Identified Information.....	9
Policies on Individual Rights	11
Access to Protected Health Information and Requests for Amendment.....	11
Accounting.....	11
Requests for Alternative Communication Means or Locations.....	12
Requests for Restrictions on Uses and Disclosures of Protected Health Information	12

CMS Health Plans HIPAA Privacy Policy

Introduction

Pierce County, (“County”) sponsors one or more than one group health plan:

CMS(Claims Management Services, INC.) Health Plans

(“Plan”) for its employees or certain of its residents. Members of the County’s workforce may have access to the individually identifiable health information of Plan participants (1) on behalf of the Plan itself; or (2) on behalf of the County, for administrative functions of the Plan.

The Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (“HIPAA”) restrict the County’s ability to use and disclose protected health information (“PHI”). PHI means information that is created or received by the plan and relates to the past, present, or future physical or mental health or condition of a participant; the provision of health care to a participant; or the past, present, or future payment for the provision of health care to a participant; and that identifies the participant or for which there is a reasonable basis to believe the information can be used to identify the participant. PHI includes information of persons living or deceased.

It is the County’s policy to comply fully with HIPAA’s requirements. The County recognizes that only certain members of its workforce have access to PHI. Accordingly, only those members of the County’s workforce must comply with this Privacy Policy and all related procedures. The term “workforce,” as defined under HIPAA, includes those employees, volunteers, trainees, and other persons whose work performance is under the direct control of the County, whether or not they are paid by the County, and whose job entails the use, maintenance or disclosure of PHI.

No third party rights (including but not limited to rights of Plan participants, beneficiaries, covered dependents, or business associates) are intended to be created by this Policy. The County reserves the right to amend or change this Policy at any time (even retroactively) without notice. To the extent this Policy establishes requirements and obligations above and beyond those required by HIPAA, the Policy shall be aspirational but not be binding upon the County. This Policy does address requirements under other federal laws or under state laws.

CMS Health Plans

The Plan's Responsibilities as Covered Entity

Privacy Official and Contact Person

Insurance Coordinator will be the Privacy Official for the Plan. The Privacy Official will be responsible for the development and implementation of policies and procedures relating to privacy, including but not limited to this Privacy Policy and any implementing Procedures. The Privacy Official has also designated a contact person, Corporation Counsel for participants who have questions, concerns, or complaints about the privacy of their PHI.

Workforce Training

It is County's policy to train all members of its workforce on its privacy policies and procedures. The Privacy Official (directly or through his/her staff) is charged with developing training schedules and programs so that all workforce members receive the training necessary and appropriate to permit them to carry out their functions within Plan.

Technical, Physical and Firewall Safeguards

The County will establish, on behalf of the Plan, the appropriate technical and physical safeguards to prevent PHI from being used or disclosed in violation of HIPAA's requirements. Technical safeguards include limiting access to information by creating computer firewalls. Physical safeguards include locking doors or filing cabinets.

Firewalls will ensure that only authorized employees will have access to PHI, that they will have access to only the minimum amount of PHI necessary for plan administrative functions, and that they will not further use or disclose PHI in violation of HIPAA's privacy rules.

Privacy Notice

The Privacy Official is responsible for developing and maintaining a notice of the Plan's privacy practices that describes the uses and disclosures of PHI that may be made by the Plan, the individual's rights, and the Plan's legal duties with respect to the PHI.

The privacy notice will inform participants that the County will have access to PHI in connection with its plan administrative functions. The privacy notice will also provide a description of the County's complaint procedures, the name and telephone number of the contact person for further information, and the date of the notice.

The notice of privacy practices will be individually delivered to all participants:

- No later than April 14, 2004;
- On an ongoing basis, at the time of an individual's enrollment in the Plan; and
- Within 60 days after a material change to the notice.
- The Plan will also provide a notice of availability of the privacy notice at least once every three years.

Complaints

Corporation Counsel will be the Plan's contact person for receiving complaints. The Privacy Officer, Insurance Coordinator is responsible for creating a process for individuals to lodge complaints about the Plan's privacy procedures and for creating a system for handling such complaints. A copy of the complaint procedure shall be provided to any participant upon request.

Sanctions for Violations of Privacy Policy

Sanctions for using or disclosing PHI in violation of this HIPAA Privacy Policy will be imposed in accordance with County's discipline policy, which includes termination.

Mitigation of Inadvertent Disclosures of Protected Health Information

The County shall mitigate, to the extent possible, any harmful effects that become known to it of a use or disclosure of an individual's PHI in violation of the policies and procedures set forth in this Policy. As a result, if an employee becomes aware of a disclosure of PHI, either by an employee of the Plan or an outside consultant/contractor, that is not in compliance with this Policy, immediately contact the Privacy Official so that the appropriate steps to mitigate the harm to the participant can be taken.

No Intimidating or Retaliatory Arts; 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.

Plan Document

The Plan document shall include provisions to describe the permitted and required uses and disclosures of PHI by the County for plan administrative purposes. Specifically, the Plan document shall require the County to:

- Not use or further disclose PHI other than as permitted by the Plan documents or as required by law;
- Insure that any agents or subcontractors to whom it provides PHI received from the Plan agree to the same restrictions and conditions that apply to the County;
- 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;

- Make the County's internal practices and records relating to the use and disclosure of PHI received from the plan available to DHSS upon request; and
- If feasible, return or destroy all PHI received from the Plan that the County still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

The Plan document must also require the County to (1) certify to the Privacy Official that the Plan documents have been amended to include the above restrictions and that the County agrees to those restrictions; and (2) provide adequate firewalls.

Documentation and Retention

The Plan's and the County's privacy policies and procedures shall be documented and all policies and procedures shall be retained for at least six years from the date of issue. 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 promptly be documented. If a change in law affects the privacy notice, the privacy policy must promptly be revised and made available. Such change is effective only with respect to PHI created or received after the effective date of the notice. The Plan and the County shall document certain events and actions (including authorizations, requests for information, sanctions, and complaints) 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 until the later of six years from the date of its creation or the date when it was last in effect.

CMS Health Plans

Policies on Use and Disclosure of PHI

Use and Disclosure Defined

Pierce County ("County") and the CMS (the "Plan") will use and disclose PHI only as permitted under HIPAA. The terms "use" and "disclosure" are defined as follows:

Use. The, sharing, employment, application, utilization, examination or analysis of individually identifiable health information by any appropriately designated person working for or within the County, or by a Business Associate (defined below) of the Plan.

Disclosure. For information that is protected health information ("PHI"), disclosure means any release, transfer, provision of access to, or divulging in any other manner of individually identifiable health information to persons not employed by or working within the Benefits Department of the County.

Workforce Must Comply With County's Policy and Procedures

All members of the County's workforce (described at the beginning of this Policy) must comply with this Policy and all related procedures, which are set forth in a separate document.

Access to PHI Is Limited to Certain Employees

Only those employees and other individuals who are within the definition of "workforce" as defined above in this policy shall have access to PHI. These employees may use and disclose PHI for Plan administrative functions, and they may disclose PHI to other employees with access for Plan administrative functions (as limited to the minimum amount necessary to perform Plan administrative functions). Other employees of the County may have access to health information, but it shall only be for legitimate employment-related purposes and only if a proper authorization of the health information is in place.

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 covered entity for the payment purposes of that covered entity.

Payment. Payment includes activities undertaken to obtain Plan contributions or 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; and billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess loss insurance) 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 purposes of the other covered entity's quality assessment and improvement, case management, or health care fraud and abuse detection programs, if the other covered entity has (or had) a relationship with the participant and the PHI requested pertains to that relationship.

Health Care Operations. 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 Plan performance; underwriting and premium rating; conducting or arranging for medical review; legal services and auditing functions; business planning and development; and business management and general administrative activities.

No Disclosure of PHI for Non-Health Plan Purposes

PHI may not be used or disclosed for the payment or operations of the County’s “non-health” benefits (e.g., disability, workers’ compensation, life insurance, etc.), unless the participant has provided an authorization for such use or disclosure (as discussed in “Disclosures Pursuant to an Authorization”) or such use or disclosure is required by applicable state law and particular requirements under HIPAA are met.

Mandatory Disclosures of PHI: to Individual and DHHS

A participant’s PHI must be disclosed as required by HIPAA in two situations: the disclosure is to the individual who is the subject of the information (see the policy for “Access to Protected Information and Request for Amendment” that follows); and the disclosure is made to DHHS for purposes of enforcing of HIPAA.

Permissive Disclosures of PHI: for Legal and Public Policy Purposes

PHI may be disclosed in the following situations without a participant’s authorization when specific requirements are satisfied. The County’s disclosure procedures describe specific requirements that must be met before these types of disclosures may be made. The requirements include prior approval of the County’s Privacy Official. Permitted are disclosures:

- About victims of abuse, neglect or domestic violence;
- For judicial and administrative proceedings;
- For law enforcement purposes;
- For public health activities;
- For health oversight activities;
- About decedents;
- For cadaveric organ, eye or tissue donation purposes;
- For certain limited research purposes;
- To avert a serious threat to health or safety;
- For specialized government functions; and
- That relate to workers’ compensation programs.

Disclosures of PHI Pursuant to an Authorization

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

Complying With the “Minimum Necessary” Standard

HIPAA requires that when PHI is used or disclosed, the amount disclosed generally 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 Department of Labor
- Uses or disclosures required by law

Minimum Necessary When Disclosing PHI. For making disclosures of PHI for which the minimum necessary rule applies, the disclosure must be reviewed on an individual basis by the Privacy Official or his designated staff to ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure. Recurring disclosures may, in the Privacy Official's discretion, be disclosed based on a procedure established by the Privacy Official and thereby without review of each individual disclosure.

Minimum Necessary When Requesting PHI. For making requests for disclosure of PHI from another covered entity for purposes of plan operations, only the minimum information necessary for the purpose will be requested.

Disclosures of PHI to Business Associates

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, employees must contact the Privacy Official and verify that a business associate contract is in place.

Business Associate is an entity that performs or assists in performing a Plan function or activity involving the use and disclosure of protected health information (including claims processing or administration, data analysis, underwriting, etc.); or provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to PHI.

Disclosures of De-Identified Information

The Plan may freely use and disclose de-identified information. De-identified information is health information that cannot identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. There are two ways a covered entity can determine that information is de-identified: either by professional

statistical analysis, or by removing 18 specific identifiers (i.e., name, social security number, etc.).

CMS Health Plans

Policies on Individual Rights

Access to Protected Health Information and Requests for Amendment

HIPAA gives participants the right to access and obtain copies of their PHI that the Plan (or its Business Associates) maintains in Designated Record Sets (as defined below). HIPAA also provides that participants may request to have their PHI amended. The Plan will provide access to PHI and it will consider requests for amendment that are submitted in writing by participants.

Designated Record Set is a group of records maintained by or for the County that includes:

- The enrollment, payment, and claims adjudication record of an individual maintained by or for the Plan; or
- Other PHI used, in whole or in part, by or for the Plan to make coverage decisions about an individual.

Accounting

An individual has the right to obtain an accounting of certain disclosures of his or her own PHI. This right to an accounting extends to disclosures made in the last six years. Several disclosures are not included in this accounting, such as disclosures:

- To carry out treatment, payment or health care operations;
- To individuals about their own PHI;
- Incident to an otherwise permitted uses or disclosures;
- Pursuant to an authorization;
- For purposes of creation of a facility directory or to persons involved in the patient's care or other notification purposes;
- As part of a limited data set; and
- For other national security or law enforcement purposes.

The Plan shall respond to an accounting request within 60 days. If the Plan is unable to provide the accounting within 60 days, it may extend the period by 30 days, provided that it gives the participant notice (including the reason for the delay and the date the information will be provided) 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 (or a copy of the written request for disclosure, if any).

The first accounting in any 12-month period shall be provided free of charge. The Plan may impose reasonable production and mailing costs for subsequent accountings.

Requests for Alternative Communication Means or Locations

Participants may request to receive communications regarding their PHI by alternative means or at alternative locations. For example, participants may ask to be called only at work rather than at home. Such requests may be honored if, in the sole discretion of the County, the requests are reasonable.

However, the County shall accommodate such a request if the participant clearly provides information that the disclosure of all or part of that information could endanger the participant. The Privacy Official has responsibility for administering requests for confidential communications.

Requests for Restrictions on Uses and Disclosures of Protected Health Information

A participant may request restrictions on the use and disclosure of the participant's PHI. It is the County's policy to attempt to honor such requests if, in the sole discretion of the County, the requests are reasonable.

CMS Health Plan

Guide to HIPAA Privacy Use and Disclosure Procedures

The HIPAA Privacy Use and Disclosure Procedures that follow are for use by CMS, a self-funded group health plan with 50 or more participants. As such, the Plan is a covered entity, making the County responsible for the Plan's compliance with HIPAA's privacy requirements. The plan will be administered by employees of the County who will have access to protected health information (PHI) in connection with their duties, regardless of the use of a TPA to perform most or even virtually all administrative functions related to the group health plan.

It is assumed that the County will elect to declare itself a hybrid entity, with the establishment of a clear separation between the employees (“workforce” under HIPAA) who will have the use of and access to PHI as a part of their duties in regards to the administration of the group health plan (the covered component) and those whose job do not involve PHI; i.e., those who perform all the other tasks within the County.

This policy addresses (1) the requirements that must be satisfied by the Plan as a covered entity; and (2) the requirements that must be satisfied by the Plan and the County in order for the Plan to provide PHI to the sponsor for Plan administrative functions. Furthermore, this policy addresses privacy requirements under applicable state and other federal laws.

CMS Health Plan

HIPAA Privacy Use and Disclosure Procedures

Table of Contents

	Page
Introduction.....	15
Procedures for Use and Disclosure of PHI	16
Use and Disclosure Defined.....	16
Workforce Must Comply With County’s Policy and Procedures.....	16
Access to PHI Is Limited to Certain Employees	16
Permitted Uses and Disclosures of PHI: Payment and Health Care Operations	16
Mandatory Disclosures of PHI: to Individuals and DHHS.....	18
Permissive Disclosures of PHI: for Legal and Public Policy Purposes	19
Disclosures of PHI pursuant to an Authorization	20
Disclosure of PHI to Business Associates	21
Requests for Disclosure of PHI From Spouses, Family Members, and Friends.....	22
Disclosures of De-Identified Information	22
Verification of Identity of Those Requesting PHI.....	23
Complying With the “Minimum-Necessary” Standard	24
Retention of Documentation	25
Mitigation of Inadvertent Disclosures of PHI.....	26
Procedures for Complying With Individual Rights of Access, Amendment and Disclosure.....	27
Individual’s Request for Access	27
Individual’s Request for Amendment.....	28
Processing Requests for an Accounting of Disclosures of PHI.....	30
Processing Requests for Confidential Communications.....	31
Processing Requests for Restrictions on Uses and Disclosures of PHI	32

CMS Health Plans

HIPAA Privacy Use and Disclosure Procedures

Introduction

Pierce County ("County") sponsors a self-insured group health plan, the CMS (the "Plan"). Members of the County's workforce may have access to the individually identifiable health information of Plan participants (1) on behalf of the Plan itself; or (2) on behalf of the County, for administrative functions of the Plan.

The Health Insurance Portability and Accountability Act of 1996 and its implementing regulations ("HIPAA") restrict the County's ability to use and disclose protected health information ("PHI"). PHI means information that is created or received by the Plan and relates to the past, present, or future physical or mental health or condition of a participant; the provision of health care to a participant; or the past, present, or future payment for the provision of health care to a participant; and that identifies the participant or for which there is a reasonable basis to believe the information can be used to identify the participant. PHI includes information of persons living or deceased.

It is the County's policy to comply fully with HIPAA's requirements. To that end, all members of the County's workforce, as defined by HIPAA and the County's HIPAA Privacy Policy must comply with these HIPAA Privacy Use and Disclosure Procedures.

No third party rights (including but not limited to rights of Plan participants, beneficiaries, covered dependents, or business associates) are intended to be created by these Use and Disclosure Procedures. The County reserves the right to amend or change these Use and Disclosure Procedures at any time (and even retroactively) without notice. To the extent these Use and Disclosure Procedures establish requirements and obligations above and beyond those required by HIPAA, these Use and Disclosure Procedures shall be aspirational and shall not be binding upon the County. These Use and Disclosure Procedures does address privacy requirements under applicable state and other federal laws.

These Use and Disclosure Procedures include two Parts.

"Procedures for Use and Disclosure of PHI" includes the use and disclosure procedures that must be followed when PHI will be used or disclosed for the plan's own payment and health care operations purposes and when PHI will be disclosed to third parties.

"Procedures for Complying With Individual Rights" include procedures for complying with an individual's right to access, amendment, and accounting of disclosures of PHI held in a Designated Record Set. This section also includes procedures for addressing individual requests for confidential communications and for limits on use and disclosure.

CMS Health Plans

Procedures for Use and Disclosure of PHI

Use and Disclosure Defined

The County and the Plan will use and disclose PHI only as permitted under HIPAA. The terms “use” and “disclosure” are defined as follows:

Use. The sharing, employment, application, utilization, examination, or analysis of individually identifiable health information by any person working for or within the Benefits Department of the County, or by a Business Associate (defined below) 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 persons not employed by or working within the Benefits Department of the County.

Workforce Must Comply With County’s Policy and Procedures

All members of the County’s workforce (described at the beginning of these Use and Disclosure Procedures) must comply with these Use and Disclosure Procedures and the County’s HIPAA Privacy Policy.

Access to PHI Is Limited to Certain Employees

Only those employees and other individuals who are within the definition of “workforce” as defined above in this policy shall have access to PHI. These employees may use and disclose PHI for Plan administrative functions, and they may disclose PHI to other employees with access for Plan administrative functions (as limited to the minimum amount necessary to perform Plan administrative functions). Other employees of the County may have access to health information, but it shall only be for legitimate employment-related purposes and only if a proper authorization of the health information is in place.

Permitted Uses and Disclosures of PHI: Payment and Health Care Operations

Objective: To facilitate the use or disclosure of PHI for payment purposes and health care operations under circumstances permitted by HIPAA.

Definitions:

Payment. Payment includes activities undertaken to obtain Plan contributions or 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; and

- Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess loss insurance) and related health care data processing.

Health Care Operations. 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; and
- Business management and general administrative activities.

Procedure:

Uses and Disclosures for Plan’s Own Payment Activities or Health Care Operations. Plan workforce may use and disclose a Plan participant’s PHI to perform the Plan’s own payment activities or health care operations.

1. Disclosures must comply with the “Minimum Necessary” Standard. Under that procedure, if the disclosure is not recurring and for which a specific disclosure procedure has been created, the disclosure must be approved by the Privacy Official.
2. Disclosures must be documented in accordance with the procedure for “Documentation Requirements.”

Disclosures for Another Entity’s Payment Activities. Plan workforce may disclose a Plan participant’s PHI to another covered entity or health care provider to perform the other entity’s payment activities. Disclosures may be made under the following procedures:

1. Disclosures must comply with the “Minimum Necessary” Standard. Under that procedure, if the disclosure is not recurring and for which a specific disclosure procedure has been created, the disclosure must be approved by the Privacy Official.
2. Disclosures must be documented in accordance with the procedure for “Documentation Requirements.”

Disclosures for Certain Health Care Operations of the Receiving Entity. Plan workforce may disclose PHI for purposes of another covered entity’s quality assessment and improvement, case management, or health care fraud and abuse detection programs, if the other covered entity has (or had) a relationship with the individual and the PHI requested pertains to that relationship. Such disclosures are subject to the following:

1. The disclosure must be approved by the Privacy Official.
2. Disclosures must comply with the “Minimum-Necessary” Standard.
3. Disclosures must be documented in accordance with the procedure for “Documentation Requirements.”

Use or Disclosure for Purposes of Non-Health Benefits. Unless an authorization from the individual (as discussed in “Disclosures Pursuant to an Authorization”) has been received, no County employee may use a participant’s PHI for the payment or operations of the County’s non-healthcare benefits (e.g., disability, worker’s compensation, and life insurance). If an employee requires a participant’s PHI for the payment or health care operations of non-healthcare, follow these steps:

1. Obtain an Authorization. First, contact the Privacy Official to determine whether an authorization for this type of use or disclosure is on file. If no form is on file, request an appropriate form from the Privacy Official. Employees shall not attempt to draft authorization forms. All authorizations for use or disclosure for non-healthcare purposes must be on a form provided by (or approved by) the Privacy Official.
2. The disclosure must be approved by the Privacy Official.
3. Disclosures must comply with the “Minimum Necessary” Standard.
4. Disclosures must be documented in accordance with the procedure for “Documentation Requirements.”

Questions. If there are any questions or if any employee who is unsure as to whether a task he or she is asked to perform qualifies as a payment activity or a health care operation of the Plan should contact the Privacy Official.

Mandatory Disclosures of PHI: to Individuals and DHHS

Objective: To facilitate disclosures when required by HIPAA to individuals upon request and to DHHS for purposes of enforcing HIPAA.

Procedure:

Request From Individual. Upon receiving a request from an individual (or an individual’s representative) for disclosure of the individual’s own PHI, the employee must follow the procedure for “Disclosures to Individuals Under Right to Access Own PHI.”

Request From DHHS. Upon receiving a request from a DHHS officer for disclosure of PHI, the employee must follow the procedures for verifying the identity of a public officer set forth in “Verification of Identity of Those Requesting Protected Health Information” and disclosures be documented in accordance with the procedure for “Documentation Requirements.”

Permissive Disclosures of PHI: for Legal and Public Policy Purposes

Objective: To facilitate disclosures for legal and public policy purposes under circumstances permitted by HIPAA.

Procedure:

Disclosures for Legal or Public Policy Purposes. An employee who receives a request for disclosure of an individual's PHI that appears to fall within one of the categories described below under "Legal and Public Policy Disclosures Covered" must contact the Privacy Official. Disclosures may be made under the following procedures:

1. The disclosure must be approved by the Privacy Official.
2. Disclosures must comply with the "Minimum Necessary" Standard.
3. Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

Legal and Public Policy Disclosures Covered:

Disclosures about victims of abuse, neglect or domestic violence, if the following conditions are met:

- a. The individual agrees with the disclosure; or
- b. The disclosure is expressly authorized by statute or regulation and the disclosure prevents harm to the individual (or other victim) or the individual is incapacitated and unable to agree and information will not be used against the individual and is necessary for an imminent enforcement activity. In this case, the individual must be promptly informed of the disclosure unless this would place the individual at risk or if informing would involve a personal representative who is believed to be responsible for the abuse, neglect or violence.

For Judicial and Administrative Proceedings, in response to:

- a. An order of a court or administrative tribunal (disclosure must be limited to PHI expressly authorized by the order); or
- b. Generally speaking, although allowed by HIPAA, applicable state law bars the release of health information in response to a subpoena, discovery request or other lawful process not accompanied by a court order. If a subpoena is received for the release of health information, the Privacy Official should be notified immediately.

To a Law Enforcement Officer for Law Enforcement Purposes, under the following conditions:

- a. Pursuant to a process and as otherwise required by law, but only if the information sought is relevant and material, the request is specific and limited to amounts reasonably necessary, and it is not possible to use de-identified information.
- b. Information requested is limited information to identify or locate a suspect, fugitive, material witness or missing person.
- c. Information about a suspected victim of a crime (1) if the individual agrees to disclosure; or (2) without agreement from the individual, if the information is not to be used against the victim, if need for information is urgent, and if disclosure is in the best interest of the individual.
- d. Information about a deceased individual upon suspicion that the individual's death resulted from criminal conduct.
- e. Information that constitutes evidence of criminal conduct that occurred on the County's premises.

To Appropriate Public Health Authorities for Public Health Activities.

To a Health Oversight Agency for Health Oversight Activities, as authorized by law.

To a Coroner or Medical Examiner About Decedents, for the purpose of identifying a deceased person, determining the cause of death or other duties as authorized by law.

For Cadaveric Organ, Eye or Tissue Donation Purposes, to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of organs, eyes or tissue for the purpose of facilitating transplantation.

For Certain Limited Research Purposes, provided that a waiver of the authorization required by HIPAA has been approved by an appropriate privacy board.

To Avert a Serious Threat to Health or Safety, upon a belief in good faith that the use or disclosure is necessary to prevent a serious and imminent threat to the health or safety of a person or the public.

For Specialized Government Functions, including disclosures of an inmates' PHI to correctional institutions and disclosures of an individual's PHI to authorized federal officers for the conduct of national security activities.

For Workers' Compensation Programs, to the extent necessary to comply with laws relating to workers' compensation of other similar programs.

Disclosures of PHI pursuant to an Authorization

Objective: To facilitate disclosures of PHI as permitted by HIPAA when authorized by the individual whose PHI will be disclosed. PHI disclosed pursuant to an individual authorization

may be disclosed for any purpose so long as the disclosure is consistent with the terms of the authorization.

Procedure:

Disclosure Pursuant to Individual Authorization. Any requested disclosure to a third party (i.e., 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 these Use and Disclosure Procedures may be made pursuant to an individual authorization. If disclosure pursuant to an authorization is requested, the following procedures should be followed:

1. Follow the procedures for verifying the identity of the individual (or individual's representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."
2. Verify that the authorization form is valid. Valid authorization forms are those that:
 - a. Are properly signed and dated by the individual or the individual's representative;
 - b. Are not expired or revoked. The expiration date of the authorization form must be a specific date (such as July 1, 2003) or a specific time period (e.g., one year from the date of signature), or an event directly relevant to the individual or the purpose of the use or disclosure (e.g., for the duration of the individual's coverage);
 - c. Contain a description of the information to be used or disclosed;
 - d. Contain the name of the entity or person authorized to use or disclose the PHI;
 - e. Contain the name of the recipient of the use or disclosure;
 - f. Contain a statement regarding the individual's right to revoke the authorization and the procedures for revoking authorizations; and
 - g. Contain a statement regarding the possibility for a subsequent re-disclosure of the information. All uses and disclosures made pursuant to an authorization must be consistent with the terms and conditions of the authorization.
3. Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

Disclosure of PHI to Business Associates

Objective: To verify that disclosure of PHI to business associates is consistent with a valid business associate contract.

Definition of Business Associate: An entity or person who:

- Performs or assists in performing a Plan function or activity involving the use and disclosure of PHI (including claims processing or administration; data analysis, underwriting, etc.); or
- Provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to PHI.

Procedure:

Use and Disclosure of PHI by Business Associate. All uses and disclosures by a “business associate” must be made in accordance with a valid business associate agreement. Before providing PHI to a business associate, employees must contact the Privacy Official and verify that a business associate agreement is in place. The following additional procedures must be satisfied:

1. Disclosures must be consistent with the terms of the business associate agreement.
2. Disclosures must comply with the “Minimum Necessary” Standard.
3. Disclosures must be documented in accordance with the procedure for “Documentation Requirements.”

Requests for Disclosure of PHI From Spouses, Family Members, and Friends

Objective: To protect privacy of individual’s PHI by disclosing it only as authorized.

The Plan and County will not disclose PHI to family and friends of an individual except as required or as permitted by HIPAA. Generally, an authorization is required before another party, including a spouse, family member or friend, will be able to access PHI.

If an employee receives a request for disclosure of an individual’s PHI from a spouse, family member, or personal friend of an individual, 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 follow the procedure for “Verification of Identity of Those Requesting Protected Health Information.”

Once the identity of a parent or personal representative is verified, then follow the procedure for “Request for Individual Access.”

All other requests from spouses, family members, and friends must be authorized by the individual whose PHI is involved. See the procedures for “Disclosures Pursuant to Individual Authorization.”

Disclosures of De-Identified Information

Objective: To permit disclosure of de-identified information in accordance with HIPAA.

Definition of De-Identified Information: health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. There are two ways the Plan may determine that information is de-identified: either by professional statistical analysis, or by removing 18 specific identifiers

Procedure:

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

Verification of Identity of Those Requesting PHI

Objective: To verify the identity and authority of individual requesting access to PHI.

Employees must take steps to verify the identity of individuals who request access to PHI. They must also verify the authority of any person to have access to PHI, if the identity or authority of such 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, a parent seeking access to the PM of his or her minor child, a personal representative, or a public officer seeing access.

Request Made by Individual. When an individual requests access to his or her own PHI, the following steps should be followed:

1. Request a form of identification from the individual. Employees may rely on a valid drivers license, passport or other photo identification issued by a government agency.
2. Verify that the identification matches the identity of the individual requesting access to the PHI. If you have any doubts as to the validity or authenticity of the identification provided or the identity of the individual requesting access to the PHI, contact the Privacy Official.
3. Make a copy of the identification provided by the individual and file it with the individual's Designated Record Set.
4. If the individual requests PHI over the telephone, [insert what sort of code Plan will use to know it is the individual]. Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

Request Made by Parent Seeking PHI of Minor Child. When a parent requests access to the PHI of the parent's minor child, the following steps should be followed:

1. Seek verification of the person's relationship with the child. Such verification may take the form of confirming enrollment of the child in the parent's plan as a dependent.
2. Disclosures must be documented in accordance with the procedure "Documentation Requirements."

Request Made by Personal Representative. When a personal representative requests access to an individual's PHI the following steps should be followed:

1. Require a copy of a valid power of attorney or other documentation providing evidence of personal representative status. If there are any questions about the validity of this document, seek review by the Privacy Official.
2. Make a copy of the documentation provided and file it with the individual's Designated Record Set.
3. Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

Request Made by Public Officer. If a public officer 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," the following steps should be followed to verify the officer's identity and authority:

1. 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.
2. If the request is in writing, verify that the request is on the appropriate government letterhead.
3. 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.
4. Request a written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, 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 a judicial or administrative tribunal, contact the Privacy Official.
5. Disclosures must be documented in accordance with the procedure for "Documentation Requirements."

Complying With the "Minimum-Necessary" Standard

Objective: To limit the PHI used, disclosed or requested to the "minimum necessary" to accomplish the purpose of the use, disclosure or request unless an exception applies.

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 an individual authorization;

- Disclosures made to DHHS;
- Uses or disclosures required by law; and
- Uses or disclosures required to comply with HIPAA.

Procedures for Disclosures:

For any disclosure not listed above, notify the Privacy Official prior to disclosure. The Privacy Official will determine whether the PHI to be released complies with the minimum necessary rule. The Privacy Official may identify regularly recurring disclosures and identify the types of PHI to be disclosed, the types of person who may receive the PHI, and the conditions that would apply to such access for these regularly recurring disclosures.

Procedures for Requests:

For any request not exempted from the minimum necessary rule, notify the Privacy Official prior to disclosure. The Privacy Official will determine whether the PHI to be released complies with the minimum necessary rule. The Privacy Official may identify regularly recurring disclosures and identify the types of PHI to be disclosed, the types of person who may receive the PHI, and the conditions that would apply to such access for these regularly recurring disclosures.

Retention of Documentation

Objective: To comply with the HIPAA mandate to document uses and disclosures of PHI.

Procedure:

Documentation. The County shall maintain copies of all of the following items for a period of at least six years from the date the documents were created or were last in effect, whichever is later:

1. Notices of Privacy Practices that are issued to participants.
2. When a disclosure of PHI is made, documentation of:
 - a. The date of the disclosure;
 - b. The name of the entity or person who received the PHI and, if known, the address of such entity or person;
 - c. A brief description of the PHI disclosed;
 - d. A brief statement of the purpose of the disclosure; and
 - e. Any other documentation required under these Use and Disclosure Procedures.
3. Individual authorizations.
4. Any written communications to participants involving their individual rights under HIPAA.

5. Hybrid designation form.
6. These Policies and Procedures.
7. Business Associate Agreements.
8. Plan Certification.
9. Plan Amendments.

Mitigation of Inadvertent Disclosures of PHI

HIPAA requires that the Plan mitigate, to the extent possible, any harmful effects that become known to us of a use or disclosure of an individual's PHI in violation of the policies and procedures set forth in this manual. As a result, if you become aware of a disclosure of PHI, either by an employee of County or an outside consultant/contractor, that is not in compliance with the policies and procedures set forth in this manual, immediately contact the Privacy Official so that the appropriate steps to mitigate the harm to the individual can be taken.

CMS Health Plans

Procedures for Complying With Individual Rights of Access, Amendment and Disclosure

HIPAA gives individuals the right to access and obtain copies of their protected health information (“PHI”) that Pierce County or its Business Associates (the Plan) maintains in Designated Record Sets. HIPAA also provides that individuals may request to have their PHI amended, and that they are entitled to an accounting of certain types of disclosures.

Individual’s Request for Access

Objective: To facilitate compliance with HIPAA’s requirement to provide individuals with access to their own PHI maintained in a Designated Record Set.

“Designated Record Set” is defined as a group of records maintained by or for the County that includes:

- The enrollment, payment, and claims adjudication record of an individual maintained by or for the Plan; or
- Other protected health information used, in whole or in part, by or for the Plan to make coverage decisions about an individual.

Procedure:

Request From Individual, Parent of Minor Child, or Personal Representative. Upon receiving a request from an individual (or from a minor’s parent or an individual’s personal representative) for disclosure of an individual’s PHI, the employee must take the following steps

1. Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in “Verification of Identity of Those Requesting Protected Health Information.”
2. Review the disclosure request to determine whether the PHI requested is held in the individual’s Designated Record Set. See the Privacy Official if it appears that the requested information its not held in the individual’s Designated Record Set. No request for access may be denied without approval, from the Privacy Official.
3. Review the disclosure request to determine whether an exception to the disclosure requirement might exist; for example, disclosure may be denied for requests to access:
 - a. Psychotherapy notes;
 - b. Documents compiled for a legal proceeding;
 - c. Certain requests by inmates;

- d. Information compiled during research when the individual has agree to denial of access;
 - e. Information obtained under a promise of confidentiality; or
 - f. Other disclosures that are determined by a health care professional to be likely to cause harm.
4. See the Privacy Official if there is any question about whether one of these exceptions applies. No request for access may be denied without approval from the Privacy Official.
 5. Respond to the request for access by providing the information or denying the request within 30 days (60 days if the information is maintained off site). If the requested PHI cannot be accessed within the 30-day (or 60-day) period, the deadline may be extended for 30 days by providing written notice to the individual within the original 30- or 60-day period of the reasons for the extension and the date by which the County will respond.
 6. A Denial Notice must contain (1) the basis for the denial; (2) a statement of the individual's right to request a review of the denial, if applicable; and (3) a statement of how the individual may file a complaint concerning the denial. All notices of denial must be prepared or approved by the Privacy Official.
 7. Provide the information requested in the form or format requested by the individual, if readily producible in such form. Otherwise, provide the information in a readable hard copy or such other form as is agreed to by the individual.
 8. Individuals (except for inmates) have the right to receive a copy by mail or by e-mail or can come in and pick up a copy. Individuals (including inmates) also have the right to come in and inspect the information.
 9. If the individual has requested a summary and explanation of the requested information in lieu of, or in addition to, the full information, prepare such summary and explanation of the information requested and make it available to the individual in the form or format requested by the individual.
 10. The County may charge a reasonable fee for copying or otherwise reproducing the PHI.
 11. Disclosures must be documented in accordance with the procedure "Documentation Requirements."

Individual's Request for Amendment

Objective: To facilitate compliance with HIPAA's requirement to provide individuals with the right to request amendments to their own PHI.

Procedure:

Request From Individual, Parent of Minor Child, or Personal Representative. Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) for

amendment of an individual's PHI held in a Designated Record Set, the employee must take the following steps:

1. Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."
2. Review the disclosure request to determine whether the PHI at issue is held in the individual's Designated Record Set. See the Privacy Official if it appears that the requested information is not held in the individual's Designated Record Set. No request for amendment may be denied without approval from the Privacy Official.
3. Review the request for amendment to determine whether the information would be accessible under HIPAA's right to access (see the access procedures above). See the Privacy Official if there is any question about whether one of these exceptions applies. No request for amendment may be denied without approval from the Privacy Official.
4. Review the request for amendment to determine whether the amendment is appropriate. That is, determine whether the information in the Designated Record Set is accurate and complete without the amendment.
5. Respond to the request within 60 days by informing the individual in writing that the amendment will be made or that the request is denied. If the determination cannot be made within the 60-day period, the deadline may be extended for another 30 days by providing written notice to the individual within the original 60-day period of the reasons for the extension and the date by which the County will respond.
6. If an amendment is accepted, make the change in the Designated Record Set, and provide appropriate notice to the individual and all persons or entities listed on the individual's amendment request form, if any, and also provide notice of the amendment to any persons/entities who are known to have the particular record and who may rely on the uncorrected information to the detriment of the individual.
7. When an amendment request is denied, the following procedures apply:
 - a. All notices of denial must be prepared or approved by the Privacy Official. A Denial Notice must contain (1) the basis for the denial; (2) information about the individual's right to submit a written statement disagreeing with the denial and how to file such a statement; (3) an explanation that the individual may (if he or she does not file a statement of disagreement) request that the request for amendment and its denial be included in future disclosures of the information; and (4) a statement of how the individual may file a complaint concerning the denial.
 - b. If, following the denial, the individual files a statement of disagreement, include the individual's request for an amendment; the denial notice of the request; the individual's statement of disagreement, if any; and the County's rebuttal/response to such statement of disagreement, if any, with any subsequent disclosure of the record to which the request for amendment relates. If the individual has not

submitted a written statement of disagreement, include the individual's request for amendment and its denial with any subsequent disclosure of the protected health information only if the individual has requested such action.

Processing Requests for an Accounting of Disclosures of PHI

Objective: To facilitate compliance with HIPAA's requirement to provide individuals with the right to receive an accounting of certain disclosures of their PHI.

Procedure:

Request From Individual, Parent of Minor Child, or Personal Representative. Upon receiving a request from an individual, (or a minor's parent or an individual's personal representative) for an accounting of disclosures, the employee must take the following steps:

1. Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."
2. If the individual requesting the accounting has already received one accounting within the 12 month period immediately preceding the date of receipt of the current request, prepare a notice to the individual informing him or her that a fee for processing will be charged and providing the individual with a chance to withdraw the request.
3. Respond to the request within 60 days by providing the accounting (as described in more detail below), or informing the individual that there have been no disclosures that must be included in an accounting (see the list of exceptions to the accounting requirement below). If the accounting cannot be provided within the 60-day period, the deadline may be extended for another 30 days by providing written notice to the individual within the original 60-day period of the reasons for the extension and the date by which the County will respond.
4. The accounting must include disclosures (but not uses) of the requesting individual's PHI made by Plan and any of its business associates during the period requested by the individual up to six years prior to the request. (Note, however, that the plan is not required to account for any disclosures made prior to April 14, 2004.)The accounting does not have to include disclosures made:
 - a. To carry out treatment, payment and health care operations;
 - b. To the individual about his or her own PHI;
 - c. Incident to an otherwise permitted use or disclosure;
 - d. Pursuant to an individual authorization;
 - e. For specific national security or intelligence purposes;

- f. To Correctional institutions or law enforcement when the disclosure was permitted without an authorization; and
 - g. As part of a limited data set.
5. If any Business Associate of the Plan has the authority to disclose the individual's PHI, then the Privacy Official will obtain a listing of disclosures that must be accounted by the Business Associate.
 6. The accounting must include the following information for each reportable disclosure of the individual's PHI.
 - a. The date of disclosure;
 - b. The name (and if known, the address) of the entity or person to whom the information was disclosed;
 - c. A brief description of the PHI disclosed; and
 - d. A brief statement explaining the purpose for the disclosure. (The statement of purpose may be accomplished by providing a copy of the written request for disclosure, when applicable.)
 7. If the Plan has received a temporary suspension statement from a health oversight agency or a law enforcement officer indicating that notice to the individual of disclosures of PHI would be reasonably likely to impede the agency's activities, disclosure may not be required. If an employee receives such a statement, either orally or in writing, the employee must contact the Privacy Official for more guidance.
 8. Accountings must be documented in accordance with the procedure for "Documentation Requirements."

Processing Requests for Confidential Communications

Objective: To facilitate processing of requests for confidential communications.

Procedure:

Request From Individual, Parent of Minor Child, or Personal Representative. Upon receiving a request from an individual (or a minor's parent or an individual's personal representative) to receive communications of PHI by alternative means or at alternative locations, the employee must take the following steps:

1. Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."
2. Determine whether the request contains a statement that disclosure of all or some of the information to which the request pertains could endanger the individual.

3. The employee should take steps to honor requests that are reasonable. Requests for confidential communications must be honored by the Plan if the individual states that disclosure could endanger the individual.
4. If a request will not be accommodated, the employee must contact the individual in person, in writing, or by telephone to explain why the request cannot be accommodated.
5. All confidential communication requests that are approved must be tracked by the Privacy Official to ensure compliance.
6. Requests and their dispositions must be documented in accordance with the procedure for “Documentation Requirements.”

Processing Requests for Restrictions on Uses and Disclosures of PHI

Objective: To facilitate the processing of requests for restrictions on uses and disclosures of PHI.

Procedure:

Request From Individual, Parent of Minor Child or Personal Representative. Upon receiving a request from an individual (or a minor’s parent or an individual’s personal representative) for restrict any otherwise permitted use or disclosure of an individual’s PHI, the employee must take the following steps:

1. Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in “Verification of Identity of Those Requesting Protected Health Information.”
2. The employee should take steps to honor requests that are reasonable; that is, requests that will not unduly impede the ability of the Plan to fulfill its legal obligations.
3. If a request will not be accommodated, the employee must contact the individual in person, in writing, or by telephone to explain why the request cannot be accommodated.
4. All requests for limitations on use or disclosure of PHI that are approved must be tracked by the Privacy Official to ensure compliance.
5. All business associates that may have access to the individual’s PHI must be notified of any agreed-to restrictions by the Privacy Official.
6. Requests and their dispositions must be documented in accordance with the procedure for “Documentation Requirements.”

CMS Health Plans

Guide to Authorization for Release of Information

The Authorization for Release of Information that follows is designed to provide a mechanism for a participant in the Plan (or his/her covered dependents) to authorize the use or disclosure of protected health information (PHI) by the Plan for a specific purpose other than treatment, payment, and health care operations.

To comply with HIPAA's requirements, the Authorization Form must be filled out completely, and it must specifically and meaningfully describe the information to be disclosed and the purpose for the disclosure. The Authorization Form assumes that treatment, payment, or enrollment are not conditioned upon receipt of the Authorization Form by the Plan (a covered entity may not condition treatment, payment or enrollment upon completion of an Authorization Form, except in limited circumstances specified in the regulations).

Record keeping: The Plan, as required by HIPAA, must keep records relating to the disclosure and authorization.

CMS Health Plans Authorization For Release of Information

I hereby authorize the use or disclosure of my individually identifiable health information as described below. I understand that this authorization is voluntary and that I may revoke it at any time by submitting my revocation in writing to the entity providing the information.

Individual's name: _____

Insured's name: _____

Insured's ID No: _____

Persons/organizations authorized to provide the information: _____

Persons/organizations authorized to receive the information: _____

Specific description of information to be used or disclosed (including date(s)):

Specific purpose of the disclosure:

Will the Plan receive financial or in-kind compensation in exchange for using or disclosing the health information described above?

No: _____ Yes: _____ (describe) _____

This authorization will expire (indicate date, or an event relating to you personally or to the purpose of the authorization) _____

Important Information About Your Rights

I have read and understood the following statements about my rights:

- I may revoke this authorization at any time prior to its expiration date by notifying the providing organization in writing, but the revocation will not have any affect on any actions the entity took before it received the revocation.
- I may see and copy the information described on this form if I ask for it.
- I am not required to sign this form to receive my health care benefits (enrollment, treatment, or payment).The information that is used or disclosed pursuant to this authorization may be redisclosed by the receiving entity.
- I have the right to seek assurances from the above-named persons/organizations authorized to receive the information that they will not redisclose the information to any other party without my further authorization.

Signature of Individual or Individual’s Representative

Signature of Individual or Individual’s representative
(Form MUST be completed before signing.)

Printed name of the Individual’s personal representative

Relationship to the Individual, including authority for status as representative:

Date

YOU MAY REFUSE TO SIGN THIS AUTHORIZATION

You may not use this form to release information for treatment or payment except when the information to be released is psychotherapy notes or certain research information.

CMS Health Plans

Guide to Documents for Implementing Individual Rights

The HIPAA Privacy Documents that follow are designed for use by The CMS (the Plan) for the purposes of implementing HIPAA's individual rights to access, amendment, and accounting with respect to protected health information (PHI) held in a Designated Record Set. Forms are included for implementing the right to request confidential communications, and the right to request restrictions on the use or disclosure of PHI.

Separate forms are provided for making each of these requests, and for responding to each of these requests, as follows:

Access:

- Request for Access to PHI
- Response to Request for Access to PHI

Amendment:

- Request to Amend or Correct PHI
- Response to Request to Amend or Correct PHI

Accounting:

- Request for an Accounting of Disclosures of PHI
- Response to Request for an Account of Disclosures of PHI

Restrictions:

- Request for Restrictions on Use or Disclosure of PHI
- Response to Request for Restrictions on Use or Disclosure of PHI

Alternate Communications:

- Request for Alternate Communications
- Response to Request for Alternate Communications

HIPAA requires that documentation of a Designated Record Set be maintained for six years from the date of its creation or the date of its last use, whichever is longer.

REQUEST TO INSPECT OR COPY PHI

I hereby request to review protected health information (“PHI”) about me in a “designated record set” held by CMS (the “Plan”) in accordance with the Health Insurance Portability and Accountability Act of 1996, as amended (“HIPAA”).

A “designated record set” is a group of records maintained by or for the Plan including enrollment, payment, claims adjudication and health plan case or medical management record systems; or records used by or for the Plan to make decisions about individuals.

Check any of the below, as applicable:

- I wish to inspect PHI about me maintained in a designated record set.
- I wish to obtain a copy of PHI about me that is maintained in a designated record set.
- I request that a copy of PHI about myself be mailed to the following address:

- I request that the information be provided in the following format: _____
If I fail to request a specific format (e.g., hard copy, computer disk, CD-ROM, e-mail, etc.), the Plan will provide any format it desires. I understand that if the format requested by me is not readily producible, the Plan will provide me with a hard copy or other form or format as the Plan and I agree.

In the event the same PHI that is the subject of a request for access is maintained in more than one designated record set or at more than one location, the Plan will only produce the PHI once in response to a request.

I do ___ do not ___ agree that the Plan may provide a *summary of the health information* instead of allowing me to review the information.

I understand that the Plan has 30 days to respond to this request, and that if another person or entity holds the information or it is off site, the Plan has 60 days to respond to this request. If the Plan is unable to take action within the applicable time period, the Plan may extend the time for such action one 30 day period, provided the Plan, within the applicable time period, gives me a written statement of the reasons for the delay and the date by which the Plan will complete its action on the request.

I understand that if the Plan grants this request, in whole or in part, it will inform me of the acceptance of this request and provide the access requested. In that event, the Plan will arrange with me for a convenient time and place to inspect or copy the PHI, or it will provide me with a copy as I have requested. ***I understand that the Plan may deny this request (in whole or in part), in which case the Plan will provide me a written denial.***

I agree to pay any fees for copying, summarizing, or explaining my health information. Fees will be reasonable and will include only the cost of copying (including labor and supplies), postage (if I request that a copy or summary be mailed), and preparation of a summary (if I agree to or request a summary).

I understand that this request does not apply to all health information and that certain information may be excluded, such as (a) information that is not held in a designated record set; (b) psychotherapy notes; (c) information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding; and (d) other health information not subject to the right to access information under HIPAA

Signature

By: _____

Name: _____

Date: _____

Insured: _____

Insured's ID No. _____

If acting as a personal representative,

Name: _____

Relationship to individual _____

RESPONSE TO REQUEST TO INSPECT OR COPY PHI

Date: _____

Individual: _____

Insured: _____

CCS/tpa & Atrium (the "Plan") received your Request to Inspect or Copy PHI on date: _____

Grant of Request

- Your request has been granted in its entirety.
- Your request has been granted in part. (See the section entitled "Denial of Access" for an explanation regarding that portion of your request that has been denied.)

Access will be provided as follows:

- The Plan will provide you with access. Please contact Insurance Coordinator at 715-273-3531 Ext6430 to arrange a convenient time to copy and/or inspect your health information.
- A copy of the protected health information will be provided in the format you requested and it will be mailed to you pursuant to your prior instructions.
- The Plan cannot readily produce the form/format requested. Instead, the Plan will:
- provide access in a readable hard copy form; OR
 - contact you to agree upon an alternative form/format.
- A summary has ____ has not ____ been created based on the advance agreement provided by you.
- In accordance with your prior agreement, you must pay the Plan the following fees: 25 cents per copy. The fees may relate to any of the following, as applicable: (1) cost of copying; (2) postage; and (3) cost of preparing an explanation of health information and/or summary of health information.

Need for Extension of Time

The Plan is reviewing your request but is unable to determine if it should be granted. A delay in rendering a decision regarding the requested access is necessary for the following reason(s):

The Plan will respond to your request by [insert date, but no more than 90 days from the date of receipt of the individual's request].

Denial of Access

Your request to access your health information is denied, in whole or in part, for the following reason(s):

If your request was denied in part, the Plan will give you access to other protected health information requested, after excluding the information for which it has denied access, as set forth in the section entitled “Grant of Request.”

This denial is is not subject to appeal. You are entitled to an appeal if access was denied because:

- in the opinion of the licensed health care professional, granting access is likely to endanger the life or physical safety of your or another person;
- the protected health information makes reference to another person (unless that other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or
- the request for access was made by your personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to you or another person.

In these cases, if you appeal, your appeal will be reviewed by a licensed health care professional, designated by the Plan, who did not participate in the original decision. The appeal and notice of appeal decision will be conducted as soon as reasonably practical. Following review of the appeal, the Plan will provide or deny access in accordance with the determination of the reviewing official. Any appeal must be in writing and addressed as follows: Corporation Counsel, PO Box 367 Ellsworth, WI 54011 715-273-3531

Complaint Procedures

You may file a complaint regarding this decision with the Plan by filing it in writing with the following person: Corporation Counsel, 715-273-3531 Ext6436. Your complaint should include the reason(s) for the complaint, the grounds for disagreement with the Plan’s decision to deny your requested access and any other relevant information.

Alternatively, you may file a complaint with the Secretary of the U.S. Department of Health and Human Services. It should be addressed as follows: The Hubert H. Humphrey Building, 200 Independence Avenue, S.W., Washington, D.C. 20201. A complaint filed with the Secretary must meet the following requirements: (1) it must be filed in writing, either in paper or electronically; (2) it must name the plan that is the subject of the complaint and describe the acts or omissions believed to be in violation of the Privacy Standards; and (3) it must be filed within 180 days after receipt of this denial of access.

REQUEST TO AMEND OR CORRECT PHI

Request for Amendment

I hereby request to amend protected health information (“PHI”) about me in a “designated record set” held by CMS (the “Plan”) in accordance with the Health Insurance Portability and Accountability Act of 1996 and implementing regulations, as amended (“HIPAA”).

A “designated record set” is a group of records maintained by or for the Plan including enrollment, payment, claims adjudication and health plan case or medical management record systems; or records used by or for the Plan to make decisions about individuals.

Describe Requested Amendment:

Reason for Requested Amendment:

I understand that the Plan is not required to make the requested amendment if it determines, in good faith, that the information that is the subject of the requested amendment:

- Was not created by the Plan (e.g., the information to be amended is contained in a medical report created by my provider);
- Is not part of the designated record set;
- Would not be available for my inspection under HIPAA; or
- Is accurate and complete, as determined by the Plan.

I understand that the Plan will respond to my request within 60 days of receipt of this completed form. If the Plan is unable to take action within this time period, the Plan may extend the time for such action by 30 days, provided the Plan, within the original 60-day time period, gives me a written statement of the reasons for the delay and the date by which it will complete its action on the request.

If the Plan accepts the requested amendment, the Plan shall make the appropriate amendment to the PHI or record that is the subject of the request by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise provided a link to the location of the amendment. The Plan shall timely inform me that the amendment is accepted and obtain my identification of relevant persons with which the amendment needs to be shared as provided in HIPAA, and I understand that I must provide the Plan with identification of such relevant persons and permit the Plan to notify such persons of the amendment. The Plan shall make reasonable efforts to inform (a) persons identified by me as having received my PHI and needing amendment, and (b) persons, including business associates (as defined in HIPAA) of the Plan, that the Plan knows have the PHI that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information.

If the request is denied in whole or in part, the Plan will provide me with a written denial, which will include the basis for the denial and explain how a complaint and a statement of disagreement can be filed.

Signature

By: _____

Name: _____

Date: _____

Insured _____

Insured's ID No. _____

If acting as a personal representative,

Name: _____

Relationship to individual: _____

RESPONSE TO REQUEST TO AMEND OR CORRECT PHI

Date: _____

Individual: _____

Insured: _____

CMS (the “Plan”) received your Request to Amend or Correct PHI on Date _____.

Grant of Request

- Your request to amend or correct your protected health information (“PHI”) held in a Designated Record Set has been granted. The Plan will make an appropriate amendment to the Designated Record Set (as defined in Health Insurance Portability and Accountability Act and its implementing regulations (“HIPAA”).

- You must provide the Plan with the names of any persons to which you wish to provide the amended information. The Plan will make reasonable efforts to inform (a) persons identified by you as having received my PHI and needing amendment, and (b) persons, including business associates (as defined in HIPAA) of the Plan, that the Plan knows have the PHI that is the subject of the amendment and that may have (or could foreseeably) relied on such information.

Need for Extension of Time

- The Plan received your request. The Plan is reviewing your request but is unable to determine if the requested correction or amendment should be granted. A delay in rendering the Plan’s decision is necessary for the following reason(s):

The Plan will respond to your request by [insert date, but no more than 90 days from the date of receipt of the individual’s request]

Denial of Request

- Your request is denied for the following reason:

Statement of Disagreement

You have the right to file a written statement disagreeing with the denial of amendment. The statement of disagreement should be filed within 60 days of this notice with the Plan’s Privacy Official. The Plan has the right to prepare a rebuttal statement to your statement of disagreement. If it does so, you will receive a copy.

Recordkeeping

The Plan shall, as appropriate, identify the record or PHI in the Designated Record Set that is the subject of the disputed amendment and append or otherwise link your request for an amendment, the Plan's denial of the request, your statement of disagreement, if any, and the Plan's rebuttal, if any, to the Designated Record Set.

Future Disclosures

If a statement of disagreement has been submitted, the Plan will include the above-referenced material, or, at the Plan's election, an accurate summary of such information, with any subsequent disclosure of the PHI to which the disagreement relates. If you do not submit a written statement of disagreement, the Plan shall include your request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the PHI only if requested by you.

Complaint Procedures

You may file a complaint regarding this decision with the Plan by filing it in writing with Corporation Counsel, PO Box 367 Ellsworth, WI 54011. Your complaint should include the reason(s) for the complaint, the grounds for disagreement with the Plan's decision to deny your request to amend or correct your protected health information and any other relevant information.

Alternatively, you may file a complaint with the Secretary of the U.S. Department of Health and Human Services. It should be addressed as follows: The Hubert H. Humphrey Building, 200 Independence Avenue, S.W., Washington, D.C. 20201. A complaint filed with the Secretary must meet the following requirements: (1) it must be filed in writing, either in paper or electronically; (2) it must name the Plan and describe the acts or omissions believed to be in violation of the Privacy Standards; and (3) it must be filed within 180 days after receipt of this denial.

REQUEST FOR ACCOUNTING OF DISCLOSURES

Request for Accounting

I hereby request an accounting of disclosures of my protected health information (“PHI”) in a “designated, record set” held by CMS (the “Plan”) in accordance with the Health Insurance Portability and Accountability Act of 1996, as amended (“HIPAA”). Please provide an accounting of disclosures of PHI that occurred during the following period (please note that the maximum period is 6 years): _____

I understand that the Plan is not required to provide an accounting of disclosures of PHI made: (a) to carry out treatment, payment or health care operations; (b) to me; (c) incident to a use or disclosure otherwise permitted or required under HIPAA; (d) pursuant to an authorization; (e) to certain persons involved in my care or payment for that care; (f) to notify certain persons of my location, general condition or death; (g) for national or intelligence purposes; (h) to a correctional institution or law enforcement officials; (i) as part of a “limited data set” (as defined in HIPAA), which largely relates to research purposes; or (j) prior to the compliance date of April 14, 2003. I also understand that the Plan may not be able to provide an accounting at certain times when prohibited by a health oversight agency or law enforcement official.

I understand that the accounting will include disclosures of PHI that occurred during the six years (or such shorter time period, if applicable) prior to the date of this request, including disclosures to or by business associates of the Plan. Except as otherwise provided below, for each disclosure, the accounting will include:

- The date of the disclosure;
- The name of the entity or person who received the PHI and, if known, the address of such entity or person;
- A brief description of the PHI disclosed; and
- A brief statement of the purpose of the disclosure that reasonably informs me of the basis for the disclosure, or, in lieu of such statement, a copy of a written request for disclosure.

Signature

By: _____
Name: _____
Date: _____
Insured: _____
Insured’s ID No. _____

If acting as a personal representative,

Name: _____
Relationship to individual: _____

If during the period covered by the accounting, the Plans has made multiple disclosures of PHI to the same person or entity for a single purpose, that accounting may, with respect to such multiple disclosures, provide the above-referenced information for the first disclosure; the frequency, periodicity or number of the disclosures made during the accounting period; and the date of the last disclosure.

If during the period covered by the accounting, the Plan has made disclosures of PHI for a particular research purpose for 50 or more individuals; the accounting may, with respect to such disclosures for which my PHI may have been included, provide certain information as permitted by HIPAA. If the Plan provides an accounting for such research disclosures and if it is reasonably likely that my PHI was disclosed for such research activity, the Plan shall (upon my request) assist in contacting the entity that sponsored the research and the researcher.

I understand that the Plan has 60 days to respond to this request. If the Plan is unable to take action within the applicable time period, the Plan may extend the time for such action by 30 days, provided the Plan, within the applicable time period, gives me a written statement of the reasons for the delay and the date by which the Plan will complete its action on the request.

The first request for an accounting of disclosures in one 12 month period will be free. The Plan may impose a reasonable, cost-based fee for any subsequent accounting request., however, I may withdraw or modify my request after I am informed of any such fee by the Plan.

RESPONSE TO REQUEST FOR ACCOUNTING OF DISCLOSURES

Date: _____

Individual: _____

Insured: _____

CMS (“the “Plan”) received your Request for an Accounting of Disclosures on Date_____.

Grant of Request

- Your request for an accounting of disclosures by the Plan of your protected health information (“PHI”) has been granted. The accounting is attached.
- You will not be charged for the costs incurred by the County in complying with your request.
- This request is for a second or subsequent accounting within a 12-month period. Therefore, you must agree to pay a reasonable fee for the accounting, or you must withdraw or modify your request in order to avoid or reduce the fees. Please consider the options below and indicate your preference. Upon receipt of a completed form, indicating your choice below, the accounting will be provided. Please check one of the following three boxes:
 - I agree to pay the following fees for the accounting, which are reasonable and cost-based: [insert fee amount(s)].
 - I hereby withdraw my request for an accounting.
 - I hereby modify my request as follows: _____.

Need for Extension of Time

- The Plan is unable to provide your accounting within the 60-day period from the date of receipt or your request, as required by law. A delay in providing the accounting is necessary for the following reason(s):

The Plan will provide your accounting by [insert date, but no more than 90 days from the date of receipt of the individual’s request].

Denial of Request

- Your request for an accounting of disclosures by the Plan of your PHI has been denied. See the Plan’s Notice of Privacy Practices for more information about your rights. For a copy, contact the Plan’s Privacy Official, Insurance Coordinator, PO Box 119 Ellsworth, WI 54011 715-273-3531 Ext6430

REQUEST FOR RESTRICTIONS ON USE OR DISCLOSURE OF PHI

Request for Restriction(s)

I hereby understand that CMS (the “Plan”) may use and disclose protected health information (“PHI”) about me for purposes of health care treatment, payment and health care operations without my authorization or opportunity to agree or object. I request to restrict use and disclosure of PHI concerning treatment, payment and health care operations about me, or to restrict disclosures to family members, relatives, friends or other persons identified by me who are involved in my care or payment for that care, in accordance with the Health Insurance Portability and Accountability Act of 1996, as amended (“HIPAA”).

I request that the restrictions described below apply to the following information:

I request that the use and disclosure of the information described above be restricted in the following manner:

I request that my PHI **not** be disclosed to the following individuals or entities:

I understand that the Plan is not required to agree to this restriction. I understand that if a restriction is not specifically listed above and agreed to in writing by the Plan, it will not be effective.

I understand that if the Plan agrees to this restriction, either the Plan or I may terminate this restriction at any time. If the Plan informs me that it is terminating its agreement to a restriction, the termination of the restriction is only effective with respect to PHI created or received after the Plan informs me of the termination.

I understand that if I am in need of emergency treatment, the above requested restriction may not be effective if the restricted information is needed, in good faith, to provide emergency treatment. I further understand that if a restriction is agreed to by the Plan, it is not effective to prevent uses or disclosures required by the Secretary of the U.S. Department of Health and Human Services to investigate the Plan’s compliance with HIPAA or uses or disclosures that are otherwise required by law.

Signature

By: _____

Name: _____

Date: _____

Insured: _____

Insured’s ID No. _____

If acting as a personal representative,

Name: _____

Relationship to individual: _____

**RESPONSE TO
REQUEST FOR RESTRICTIONS ON USE OR DISCLOSURE OF PHI**

Date: _____

Individual: _____

Insured: _____

CMS (the "Plan") received your Request for Restrictions on Use or Disclosure of PHI on Date_____.

Grant of Request

- Your request to restrict the use and disclosure of protected health information has been granted in accordance with your request, subject to the following:
- Either you or the Plan may terminate this restriction at any time. If the Plan informs you that it is terminating its agreement to this restriction, the termination of the restriction is only effective with respect to PHI created or received after the Plan informs you of the termination.
 - If restricted PHI must be used or disclosed to provide emergency treatment for you, then this restriction is void and ineffective.
 - The restriction is not effective to prevent uses or disclosures required by the Secretary of the U.S. Department of Health and Human Services to investigate the Plan's compliance with the Health Insurance Portability and Accountability Act and its implementing regulations (HIPAA) or uses or disclosures that are otherwise required by law.
 - If a restriction is not specifically listed on the request, it will not be effective.

Denial of Request

- Your request to restrict use and disclosure of protected health information has been denied. See the Plan's Notice of Privacy Practices for more information about your rights. For a copy, contact the Plan's Privacy Official, Insurance Coordinator PO Box 119 Ellsworth, WI 54011.

REQUEST FOR ALTERNATE COMMUNICATIONS

Request for Alternate Communications

I hereby request that I receive communications of my protected health information (“PHI”) from CMS (the “Plan”) in accordance with the following:

The disclosure of all or part of information to which this Request for Alternate Communications pertains could endanger me. If this statement is true, please check here: .

- I request that the following communications be subject to this Request for Alternate Communications (please specify kinds of information):

- Please contact me using the following alternative means:

- Please contact me at the following alternate location:

I understand that the Plan will agree to all reasonable requests to receive communications by alternate means or at alternate locations if I clearly state that the disclosure of all or part of my PHI could endanger me. I further understand that the Plan may condition accommodation of my request on (a) when appropriate, information as to how payment, if any, will be handled; and (b) specification of an alternative address or method of contact.

Signature

By: _____

Name: _____

Date: _____

Insured: _____

Insured's ID No. _____

If acting as a personal representative,

Name: _____

Relationship to individual: _____

RESPONSE TO REQUEST FOR ALTERNATE COMMUNICATIONS

Date: _____

Individual: _____

Insured: _____

CMS (“Plan”) received your Request for Alternative Communications of protected health information on Date_____.

Grant of Request

Your request for alternate confidential communications of protected health information has been granted in accordance with your request.

Your request for alternate confidential communications of protected health information has been received; however, your request did not include the information indicated below. If you submit the following information, your request will then be granted.

Please provide:

Alternative address

Alternative method of contact:

Payment Information

Please specify how payment of benefits under the Plan should be handled:

Denial of Request

Your request for confidential communications of protected health information has been denied. See the Plan’s Notice of Privacy Practices for more information about your rights. For a copy, contact the Privacy Official, Insurance Coordinator PO Box 119 Ellsworth, WI 54011.

CMS

APPENDIX

Table of Contents

	Page
Guide to HIPAA Privacy Compliance Checklist for The Plan Sponsor.....	ii
HIPAA Privacy Compliance Checklist for Plan Sponsor.....	iii
Guide to HIPAA Privacy Compliance Checklist for Business Associates.....	xii
HIPAA Privacy Compliance Checklist for Business Associates.....	xiii
Guide to PHI Tracking Materials.....	xix
PHI Tracking Materials Internal PHI Flowchart	xx
PHI Tracking Materials Internal PHI Questionnaire	xxi
PHI Tracking Materials Health Plan Identifier Worksheet.....	xxiii
PHI Tracking Materials External PHI Flowchart	xxiv
PHI Tracking Materials Business Associate Tracking Worksheet.....	xxv

CMS Health Plans

Guide to HIPAA Privacy Compliance Checklist for The Plan Sponsor

HIPAA and its implementing privacy regulations impose rules for use and disclosure of protected health information (PHI) in various situations. All PHI used or disclosed by “covered entities” is protected under these rules, whether it is communicated in oral, written or electronic form. As a covered entity, the Plan must implement administrative safeguards and provide individual rights for participants. For purposes of these rules, “covered entities” include health plans, clearinghouses, and most health care providers. The Plan Sponsor, by force of law, and the Plan’s “business associates” (including the Plan’s TPA), by contract, will be required to comply with the requirements that apply to the Plan. Moreover, the Plan Sponsor must agree to comply with certain privacy requirements in order to receive health information from the Plan.

The HIPAA Privacy Compliance Checklist that follows is intended to be a list of actions that the Plan Sponsor should consider taking in anticipation of the HIPAA privacy requirements that must be implemented by April 14, 2003 (2004 for small employers).

Keep in mind that the Plan Sponsor and the Plan must not only comply with these HIPAA privacy requirements – they also must comply with other federal laws and any relevant state laws. Note: As necessary, the foregoing policies and procedures have taken privacy requirements under applicable state and other federal laws into account.

CMS Health Plans

HIPAA Privacy Compliance Checklist for Plan Sponsor

Task	Task Assigned to	Status/Work Performed
Obtain Education on HIPAA Privacy Requirements		
1. HIPAA EDI requirement.		
2. HIPAA privacy requirements		
Organize the HIPAA Privacy Team and Create a “Game Plan”		
1. Obtain requisite board and management approval to develop HIPAA implementation team and plan.		
2. Establish a privacy budget.		
3. Assemble the HIPAA privacy team. <ul style="list-style-type: none"> • identify all departments that should be represented (e.g., HR, benefits, accounting, information systems, legal, etc. • identify individuals from each department to be part of privacy team 		
4. Appoint a privacy officer		
5. Establish internal timeline and meeting schedule (by working back from the April 2003 (or 2004) implementation deadline).		
Assess the Way Health Information Is Currently Handled Within the County		
1. Identify health plans subject to HIPAA and individuals with access to health information. <ul style="list-style-type: none"> • Identify health plans subject to HIPAA • describe known uses for health information • list outside entities/vendors with which health information is shared • list outside entities/vendors that provide health information 		
2. Identify non-health plans and programs with access to health information <ul style="list-style-type: none"> • identify non-health plans/programs subject to HIPAA • identify internal personnel with access to health information 		

Task	Task Assigned to	Status/Work Performed
<ul style="list-style-type: none"> • describe known uses for health information • list outside entities/vendors with which health information is shared • list outside entities/vendors that provide health information 		
<ul style="list-style-type: none"> • identify non-health plans/programs subject to HIPAA • identify internal personnel with access to health information • describe known uses for health information • list outside entities/vendors with which health information is shared • list outside entities/vendors that provide health information 		
<p>3. Identify additional individuals with access to health information e-mail/intranet survey.</p>		
<p>4. Identify specific health information exchanges engaged in by personnel identified in Steps 1-3.</p> <ul style="list-style-type: none"> • identify specific health information exchanges • identify purpose for which health information is currently used • identify source of health information • identify outside entities with which health information is shared (and purpose) • identify additional personnel within the County with whom health information is shared • determine whether release/authorization is currently used • determine security measures/safeguards currently in place 		
<p>Evaluate the County’s Need for Protected Health Information and Desired Approach (“Hands-Off” or “Involved”)</p>		
<p>In complying with the HIPAA privacy rules, the regulations allow plan sponsors to choose between the “Hands-Off PHI” Approach and the “Involved Sponsor” Approach.</p> <ul style="list-style-type: none"> • “Hands-Off PHI” Approach: Group health plans that provide health benefits only through an insurance contract (fully-insured plans), and that do not create, maintain, or receive PM, can largely avoid the burdensome privacy requirements 		

Task	Task Assigned to	Status/Work Performed
<ul style="list-style-type: none"> • “Involved Sponsor” Approach: Group health plans that either are self-funded or that create, maintain; or receive PHI generally are subject to the full panoply of privacy requirements. <p>Based on information obtained from the inquiries outlined above, the County must decide, in regard to each of its plans, whether it will adopt the “Involved Sponsor” Approach or the “Hands-Off” PHI Approach. In choosing between the “Hands-Off” PHI Approach and the “Involved Sponsor” Approach, the County must evaluate the benefits it offers, as well as its current level of involvement in administering such benefits.</p>		
<ol style="list-style-type: none"> 1. List the various benefits offered (i.e., medical, dental, health FSA, EAP, vision, etc.) 		
<ol style="list-style-type: none"> 2. Identify whether each of the benefits is fully insured or self-funded. 		
<ol style="list-style-type: none"> 3. Identify the type of PHI that is involved with each benefit. 		
<ol style="list-style-type: none"> 4. Identify the purposes for which the PHI is currently being used within the County. These purposes should then be divided into three categories: <ul style="list-style-type: none"> • uses permitted by the privacy rules • non-permitted uses that are deemed vital, and for which an employee authorization should thus be obtained • non-permitted uses that are not vital and should thus be discontinued 		
<ol style="list-style-type: none"> 5. Evaluate whether other uses are necessary. <ul style="list-style-type: none"> • determine whether such uses are permissible under the privacy rules • if not, evaluate whether the uses are vital enough to seek an employee authorization so that the uses are permitted under the rules 		
<ol style="list-style-type: none"> 6. Determine whether any safeguards are already in place to protect the PHI. <ul style="list-style-type: none"> • compare these safeguards to those that are required by HIPAA (discussed below) determine what changes will need to be made 		

Task	Task Assigned to	Status/Work Performed
<p>7. For fully-insured benefits, determine the extent to which the County desires to have PHI access that extends beyond the following three scenarios:</p> <ul style="list-style-type: none"> • advocating on behalf of group health plan participants in benefit disputes or appeals, and providing employees with assistance in understanding their health plan benefits (but <i>not</i> obtaining any PHI from a group health plan or a covered provider without obtaining the individual’s authorization) • obtaining from the group health plan or its health insurance issuer (upon request) “summary information” for the limited purpose of (a) obtaining premium bids for providing health insurance coverage under the group health plan; or (b) modifying, amending or terminating the group health plan. • obtaining information relating to enrollment and disenrollment under the group health plan 		
<p><i>Self-funded plans:</i> Plans that are self-funded generally are covered entities, regardless of contracting with a TPA to administer the health plan. Therefore, self-funded plans are <i>not</i> eligible for the “Hands-Off PHI” Approach and should thus prepare to comply with the privacy rules (as outlined under the “Involved Sponsor” Approach below).</p>		
<p><i>Fully-insured plans:</i> For fully-insured plans, the County can choose between the “Involved Sponsor” Approach (discussed below) and the “Hands-Off PHI Approach, depending on whether it is willing to relinquish access to PHI and on whether it is willing to take on HIPAA administrative requirements.</p>		
<p>Involved Sponsor Approach.</p>		
<p>Health plans are subject to the following HIPAA administrative requirements.</p>		
<p>1. Administrative requirements</p> <ul style="list-style-type: none"> • appoint a privacy officer • establish a complaint office • train employees regarding the privacy rule • establish safeguards to protect PHI 		

Task	Task Assigned to	Status/Work Performed
<p>2. Prepare and distribute a summary of individuals' rights</p> <ul style="list-style-type: none"> • right to notice of uses and disclosures of PHI, and rights and the County's responsibilities with respect to those rights; • right to inspect and obtain a copy of PHI; • right to request amendments of their PHI; and • right to receive an accounting of disclosures of PHI made within past six years 		
<p>3. Design and implement internal procedures for complying with the privacy requirements.</p> <ul style="list-style-type: none"> • provide notice of uses and disclosures of PHI; • inspect and obtain a copy of PHI; • consider amending PHI records upon request; and • provide an accounting of disclosures of PHI made within past six years 		
<p>It is important to remember that even after complying with these administrative requirements, the County can use PHI only <i>for limited</i> purposes. Namely, for "plan administration functions" that are performed on behalf of the group health plan and that are specified in the plan document.</p>		
<p>Amend the Plan Document</p>		
<p>In order for a plan to disclose PHI to County benefits personnel, the plan document must be amended to:</p> <ul style="list-style-type: none"> • describe the permitted and required uses and disclosures of PHI by the County; • specify that disclosure is permitted only upon receipt of written certification that the plan documents have been amended; and • provide adequate firewall. <p>Each of these is discussed in more detail below.</p>		
<p>1. Describe the permitted and required uses and disclosures. The plan document must be amended to establish the permitted and required uses and disclosures of PHI. This must be addressed in the plan's privacy notice.</p>		

Task	Task Assigned to	Status/Work Performed
<p>2. Written certification that plan documents have been amended. The plan document must be amended to provide that the plan may disclose PHI to the County only if the County certifies that the plan documents have been amended to incorporate the following provisions and that the County agrees to:</p> <ul style="list-style-type: none"> • not use or further disclose PHI other than as permitted by the plan documents or as required by law; • ensure that any agents or subcontractors to whom it provides PHI received from the health plan agree to the same restrictions and conditions that apply to the County; • not use or disclose PHI for employment-related actions or in connection with any other employee benefit plan; • report to the health plan 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; • make its internal practices and records relating to the use and disclosure of PHI received from the health plan available to DHHS upon request; and • if feasible, return or destroy all PHI received from the health plan that the County maintains in any form and retain no copies of such information when no longer needed for the <i>purpose for which disclosure</i> was made; except that if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible. 		
<p>3. Erect firewalls. In order to ensure that “adequate separation” exists between the group health plan and the County, the plan must be amended to:</p> <ul style="list-style-type: none"> • describe the employees (or class of employees) who may be given access to PHI; • restrict access to and use by such employees to plan administration functions that the County performs for the health plan; and • provide a procedure for resolving any issues of non-compliance 		

Task	Task Assigned to	Status/Work Performed
Erect Firewalls		
Covered entities are required to erect “firewalls” to prevent PHI from being used impermissibly.		
1. Evaluate the roles of all employees to determine which employees are involved in the administration of its benefit plans.		
2. Implement a procedure to ensure that only these designated employees have access to PHI, and even then, that they have access only to the PHI necessary to perform their duties for the plan.		
3. Implement a mechanism for ensuring that these employees do not use or disclose PHI in a way prohibited by the privacy regulations. <ul style="list-style-type: none"> • provide educational training for employees concerning the HIPAA privacy rules, the statutory penalties associated with violations of the rules, and the County’s internal policies for dealing with such violations. 		
Address Relationships With Outside Third Parties (Vendors, TPAs, etc.)		
The privacy regulations require that certain restrictions be placed on health information that flows from the County to third parties known as “business associates”.		
1. Identify which third parties constitute “business associates”. HIPAA provides that a “business associate” is a person who, on behalf of a covered entity; i.e., health care providers, health plans, and health care clearinghouses: <ul style="list-style-type: none"> • performs or assists in perforating a function or activity involving the use or disclosure of individually identifiable health information or involving any other function or activity regulated by HIPAA’s administrative simplification rules; or • provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves providing such service provider with individually identifiable health information. 		

Task	Task Assigned to	Status/Work Performed
<p>2. Ensure that each plan service provider contract:</p> <ul style="list-style-type: none"> • describes the permitted and required uses and disclosures by the business associate, which may not exceed that which is allowed for the plan; • prohibits the business associate from disclosing the information further; • requires the business associate to implement safeguards to prevent the improper use or disclosure of information; • requires the business associate to report to the plan any improper use or disclosure of PHI; • imposes the same requirements on all of the business associate's subcontractors; • requires the business associate to make available PHI in compliance with individuals' rights to access, amend, and receive an accounting related to such PHI; • requires the business associate to make its internal books and records available to DHHS for purposes of determining the covered entity's compliance with HIPAA • requires the business associate to return or destroy PHI, if feasible, upon termination of the relationship; and • authorizes the plan to terminate the contract if the business associate has violated a material term of the contract. 		
<p>3. Ensure that the business associate contract includes a remedy for the plan in the event that the business associate breaches the contract.</p> <ul style="list-style-type: none"> • such remedies should include a unilateral right to terminate the contract upon a material breach of HIPAA obligations, as well as indemnity to the plan (and the County) for any damages that the plan (or the County) may incur by reason of the business associate's breach 		
<p>4. Ensure that all business associates properly sign the contract and educate the business associates regarding their responsibilities and obligations under the contract.</p>		

Task	Task Assigned to	Status/Work Performed
<p>5. Implement a program to address the plan’s obligations in the event a business associate breaches the contract.</p> <ul style="list-style-type: none"> • if the plan obtains knowledge of a pattern or practice by a business associate that violates the business associate contract, the plan is required to take reasonable steps to cure the breach or end the violation • if the reasonable steps are unsuccessful, the plan must terminate the business associate contract, or, if not feasible to terminate, report the business associate to DHHS • the plan cannot avoid responsibility by intentionally ignoring problems! 		
Evaluate Potential Impact of Privacy Regulations on Non-Health-Plan Operations		
<p>Although the HIPAA privacy regulations are targeted at <i>health</i> plans, they will have some impact on non-health-plan operations (workers’ compensation, disability, work return, etc.) that rely on access to individual health information. It is therefore important that the County consider how its non-health-plan operations may be affected by the privacy rules. Some areas to consider are set forth below. The County should evaluate all of its non-health-plan operations to see if there are additional areas.</p>		
Formalize Privacy Policy to Reflect Approach Taken and Specific Organizational Requirements		
<p>1. <i>Drug testing policies.</i> Medical providers generally will not perform drug tests without authorization by the employee. The regulations do not prohibit a plan from requiring an employee to provide such authorization as a prerequisite to his or her employment (but other federal laws, such as ADA, should be reviewed).</p>		
<p>2. <i>Disability, FMLA, life insurance underwriting and administration.</i> An employee’s authorization generally is required before the County can use PHI for non-health-plan purposes such as disability, FMLA, life insurance, underwriting, etc.</p>		
<p>3. Other Current Uses of PHI?</p>		

CCS/tpa & Atrium Health Plans

Guide to HIPAA Privacy Compliance Checklist for Business Associates

HIPAA and its implementing privacy regulations impose rules for use and disclosure of protected health information (PHI) in various situations. All PHI used or disclosed by the Plan is protected under these rules, whether it is created, maintained or communicated in oral, written or electronic form. The Plan must also implement certain administrative safeguards and provide certain individual rights for participants. Covered entities include health plans, clearinghouses, and most health care providers. Employers will be responsible for HIPAA privacy obligations if they provide a self-insured health plan, even if it is fully administered by a third party administrator (TPA). The plan itself will constitute either a covered entity or a hybrid entity (part covered entity to which HIPAA applies and part non-covered entity). TPAs will not normally be covered entities, but will be a business associate of the self-insured plan. TPAs and other service providers that assist covered entities in connection with their covered health care functions (known as “business associates”) will be required by contract to comply with many (but not all) of the requirements that apply to a covered entity through a business associate agreement. Employers who purchase health insurance plans for their employees are plan sponsors under HIPAA and have few HIPAA-related responsibilities. For the most part, all they must do is amend their plan documents to comply with certain privacy requirements in order to receive health information from their health plans

The HIPAA Privacy Compliance Checklist that follows is intended to be a list of actions that business associates (and other service providers) may wish to take in anticipation of the HIPAA privacy requirements that must be implemented by April 14, 2003 (2004 for small employers).

Keep in mind that business associates must not only comply with these HIPAA privacy requirements – also must comply with other federal laws and any relevant state laws.

This checklist is intended to help the Plan Sponsor set its expectations as to the responsibilities of the Plan’s business associates.

CCS/tpa & Atrium Health Plans

HIPAA Privacy Compliance Checklist for Business Associates

Task	Task Assigned to	Status/Work Performed
Organize HIPAA Compliance Team and Create a “Game Plan”		
Create a HIPAA compliance committee with representatives from corporate compliance, each field office, legal, operations, systems and security		
1. Designate a leader for the HIPAA privacy and security compliance project.		
2. Establish a budget and a timeline for compliance.		
3. Assign accountability and deadlines for the tasks listed below.		
Assess the Way Health Information Is Currently Being Handled Within the Organization		
Identify the services in which business units might come into contact with PHI and therefore be subject to the HIPAA privacy requirements.		
1. Gather data about the health information that flows into, through and out of the various business units in connection with providing the services listed above. Consider all formats (i.e., oral, paper and electronic) and all channels including in-person, telephone, postal mail, e-mail, intranet and Internet.		
2. For each service subject to HIPAA, identify: <ul style="list-style-type: none"> • The health information that the business unit creates, receives or stores; • The individuals with access to the health information (both internal and external); • The systems in which the health information is entered or processed. 		
3. With regard to each service, evaluate the organization’s status as business associate or covered entity. Closely evaluate carrier interface and information management functions to determine whether health care clearinghouse status is assumed (e.g., due to converting data from/to HIPAA compliant EDI format) <ul style="list-style-type: none"> • Before undertaking covered entity status, evaluate business aspects of assuming “covered entity” status 		

Task	Task Assigned to	Status/Work Performed
<ul style="list-style-type: none"> Evaluate hybrid entity implications if part(s) of operations attain covered entity status 		
<p>4. Based on the information gathered:</p> <ul style="list-style-type: none"> Compare the use and disclosures permitted by HIPAA (i.e., on behalf of a covered entity’s payment, treatment, and health care operations and other permissible uses and disclosures). If non-permissible uses (e.g., marketing functions) are found, determine how the client wishes to address the issue. Options include obtaining an authorization or consent from the individual, using de-identified information, and eliminating the function. Determine the extent to which the use and disclosure of health information satisfies the “minimum necessary” requirements set forth in 45 CFR § 164_502(b) and 164.514(d). 		
<p>5. Gather and review critical documents including:</p> <ul style="list-style-type: none"> Plan services organizational chart Employee manual Departmental privacy policies and procedures (if existing) Training plan and schedule for plan services personnel Security manual, policies and procedures (if existing) 		
<p>6. Document the assessment process, including the information gathered, the materials reviewed, the individuals interviewed and the decisions made.</p>		
Revise Client Contracts to Comply With Business Associate Requirements .		
<p>Identify each instance in which a business unit acts as a “business associate” of a covered entity, and for each of them ensure that the contract complies with HIPAA.</p>		
<p>1. A business unit may be a business associate of a covered entity when it:</p> <ul style="list-style-type: none"> Performs services for or on behalf of a covered entity involving the use and disclosure of individually identifiable health information; or Provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services for a covered entity, where the performance of services involves individually identifiable health information. 		

Task	Task Assigned to	Status/Work Performed
<p>2. The following services are likely areas in which PHI is handled – thus giving rise to business associate status:</p> <ul style="list-style-type: none"> • Insurance brokerage/agent operations • FSA claims processing and adjudication • COBRA notice and billing services • HIPAA certificate service operations • Carrier interface operations • Information management 		
<p>3. Collect and review all existing contracts with covered entities and create uniform services template for each covered service.</p>		
<p>4. With regard to each business associate relationship, determine whether the organization will use its own uniform services template or will be required to use clients template</p> <ul style="list-style-type: none"> • If using in-house template, establish process for sending out required agreements, tracking status, responding to client inquiries and handling exception requests; • If using clients’ template, establish process for document/relationship tracking and internal legal/compliance review and approval to eliminate over-reaching provisions. 		
Policies and Procedures		
<p>Implement policies and procedures to ensure business associate’s compliance with the HIPAA requirements that will be imposed on it by contract.</p>		
<p>1. HIPAA requires a business associate contract to</p> <ul style="list-style-type: none"> • limit the business associate’s uses and disclosures to uses and disclosures that would be allowed for the plan; • prohibit the business associate from disclosing the information further • require the business associate to implement safeguards to prevent the improper use and disclosure of information; • require the business associate to report to the plan any improper use or disclosure of PHI • impose the same requirements on all of the business associate’s subcontractors; • require the business associate to make available PHI in compliance with individuals’ rights to access, amend, and receive an accounting related to such PHI; 		

Task	Task Assigned to	Status/Work Performed
<ul style="list-style-type: none"> • require the business associate to make its internal books and records available to DHHS for purposes of determining the covered entity’s compliance with HIPAA • require the business associate to return or destroy PIE, if feasible, upon termination of the relationship; and • authorize the plan to terminate the contract if the business associate has violated a material term of the contract 		
<p>2. If the plan sponsor seeks access to PHI, the business associate must obtain a certification that the plan document has been amended to:</p> <ul style="list-style-type: none"> • describe the permitted and required uses and disclosures of rill by the County; and • provide adequate firewalls, <p>Procedures should be in place to track certifications and limit sponsor access when certifications have not been received.</p>		
<p>3. Evaluate what outside entities (vendors, sub-contractors, agents, etc.) have access to PHI and ensure HIPAA-compliance services agreement (with business associate-like provisions) has been entered into.</p>		
<p>4. Prepare a notice of privacy practices that complies with 45 CFR § 164.520 (only needed when contractually obligated to provide notice on behalf of clients). Develop procedures (consistent with contractual obligations) to:</p> <ul style="list-style-type: none"> • Deliver notice • Revise the notice in the event of a material change and deliver the revised notice. 		
<p>5. Draft HIPAA-compliant procedures to satisfy contractual requirement to provide individuals with access, amendment, and accounting rights. Procedures should address:</p> <ul style="list-style-type: none"> • Responding to, and implementing as appropriate, an individual’s request for protection of PHI pursuant to 45 CFR § 164.522. • Providing individuals with access to PHI as required by 45 CFR § 164-524. • Providing individuals with the ability to amend PW as required by 45 CFR § 164.526. • Providing individuals with an accounting of disclosures of PHI in accordance with 45 CFR § 164.528. 		

Task	Task Assigned to	Status/Work Performed
6. Identify the databases in which health information is stored and the application programs in which health information is processed.		
Training and Firewalls		
Employee training and firewalls address the “adequate safeguards” requirement that will be included in HIPAA-compliant business associate contracts.		
1. Evaluate the roles of all employees to determine which employees have access to client PHI.		
2. Implement a procedure to ensure that only these designated employees have access to PHI, and even then, that they have access only to the PHI necessary to perform their duties for the client:		
3. Implement a mechanism for ensuring that employees do not use or disclose PHI in a way prohibited by the privacy regulations or the client contract.		
4. Provide educational training for employees concerning the HIPAA privacy rules, the statutory penalties associated with a violation of the rules, and the County’s internal policies for dealing with such violations.		
5. Establish procedure for reporting violations.		
Evaluate Role vis-a-vis Client Plan Compliance Obligations		
Evaluate the extent to which each business associate will take a training role with its clients.		
1. Prepare client-oriented “white paper” addressing HIPAA aspects of services provided and compliance status/initiative.		
2. Educational role for clients <ul style="list-style-type: none"> • Client education seminar(s) 		
3. Develop/distribute compliance-oriented materials to assist plan(s) with their compliance. <ul style="list-style-type: none"> • Informational piece/white paper • Sample plan language • Sample privacy notice • Sample policy/procedures • Sample implementation plan 		

Task	Task Assigned to	Status/Work Performed
Evaluate State Law Requirements		
<p>State laws applicable to a business associate’s handling of health information generally will not be preempted by ERISA. As a result, an analysis of applicable state law requirements must be undertaken. The analysis should include a careful evaluation of the following:</p> <ul style="list-style-type: none"> • What state laws must be complied with (its what states is business conducted)? • What are the sources of applicable state law affecting health information (e.g., insurance code, privacy laws, health care laws)? • What types of health information are regulated? • Are any applicable state laws preempted by HIPAA or ERISA? 		

CCS/tpa & Atrium Health Plans

Guide to PHI Tracking Materials

The PHI Tracking Materials that follow are designed to assist the Plan Sponsor with tracking PHI. Members of the Plan Sponsor's workforce perform plan administrative functions and have access to protected health information ("PHI") in connection with their duties. The Plan uses third parties for certain plan functions. When those third parties have access to PHI, generally they are business associates

First Identify the Health Plans: As a preliminary matter, the Plan Sponsor will need to identify and list each health plan subject to HIPAA. Possibilities include medical (including insured, self-funded and HMO options), dental, vision, health FSA, EAP/counseling, supplemental health, and executive medical.

The sample PHI Tracking Materials that follow are intended to be used as tools need to assess which employees and which third parties have access to PHI. The tools are organized to achieve the three objectives described below. Following is a description of each step, including its objective and the PHI tracking materials that apply.

Objective 1: Determine What Areas of the County Have Access to PHI.

See "*Internal PHI Flowchart*," which demonstrates areas that typically must be addressed by the Plan Sponsor. Dashed lined boxes represent areas where further inquiry may rule an area in or out.

Objective 2: Determine Which Members of the County's Workforce Have Access to PHI.

See "*Internal PHI Questionnaire*." Note that individuals with access to health information from the Plan Sponsor may not be subject to HIPAA if they are receiving the information as part of an HR function and they are not receiving the information from or on behalf of the plan or in connection with plan administration. Ask individuals who are identified as having access to PHI to fill out a "*Health Plan Identifier Worksheet*."

Objective 3: Determine Which Third Parties Have Access to PHI and Record Status.

See "*External PHI Flowchart*." For third parties identified as Business Associates, complete "*Business Associate Tracking Worksheet*" to record status of business associate contract, permitted uses of PHI, and other information.

CCS/tpa & Atrium Health Plans

PHI Tracking Materials Internal PHI Flowchart

Objective 1: Determine What Areas of the Plan Sponsor Have Access to PHI.

This flowchart demonstrates areas that typically must be addressed by the Plan Sponsor. Dashed lined boxes represent areas where further inquiry may rule an area in or out.

CCS/tpa & Atrium Health Plans

PHI Tracking Materials Internal PHI Questionnaire

Objective 2: Determine Which Members of the Plan Sponsor’s “Workforce” have access to PHI.

Deliver this questionnaire (along with the “*Health Plan Identifier Worksheet*”) to each person in departments identified in the “*Internal PHI Flowchart*” as possibly having access to PHI. Don’t limit scope to common-law employees. All workers with potential access to PHI, even independent contractors, must complete the questionnaire. Follow up with any workers that do not return the questionnaire by the deadline.

INTEROFFICE MEMORANDUM

TO: [Identified Person]
FROM: HIPAA Compliance Team]
SUBJECT: Short Survey Regarding Access to Health Information

DATE: [Date]

CCS/tpa & Atrium is undertaking steps to ensure that its health benefit plan administration complies with the federal health information privacy requirements imposed by the Health Insurance Portability and Accountability Act (HIPAA). You have been identified as an individual who may have access to individual health information. In order to ensure our compliance, we ask that you read this memo and answer the questions below. For purposes of this survey, health plan coverage is defined in its broadest sense and includes all health coverage offered by Pierce County (e.g., medical, dental, EAP, long term care, vision, retiree medical, and health FSA). Health plan coverage does not include workers compensation, disability, or life insurance coverage.

If you answer “yes” to all three questions below, please complete the attached “*Health Information Identifier Worksheet*” and list all internal personnel and outside entities with which you share health information. As you identify such individuals, please contact Corporation Counsel so that we can ensure that the recipients have been sent a similar survey. Please note that your signed memo (with the completed Health Information Identifier Sheet if applicable) must be returned to Corporation Counsel prior to 30 days.

Please Answer the Following Three Questions:

(1) Do you have access to health information?

For this purpose, “health information” includes:

- (a) Health plan coverage or eligibility information (e.g. coverage category or option) received from a Pierce County Health plan or a plan service provider. Plan service providers include third party administrators such as CCS/tpa & Atrium. Health information does not include information on the [HR database];
 - (b) Health plan claims information;
 - (c) Health plan claims appeal information.
- (2) Does the information identify individuals, or can individual identities be determined from the information?
- (3) Was the health information obtained from a Pierce County Health Plan and not solely from: (a) HR functions (FMLA administration, ADA administration, and other HR functions); or (b) non-covered benefit plans (disability, life, workers compensation)?

Examples: Health information obtained from a Pierce County health plan may include: (i) information received from one of the plan’s health plan administrators such as CCS/tpa & Atrium; and (ii) information received from Pierce County benefits personnel that includes health information.

___ I answered “yes” to questions 1, 2 and 3 above and have attached a “*Health Information Identifier Worksheet.*”

___ I do not have access to health information, but have identified the following people in my department who should be surveyed.

___ Neither I nor others in my department have access to health information.

Name/Department

Date

CCS/tpa & Atrium Health Plans

PHI Tracking Materials Health Plan Identifier Worksheet

Objective: Determine Which Members of the Plan Sponsor’s “Workforce” Have Access to PHI.

Deliver the “*Health Plan Identifier Questionnaire*” and this worksheet to each person in departments identified in the “*Internal PHI Flowchart*” as possibly having access to PHI. Don’t limit questions to common-law employees. All workers with potential access to PHI, even independent contractors, must complete the questionnaire and this worksheet. Follow up with any workers that do not return the questionnaire by the deadline.

Instructions: If you answered “yes” to all three questions on the “*Health Information Questionnaire*,” please complete this sheet. List all internal personnel and outside entities with which you share health information. As you identify such individuals, please contact Corporation Counsel so that we can ensure that the recipients of the information have been sent a similar survey. Please note that your signed memo (with the completed *Health Information Questionnaire*) must be returned to Corporation Counsel prior to 30 days.

Name of Plan

Identify the health information received or created by the plan ¹	List of internal personnel with access to health information	Describe known uses for health information	List outside entities/ vendors with which health information is shared.	List outside entities/ vendors that provide health information.

¹ Health information includes any and all information, whether oral or communicated in any medium, that relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care.

CCS/tpa & Atrium Health Plans

PHI Tracking Materials External PHI Flowchart

Objective: Determine which third parties have access to PHI and record their status.

This flowchart demonstrates areas that typically must be addressed by the Plan Sponsor. Parties identified here that have access to PHI will generally be business associates. For third parties identified as business associates, complete the “*Business Associate Tracking Worksheet*” to record status of the business associate contract, permitted uses of PHI, and other information.

PHI Tracking Materials

Business Associate Tracking Worksheet

Objective: Determine which third parties have access to PHI and record their status.

The “*External PHI Flowchart*” demonstrates areas that typically must be addressed by the Plan Sponsor. For third parties identified as business associates, complete this tracking sheet to record the status of the business associate contract, permitted uses of PHI, and other information.

Outside Vendor	Current Contract Written Expiration		Current Uses of PHI	Uses Requiring Authorization	PHI Received from	PHI Provided to	Retention of PHI in designated record set
	Y/N	Date					
1.							