



PRIVACY IMPACT ASSESSMENT (PIA)

For the

DOD NAF Health Benefits System

ACSIM / Installation Management Command

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

- (1) Yes, from members of the general public.
- (2) Yes, from Federal personnel* and/or Federal contractors.
- (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.
- (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- New DoD Information System
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- Yes, DITPR Enter DITPR System Identification Number
- Yes, SIPRNET Enter SIPRNET Identification Number
- No

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- Yes
- No

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- Yes
- No

If "Yes," enter Privacy Act SORN Identifier

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: <http://www.defenselink.mil/privacy/notices/>

or

Date of submission for approval to Defense Privacy Office

Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

Yes

Enter OMB Control Number

Enter Expiration Date

No

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

Section 349 of Public Law number 103-337, formerly the National Defense Authorization Act for Fiscal Year 1995.

Sections 102a and 262 of Public Law number 104-191, the Health Insurance Portability and Accountability Act of 1996.

Use of Social Security Numbers to match plan members is required (effective January 1, 2009) by Section 111, P.L. 110-173 Medicare, Medicaid and SCHIP Extension Act (MMSEA) of 2007.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

The DoDNHB system is actually a service provided by Aetna (commercial entity) and is used to provide administrative services for current and retired DoD NAF employees who participate in the DoD NAF Health Benefits Program. Eligibility information is sent to Aetna by the six DoD NAF employers (USA, USN, USAF, USMC, AAFES and NEXCOM). Aetna uses this information to compile health care records, pay covered costs and manage premium charges/payments from the DoD NAF employers.

This system, owned and operated by the Aetna Insurance Company, is used by Aetna to administer health benefits for DOD Non appropriated Fund (NAF) employees. The system is also used by Aetna to store and process health benefits information for non-DOD organizations and individuals. Although the DOD NAF Health Benefits program is administered by the DOD NAF Personnel Policy Office, the Army serves as executive agent, and the contract for this service is administered by the NAF Contracting activity of the U.S. Army Family and MWR Command. The DOD NAF Personnel Policy Office, through the Army NAF contract, pays only for the Third Party Administrator services provided by Aetna and not for any system development or sustainment costs. The DOD NAF Personnel Policy Office nor the individual NAF employers have rights to access the system.

PII includes personal and medical.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

Unauthorized release of the PII and/or health information could result in identity theft, discrimination based on medical condition, or other criminal misuse.

DODNHB is hosted at the Aetna corporate datacenter. Access to DoD employee data is limited to authorized users with a need-to-know and incorporates a "least privilege" policy for file permissions. The contract between Aetna and DoD requires a high level of information protection to include data-at-rest encryption.

Regular

reports on the status of information security measures are required, as is immediate notification of possible failures. Data records are maintained in datacenter facilities that are secured 24 hours per day with restricted access.

Data access is restricted to the DoD NAF employers, individuals with a business "need-to-know" and authorized technical administrators

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

Within the DoD Component.

Specify. All Army Components United States Army

Other DoD Components.

Specify. Navy Exchange, Army, Air Force Exchange (AAFES), United State Navy, United State Air Force, United States Marine

Other Federal Agencies.

Specify.

State and Local Agencies.

Specify.

- Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

ACS, Aftermath Claim Service, AIM Healthcare Service, Connolly consulting, DiversiMed, End Game Strategy, EquiClaim(Viant/Concentra Preferred Systems), Iron Mountain, Pitney Bowes, Rawlings Company, Source One Direct, CMS

- Other** (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

- Yes** **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

Individuals who object to the collection of PII about themselves can decline participation in the health benefits plans managed by Aetna.

All Aetna members can file a complaint with the Complaint Resolution Team. The complaint will be evaluated and investigated by an employee trained in complaint handling. A letter advising the member of the complaint investigation will be sent to the member at the end of the investigation.

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

- Yes** **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

Aetna will require member authorization unless the use or disclosure is otherwise specifically allowed under the HIPAA privacy regulations or applicable law.

(2) If "No," state the reason why individuals cannot give or withhold their consent.



k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

- Privacy Act Statement
- Privacy Advisory
- Other
- None

Describe each applicable format.

Privacy Practices and Procedures
 Aetna as a Business Associate of
 A Self-Funded Plan Sponsor's Group Health Plan

Congress passed the Health Insurance Portability and Accountability Act (HIPAA) in 1996. The Privacy Rule, regulations that were issued by the Department of Health and Human Services in support of the Administrative Simplification section of HIPAA, was passed in December 2000.

The Privacy Rule went into effect on April 14, 2003. Essentially, the Privacy Rule restricts the use and disclosure of member health information by health plans (including insurers and self-insured plans), health care clearinghouses, providers who transmit member health information electronically, and their respective Business Associates. The Privacy Rule also provides members with certain rights, with respect to their health information – for example, members have the right to receive a Notice of their health plans' information practices; they also have the right to request access to or amend their health information.

To effectively administer our benefits plans, Aetna collects, creates, uses and/or discloses member health information. Member health information is information created or reviewed by Aetna that relates to the past, present or future physical or mental condition of a member; or to the provision of or payment for a member's health care. Member health information is information that either identifies, or there is reason to believe that it could be used to identify, a member.

Aetna, as a Business Associate of a Self-Funded Plan Sponsor's Group Health Plan, has access to, creates and/or receives certain member health information in conjunction with the services provided to a Self-Funded Plan Sponsor's Group Health Plan.

Aetna will use or disclose member health information only for the purpose of carrying out administrative functions for a Self-Funded Plan Sponsor's Group Health Plan in a manner consistent with the HIPAA Privacy Rule.

These administrative functions include activities such as the following:

Payment
 Aetna may use or disclose member health information for such payment-related activities as:

- Determining eligibility;
- Paying claims;
- Conducting utilization and medical necessity reviews;
- Coordinating care;
- Collecting fees and calculating cost-sharing amounts;
- Responding to complaints, appeals and requests for external review; and

- Obtaining payment under stop loss insurance.

Health Care Operations

Aetna may use or disclose member health information during the course of running our health business, that is, during operational activities such as:

- Quality assessment and improvement;
- Licensing;
- Accreditation by independent organizations;
- Performance measurement and outcomes assessment;
- Health services research;
- Preventive health, disease management, case management and care coordination.
- Underwriting and administration of stop loss policies;
- Risk management and auditing, and investigation of fraud or other unlawful conduct;
- Administration of pharmaceutical programs and payments;
- Transfer of policies or contracts from and to other health plans;
- Other general administrative activities, including data and information systems management, and customer service.

Treatment

Aetna may disclose information to doctors, dentists, pharmacies and other health care providers who are involved in a member's care. We may also use member health information in providing mail order pharmacy services and by sending certain information to doctors for patient safety or other treatment-related reasons.

Disclosures to Business Associates of the Self-Funded Plan Sponsor's Group Health Plan, or to other Covered Entities

Aetna may disclose member health information to a Business Associate of the Self-Funded Plan Sponsor's Group Health Plan for the purposes of treatment, payment and certain health care operations, but only as permitted or required by our Agreement with the Self-Funded Plan Sponsor's Group Health Plan or as required by law.

Additional Reasons for Uses or Disclosures of Member Health Information

Aetna may use or disclose member health information in order to provide members with information about treatment alternatives, treatment reminders or other health-related benefits and services. We may also disclose such information in support of:

- Research;
- Business Associates who provide services to us and assure us in writing that they will protect the information;
- Industry Regulations, such as the U.S. Food and Drug Administration, U.S. Department of Labor and other government agencies that regulate us;
- Law Enforcement;
- Legal Proceedings – in response to a court order or other lawful process;
- Public Welfare – to address matters of public interest as required or permitted by law, such as threats to public health and safety and national security.

Unintentional Disclosures

To prevent inappropriate disclosure of member health information, Aetna has adopted extensive Privacy policies and also uses rigorous quality assurance and audit procedures to assure that these policies are followed. Even with these strict safeguards in place, there may be instances where a member's health information may be disclosed due to unintentional errors that occur while handling a very high claim volume (e.g., claim volume is expected to be more than 175 million in 2004).

When unintentional disclosures are made due to clerical or computer error, Aetna will focus on identifying the cause for the error and implementing steps to prevent future occurrences. In those instances where such unintentional disclosures do not include detailed medical information or social security numbers, we will proceed to correct identified underlying problems and regard this as sufficient to satisfy our duty to manage these issues on your behalf. We will, however, notify plan sponsors of disclosures, unintentional or otherwise, that could harm a member's credit rating or cause embarrassment.

How Aetna will Respond to Requests for Member Health Information from a Member or a Member's Family and Friends

Member

All information about the member will be released if the member provides his/her Member Identity Information (i.e., the member's name, ID number and date of birth)

Parents of Unemancipated Minor Children (including Foster Parents and Guardians)

All information about the minor child will be released if the parent, foster-parent* or guardian* provides the minor child's Member Identity Information.

Stepparents, Grandparents or Domestic Partner Parents of Unemancipated Minor Children

A stepparent, grandparent or domestic partner parent who provides the minor child's Member Identity Information and confirms that he or she is involved in the member's health care or payment for such health care (and the Aetna representative determines that it is in the best interest of the minor child to provide information to the requestor) may:

- Make certain administrative changes/requests on behalf of the member (e.g., change PCP; order ID card).
- Obtain member-specific health information concerning eligibility and plan benefits (e.g., what types of services are included in the member's plan; what information needs to be provided for Aetna to process a specific claim; deductible information; treatment-related maximums; amount used against treatment-related maximums, except with respect to amounts used against behavioral health benefits, i.e., substance abuse/mental health). **
- Receive claim status information (e.g., confirmation of receipt or non-receipt of a claim, whether a claim is pending or has been paid or rejected, disclosure of date and amount of actual payment) if they can demonstrate some prior knowledge about the claim (i.e., provide some details about the service rendered, date of service, the provider's name, etc.). **

If the stepparent, grandparent or domestic partner parent submits a Third Party Authorization from the child's parent or (ii) some other legal document (e.g., Power of Attorney) authorizing them to act on the child's behalf, they may also obtain sensitive member-specific health information (e.g., diagnostic or treatment-related information).

* Aetna must also have documentation (e.g., Power of Attorney or court-order) supporting the requestor's status.

** Only that information directly relevant to the requestor's involvement in the member's health care or payment for health care will be disclosed.

Spouses and Ex-Spouses

A spouse or ex-spouse who provides the member's Member Identity Information, may:

- Make certain administrative changes/requests on behalf of the member (e.g., change PCP; order ID card).
- Obtain member-specific health information concerning eligibility and plan benefits (e.g., what types of services are included in the member's plan; what information needs to be provided for Aetna to process a specific claim; deductible information; treatment-related maximums; amount used against treatment-related maximums, except with respect to amounts used against behavioral health benefits, i.e., substance abuse/mental health).
- Receive claim status information (e.g., confirmation of receipt or non-receipt of a claim, whether a claim is pending or has been paid or rejected, disclosure of date and amount of actual payment) if they can demonstrate prior knowledge about the claim (i.e., provide some details about the service rendered, date of service, the provider's name, etc.).

If the spouse or ex-spouse submits a Third Party Authorization from the member or some other legal document (e.g., Power of Attorney), authorizing them to act on behalf of the member, they may also obtain sensitive member-specific health information (e.g., diagnostic or treatment-related information).

How Aetna will Respond to Requests for Member Health Information from a Self-Funded Plan Sponsor's Group Health Plan

A Self-Funded Plan Sponsor's Group Health Plan that provides Member Identity Information (i.e., the member's name, ID number and date of birth) may:

- Make certain administrative changes/requests on behalf of a member (e.g., change PCP; order ID card).
- Obtain member-specific health information concerning eligibility and plan benefits (e.g., what types of services are included in the member's plan; the subscriber's name; premium/rate information; what information needs to be provided for Aetna to process a specific claim; deductible information; treatment-related maximums; and amounts used against treatment-related maximums, except with respect to amounts used against behavioral health benefits, i.e., substance abuse/mental health).
- Receive claim status information (e.g., confirmation of receipt or non-receipt of a claim, whether a claim is pending or has been paid or rejected, disclosure of date and amount of actual payment) if they can demonstrate some prior knowledge about the claim (i.e., provide some details about the service rendered, date of service, the provider's name, etc.).

Additionally, a Self-Funded Plan Sponsor's Group Health Plan that is able to provide Member Identity Information and has signed either (i) an ASC agreement that contains Aetna-approved confidentiality, non-disclosure and indemnification provisions or (ii) a Plan Sponsor Letter Agreement may:

- Change the subscriber's address.
- Obtain sensitive member-specific health information. For example, the Self-Funded Plan Sponsor's Group Health Plan may obtain details about or receive copies of EOBs or claims (without having to demonstrate prior knowledge about the claim – as is required above), inquire about benefits expended, used or remaining against behavioral health benefit maximums (i.e., substance abuse/mental health), and obtain diagnostic and treatment-related information.
- Receive standard reports that are needed to administer the plan, audit stop loss coverage, facilitate other plan audits or acquire information necessary to transfer administration of the plan to another administrator.

Aetna will also release sensitive member-specific health information to a Self-Funded Plan Sponsor's Group Health Plan if the Plan representative submits a Third Party Authorization from the member or the member is on the call and explicitly authorizes Aetna to release the information to the Self-Funded Plan Sponsor's Group Health Plan Representative.

Aetna will not require a Self-Funded Plan Sponsor's Group Health Plan to submit to Aetna a list of specific Plan employees to whom member-specific health information can be released. If the Self-Funded Plan Sponsor's Group Health Plan wishes to limit Aetna's disclosure of member-specific health information to specific Plan employees, the Self-Funded Plan Sponsor's Group Health Plan can arrange this through their Aetna representative.

How Aetna will Respond to Requests for Member Health Information from Vendors who Provide Services to a Self-Funded Plan Sponsor's Group Health Plan

Vendors include brokers, agents, consultants and stop-loss carriers who contract with and provide services to a Self-Funded Plan Sponsor's Group Health Plan (e.g., eligibility, plan administration, member claim questions).

Vendors who provide Member Identity Information (i.e., the member's name, ID number and date of birth) may make the same requests or receive the same member-specific health information as a Self-Funded Plan Sponsor's Group Health Plan. That is, vendors may:

- Make certain administrative changes/requests on behalf of a member (e.g., change PCP; order ID card).
- Obtain member-specific health information concerning eligibility and plan benefits (e.g., what types of services are included in the member's plan; the subscriber's name; premium/rate information; what information needs to be provided for Aetna to process a specific claim; deductible information; treatment-related maximums; and amounts used against treatment-related maximums, except with respect to amounts used against behavioral health benefits, i.e., substance abuse/mental health).
- Receive claim status information (e.g., confirmation of receipt or non-receipt of a claim, whether a claim is pending or has been paid or rejected, disclosure of date and amount of actual payment) if they can demonstrate some prior knowledge about the claim (i.e., provide some details about the service rendered, date of service, the provider's name, etc.).

Additionally, vendors who (i) are able to provide Member Identity Information and (ii) are under

contract to a Self-Funded Plan Sponsor's Group Health Plan that has signed either (a) an ASC agreement that contains Aetna-approved confidentiality, non-disclosure and indemnification provisions or (b) a Plan Sponsor Letter Agreement and (iii) have signed Aetna's Confidentiality and Non-Disclosure Agreement, may make the same requests or receive the same sensitive member-specific health information (including standard reports) as a Self-Funded Plan Sponsor's Group Health Plan. This means vendors may:

- Change the subscriber's address.
- Obtain sensitive member-specific health information. For example, the vendor may obtain details about or receive copies of EOBs or claims (without having to demonstrate prior knowledge about the claim – as is required above), inquire about benefits expensed, used or remaining against behavioral health benefit maximums (i.e., substance abuse/mental health), and obtain diagnostic and treatment-related information.
- Receive standard reports that are needed to administer the plan, audit stop loss coverage, facilitate other plan audits or acquire information necessary to transfer administration of the plan to another administrator.

Aetna will also release sensitive member-specific health information to a vendor under contract to a Self-Funded Plan Sponsor's Group Health Plan if the vendor submits a Third Party Authorization from the member or the member is on the call and explicitly authorizes Aetna to release the information to the vendor.

Aetna Will Enable Individuals to Exercise Their HIPAA Privacy Rights

As the Business Associate of the Self-Funded Plan Sponsor's Group Health Plan, Aetna will respond to all members' requests to exercise their HIPAA Privacy rights with respect to member health information maintained by Aetna and our Business Associates. Aetna's response to member requests will not include uses or disclosures of member health information made directly by, or maintained by, the Self-Funded Plan Sponsor's Group Health Plan or any of its other business associates.

Members should contact Aetna directly at the toll-free number provided on their ID card. Our customer service staff will provide instructions and any required forms to the member (Aetna will accept forms created by the Self-Funded Plan Sponsor's Group Health Plan, but only if they contain the same information as is requested by Aetna's forms). Our response to the member will contain instructions for the member to contact his/her employer directly if he/she wishes to exercise any HIPAA Privacy Rights with regard to member health information maintained by the Self-Funded Plan Sponsor's Group Health Plan or by any of its other business associates.

Aetna will respond to the member who exercises these rights:

Right to Access Member Health Information

- Aetna will accept, on behalf of the Self-Funded Plan Sponsor's Group Health Plan, members' requests for access to member health information in a designated record set in Aetna's possession or control, or in the possession or control of our business associates.
- Aetna will provide an Access Report to the member within 30 days of receipt of the information we need to fulfill the request (if we receive the request from the Self-Funded Plan Sponsor's Group Health Plan, we will fulfill the request within 25 days). If records are stored off-site, we may request an extension of no more than an additional 30 days to fulfill the request. We will inform the member or Self-Funded Plan Sponsor's Group Health Plan (depending on who submitted the request) in writing if such an extension is needed.
- Currently, Aetna does not charge a fee for fulfilling access requests.

Right to Make Certain Amendments to Member Health Information

- Aetna will accept, on behalf of the Self-Funded Plan Sponsor's Group Health Plan, members' requests to amend member health information in a designated record set in Aetna's possession or control, or in the possession or control of our business associates.
- We will require that the request be in writing and that it include the reason for the request (Aetna does not have a form for amendment requests).
- Aetna will notify the member in writing of its decision to grant or deny the amendment request, within 60 days of receipt of the information we need to fulfill the request (if we receive the request

from the Self-Funded Plan Sponsor's Group Health Plan, we will respond within 55 days). We will notify the member or Self-funded Plan Sponsor's Group Health Plan (depending on who submitted the request) in writing if we require an extension of up to 30 days to complete the report.

- If we deny the request, the member may file a written Statement of Disagreement that Aetna will maintain on record.

Right to Receive an Accounting of Certain Disclosures of Member Health Information

• Aetna will accept, on behalf of the Self-Funded Plan Sponsor's Group Health Plan, members' requests for a report of disclosures made by Aetna or our business associates for which the HIPAA Privacy Rule requires us to provide an accounting.

• We will provide an Accounting Report to a member within 60 days of receipt of the information we need to fulfill the request (if we receive the request from the Self-Funded Plan Sponsor's Group Health Plan, we will respond within 55 days). We will notify the member or the Self-Funded Plan Sponsor's Group Health Plan (depending on who submitted the request) in writing if we require an extension of up to 30 days to complete the report.

- If the member requests such an accounting more than once in a 12-month period, we may charge the member a reasonable fee.

Right to Request Restrictions on Use or Disclosure of Member Health Information and Right to Have Member Health Information Communicated through Confidential Means

• Aetna will accept reasonable requests to communicate with members in a certain way or at a certain location.

• Aetna will consider, but may not agree to, requests to restrict the way we use or disclose member health information in connection with healthcare operations, payment or treatment, or to restrict disclosures to persons involved in the member's health care.

• If made to Aetna directly, we will not require that these requests be in writing. However, members who make these requests through the Self-Funded Plan Sponsor's Group Health Plan must complete and sign the Aetna form entitled "Notification of Restriction and/or Confidential Communications". It is important to note that the Self-Funded Plan Sponsor's Group Health Plan should not accept requests for restrictions and/or confidential communications from Aetna members, as not all such requests can be accommodated, and the HIPAA Privacy Rule does not require that all such requests be accepted.

Right to File a Complaint

• Members who believe their privacy rights have been violated have the right to file a complaint. They may do so by calling the toll-free number provided on their ID card.

- Customer service professionals will route complaints to the appropriate complaint-handling team.
- Members may also write to the Secretary of the U.S. Department of Health and Human Services.

Notification to the Self-Funded Plan Sponsor's Group Health Plan of Access, Amendment and Accounting Requests

If requested, Aetna will distribute a quarterly report to the Self-Funded Plan Sponsor's Group Health Plan which indicates the number of each type of request received per month, the average turnaround time, the number of open requests as of the date of the report, and if requested, the member name and SSN.

Transmitting Member Health Information Via Internet E-Mail

No means of communication is perfectly secure. While the Internet is relatively secure and is an appropriate means for communicating many messages, there is an increasing consensus among security personnel that the Internet is not a good means for communicating particularly sensitive messages. Aetna's Internet e-mail policy balances our desire for quick, reliable communications against our need to protect the confidentiality of member-specific health information. In striking that balance, we will continue to use Internet e-mail to communicate less sensitive member health information (e.g., confirming whether or not a claim has been received or paid) and will do so without encrypting the message. However, Aetna's policy is to encrypt e-mails that transmit sensitive member health information to anyone outside Aetna's computer network.

Self-Funded Plan Sponsor's Group Health Plans who would like to continue to receive member health information in electronically delivered standard or ad hoc reports, or wish to assist their employees to resolve claim issues with Aetna Member Services via e-mail, may obtain encryption services through the use of Secure File Transport Protocol or Secure FTP – this service is being offered at no charge

and may be arranged by contacting the Aetna representative who services the plan.

Notice of Privacy Practices

Aetna has made available to Self-Funded Group Health Plans a copy of the Notice of Privacy Practices we use for our insured plans. Aetna does not create a Notice of Privacy Practices for Covered Entities. Aetna's Notice of Privacy Practices (by Plan Type) is available online at http://www.aetna.com/about/information_practices.html.

Summary Plan Descriptions (SPDs)

The Privacy Regulations restrict a Self-Funded Plan Sponsor's Group Health Plan's ability to share member-specific health information (other than summary data) with the plan sponsor unless the sponsor has amended its plan documents in accordance with HIPAA's requirements. In addition to amending its SPD language, the plan sponsor is required to provide a certification to the Self-Funded Plan Sponsor's Group Health Plan that the plan documents have been amended appropriately.

Aetna believes these activities are between the self-funded plan and the plan sponsor; therefore, there is no need to submit a certificate of plan amendment to Aetna. For sample SPD language, contact the Aetna representative who services the plan.

Sanctions for Violations

Employee violations of Aetna's Privacy Policies and procedures may lead to disciplinary action up to and including termination.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.