

# HIPAA Administrative Simplification and Privacy An Update on Aetna's Compliance Efforts

## ***PRIVACY***

***Aetna will meet the April 14, 2003 compliance deadline for the HIPAA Privacy Rule.***

Over the past two years, Aetna's Privacy Office has been working closely with representatives from our business and IT areas to address the various requirements of the HIPAA Privacy Rule. Here are answers to some frequently asked questions about our HIPAA Privacy compliance efforts:

### **Privacy Official**

**Q. Has Aetna designated a Privacy Official?**

A. Yes. Thomas A. Young is Aetna's Chief Privacy Officer and heads our Privacy Office. The Chief Privacy Officer has responsibility for overseeing the development, implementation and enforcement of Aetna's privacy policies and procedures (see "Policies and Procedures" below for specific information about our privacy policies and procedures).

### **Notice of Privacy Practices**

**Q. Will Aetna distribute a Privacy Notice?**

A. Yes. Aetna has developed a Notice of Privacy Practices to satisfy its obligation to provide a HIPAA privacy notice to its fully-insured subscribers. During the first quarter of 2003, Aetna will distribute the Notice to all subscribers who were enrolled in Aetna insured Medical or Long Term Care benefits plans as of January 1, 2003. This chart outlines the methods that will be used to deliver the Notice to fully-insured subscribers:

<b>PLAN TYPE</b>	<b>DELIVERY METHOD</b>
<b>Health</b> (including Medical, Dental, Managed Behavioral Health, Pharmacy and Vision)	Notice included as insert in the 1Q2003 publication of <i>Healthy Insights</i> newsletter
<b>Dental Only</b>	Notice sent to subscribers via 1Q2003 direct mailing
<b>Long Term Care*</b>	Notice included as an insert in the 1Q2003 publication of the <i>Long Term Care Messenger</i> newsletter

\* Aetna will provide a Notice of Privacy Practices to individuals who subscribe to insured Long Term Care plans once they have filed a claim with Aetna

For fully-insured subscribers who enroll *after* January 1, 2003, Aetna will distribute the Notice through multiple channels -- on the back of ID card carriers, via direct mailings, in brochures that accompany enrollment materials, and as an insert to newsletters. Aetna will also remind fully-insured subscribers every three years about their right to receive a privacy notice.

After April 14, 2003, Aetna members can receive an additional copy of Aetna's Notice of Privacy Practices by contacting Aetna directly at the toll-free number found on their member ID card *or* by visiting the Aetna.com web site.

**Q. Are self-funded plan sponsors required to distribute a Privacy Notice?**

- A. Yes. Self-funded plan sponsors are required to develop and deliver a privacy notice to their plan participants prior to the April 14, 2003 HIPAA Privacy compliance date. These plan sponsors will need to determine if the information in Aetna's Notice would be helpful in creating their own Notice. Self-funded plan sponsors who have not yet created their own Notice should seek assistance from their professional advisors.

Plan Sponsors may view Aetna's Notice of Privacy Practices at:

[http://www.aetna.com/about/information\\_practices.html](http://www.aetna.com/about/information_practices.html)

**Q. Will Aetna help self-funded plan sponsors distribute their Privacy Notice? If so, what is the charge?**

- A. To the extent that our Customized Communications Group has capacity to handle a special mailing at a particular point in time, we can consider requests to assist with distribution. Plan Sponsors should contact their Aetna representative for information about obtaining a quote for this service.

### **Other Member Rights**

**Q. Has Aetna established processes to enable members to exercise the rights afforded to them under the Privacy Rule – specifically, the right to ask their health plan to:**

- **provide access to their Protected Health Information (PHI),**
- **make certain amendments to their PHI,**
- **provide an accounting of certain disclosures of their PHI,**
- **restrict uses or disclosures of their PHI and/or**
- **communicate with them in a certain way or at a certain location?**

- A. Yes. Aetna is prepared to respond to member requests to exercise their privacy rights, with respect to PHI maintained by Aetna and our business associates. Aetna members who wish to exercise their HIPAA Privacy rights should contact Aetna directly at the toll-free number found on their member ID card. It is important to note that plan sponsors 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.

**Q. Will members be required to use forms to exercise their privacy rights?**

- A. Members will be required to complete and return forms to Aetna to exercise certain of their privacy rights; other rights may be exercised without a form (e.g., by telephone):

<b>Privacy Right to be Exercised by the Member</b>	<b>Is a Form Required?</b>	<b>Name of the Form Required</b> (to be provided to the Member by Aetna at the time the request is made)	<b>Will Aetna accept a Form that has been developed by the Plan Sponsor, or a written request from the Member?</b>
<b>Access to PHI</b>	Yes	Protected Health Information (PHI) Access Request  Aetna Form #: GR-67902	Yes. However, the Plan Sponsor-developed form or Member written request must include the data elements that are included in Aetna's form*.
<b>Amendment to PHI</b>	No, but the request must be made in writing	Not applicable	Yes. Aetna will accept either a form developed by a Plan Sponsor <i>or</i> a written request from the Member.
<b>Accounting</b>	Yes	Request for an Accounting of Disclosures of Protected Health Information ("PHI")  Aetna Form #: GR-67935	Yes. However, the Plan Sponsor-developed form or Member written request must include the data elements that are included in Aetna's form*.
<b>Restriction and/or Confidential Communication</b>	No	Not Applicable	Members may make requests for, or removal of, Restrictions and/or Confidential Communications verbally. Aetna will also accept a form developed by a Plan Sponsor <i>or</i> a written request from the Member.
<b>Third Party Authorization</b>	Yes	Authorization for Release of Protected Health Information (PHI)  Aetna Form #: GR-67938	Yes. However, the Plan Sponsor-developed form or Member written request must include the data elements that are included in Aetna's form*.
<b>Revocation of Third Party Authorization</b>	Yes	Revocation of Authorization Previously Given to Aetna  Aetna Form #: GR-67943	Yes. However, the Plan Sponsor-developed form or Member written request must include the data elements that are included in Aetna's form*.

\*Plan Sponsors may contact their Aetna representative for a reference copy of Aetna's form. Aetna will contact the Member by phone if key data is missing.

**Q. Will Aetna respond to members' requests to exercise their privacy rights regarding PHI maintained by, or uses or disclosures made directly by, a self-funded group plan, or by any of the self-funded plan's other business associates?**

A. No. Aetna will instruct the member to contact his/her employer directly if he/she wishes to exercise any HIPAA Privacy rights with regard to PHI maintained by the employer's self-funded group health plan or by any of its other business associates.

### **Business Associate Agreements**

**Q. What steps has Aetna taken to enter into Business Associate Agreements with service providers who have access to member PHI?**

A. Aetna has approximately 1,200 Business Associate relationships for contracted services: off-site data storage and warehousing, printing and fulfillment services, electronic claims clearinghouse support, disease management services, delegated provider arrangements, consulting services and more.  
Aetna has drafted a standard contract amendment that conforms to the model suggested by the U.S. Department of Health and Human Services. Amendments have

been mailed to all of our Business Associates, and our re-contracting efforts with them are well under way.

**Q. Will Aetna enter into Business Associate Agreements with Self-Funded Plans?**

- A. Yes. Self-funded plans will need to enter into “business associate” agreements with all service providers who have access to Protected Health Information (PHI):
- We are a business associate to self-funded plans, and in February 2002, we signed and mailed an ASC Amendment to those customers with self-funded plans that were in force up to and including January 1, 2002.
  - In March 2002, HHS published a model Business Associate Agreement.
  - In August 2002, HHS issued final modifications to the HIPAA Privacy Regulations, which contained sample language covered entities could use in their agreements.
  - In September 2002, we updated our Amendment to the ASC Agreement to include the HHS sample Business Associate language.

Although we are willing to abide by the terms of the original Amendment we distributed in February 2002, customers may prefer to use an Amendment that includes the HHS sample Business Associate language. *Plan sponsors who have already signed and returned the February 2002 version of the Amendment to us are not required to do anything further. However, plan sponsors who wish to use the Amendment prepared in September 2002 should contact their Aetna representative to obtain a copy.*

**Q. Where should self-funded plans send their signed ASC Agreement Amendments (or alternatively, Business Associate Agreements that have been prepared by self-funded plan sponsors)?**

- A. Amendments to the ASC Agreement *or* Business Associate Agreements prepared by self-funded plans should be returned/submitted to Aetna as follows:
- Self-funded National Accounts customers should return signed ASC Amendments or submit their Business Associate Agreements to their Aetna representatives.
  - Self-funded Key Accounts customers should return signed ASC Amendments or submit their Business Associate Agreements to: Aetna Drafting Project Team; 151 Farmington Avenue, MC2L; Hartford, CT 06156.

**Q. Will Aetna enter into Business Associate Agreements with Fully-Insured Plans?**

- A. No. A Business Associate agreement between Aetna and a fully-insured plan sponsor is unnecessary – as neither party is considered a “business associate” as defined in Section 160.103 of the HIPAA Privacy Rule.

**Q. Will Aetna enter into Business Associate Agreements with Providers?**

- A. Except with regard to delegated service arrangements, Business Associate agreements between Aetna and providers are unnecessary – as neither party is considered a “business associate” as defined in Section 160.103 of the HIPAA Privacy Rule.

Aetna has mailed a Business Associate contract amendment to providers with whom Aetna has delegated claim and/or utilization management arrangements, and re-contracting efforts are well under way (see the question above that reads “What steps has Aetna taken to enter into Business Associate Agreements with service providers who have access to member PHI?”).

## **Uses and Disclosures of PHI**

### **Q. How will Aetna protect member PHI from inappropriate and unauthorized use and disclosure?**

- A. Historically, Aetna has had policies, procedures and technologies in place to protect sensitive information against inappropriate and unauthorized use and disclosure. Access to member information is highly restricted; only employees with a legitimate need to know have access. Now, Aetna’s protection of member information is more vigorous than ever.

To safeguard member PHI from inappropriate and unauthorized use and disclosure under the HIPAA Privacy Rule, Aetna has updated company-wide procedures for responding to requests for member health information. Our new procedures promote consistency across the company in handling requests for member health information. These procedures delineate, by type of requestor (e.g., Member; Spouse; Ex-Spouse; Parent of Minor Child; Plan Sponsor; Broker or Agent; Business Associate; Other Insurance Carrier), the information that can be disclosed and the circumstances under which we can disclose it.

### **Q. What information will Aetna disclose to self-funded plan sponsors?**

- A. In 1Q2003, Aetna sent a communication to self-funded plan sponsors explaining how Aetna’s revised procedures for responding to requests for member health information may impact them and included a copy of Aetna’s “Authorization for Release of Protected Health Information”. Self-funded plan sponsors who did not receive this communication should contact their Aetna representative for a copy.

### **Q. What information will Aetna disclose to fully-insured plan sponsors?**

- A. Aetna will not share PHI with fully insured plan sponsors without the member’s authorization, unless otherwise permitted by law. We have stringent guidelines in place to handle any request for an exception to this rule. We will provide “summary health information” to a fully insured plan sponsor but only if the plan sponsor sends us a written request that confirms that the information will be used for HIPAA-sanctioned purposes. If a fully insured plan sponsor wishes to receive more than “summary health information”, they will have to amend their plan documents (e.g., Summary Plan Description) to reflect the restrictions that the HIPAA Privacy Rule places on how the Plan will use or disclose such information, provide Aetna with the necessary certification and sign an Aetna confidentiality agreement.

### **Q. What guidance will Aetna provide on the Summary Plan Description (SPD) language needed to satisfy the Privacy Rule?**

- A. We have a sample ‘template’ available for self-funded plan sponsors to use (upon request) in developing a description of their privacy practices. If Aetna provides

assistance with the production of SPDs, we can incorporate this information if it is provided by the plan. We are unable to provide a ‘one size fits all’ description due to the number of possible variations in how health plans use or protect their members’ information. This template is also available to fully insured plan sponsors who use more than summary health information. See preceding Q&A.

### **Physical and Electronic Security**

**Q. Does Aetna have administrative, technical and physical safeguards to protect the privacy of PHI?**

A. Aetna has always been concerned with security, and we have policies, procedures and technologies in place that are used to protect sensitive information against inappropriate and unauthorized use and disclosure. These include security awareness training for employees, integrity and role-based access controls, message authentication and/or encryption, firewall and proxy server technologies, etc. We restrict access to member health information to those employees who need it to provide our products or services. We maintain physical, electronic and procedural safeguards to protect member health information against unauthorized access and use. Access to our facilities is limited to authorized personnel and we protect information we maintain electronically through use of a variety of technical tools.

**Q. How will Aetna handle the transmission of PHI via Internet e-mail?**

A. 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 need for quick, reliable communications against our obligation 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 health member-specific 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 use “encryption” to transmit *sensitive* PHI to anyone outside Aetna’s computer network. (“Encryption” refers to several technologies that code information so that only the intended recipient can read it).

Self-funded plan sponsors who would like to continue to receive PHI in standard or ad hoc reports, or to assist their employees to resolve claim issues with Aetna Member Services, may obtain encryption services through the use of Secure File Transport Protocol or Secure FTP – this service is being offered at no charge to you and may be arranged by contacting your Aetna representative.

### **Privacy Policies, Procedures and Training**

**Q. Has Aetna implemented policies and procedures that comply with the HIPAA Privacy Rule requirements?**

A. Aetna has created a library of company-wide Privacy policies for the business areas impacted by the HIPAA Privacy Rule. Procedures for responding to the Privacy policies are being finalized, and will be implemented by the April 14, 2003 compliance date. Among the requirements addressed by our Privacy policies and procedures are:

- *Members' privacy rights with respect to PHI:*
  - ✓ *Access*
  - ✓ *Amendment*
  - ✓ *Accounting*
  - ✓ *Restrictions and/or Confidential Communications*
  - ✓ *Privacy Notice*
- *Physical and Electronic Safeguards for PHI*
- *Privacy Complaints and Sanctions*
- *Use and Disclosure of Member PHI*
- *Privacy Training*

**Q. Has Aetna's workforce been trained on its Privacy policies and procedures?**

A. All Aetna employees have been briefed on the various HIPAA Privacy requirements via a mandatory web-based training tool and they will receive additional training in the coming months. Employees who are impacted by Aetna's new or revised privacy-related procedures will receive "just in time" training – this training will be completed by April 14, 2003. Privacy has also been incorporated into Aetna's training programs for newly hired employees, temporary employees and consultants.

**Q. Will Aetna provide copies of its Privacy policies to Plan Sponsors?**

A. Aetna's Privacy policies contain proprietary information and, therefore, cannot be distributed outside the Company. Aetna's Privacy policies are summarized in our Notice of Privacy Practices. Plan Sponsors may view Aetna's Notice of Privacy Practices at: [http://www.aetna.com/about/information\\_practices.html](http://www.aetna.com/about/information_practices.html)

### **Complaints and Sanctions**

**Q. Does Aetna have a process that enables members to make complaints concerning Aetna's privacy policies and procedures?**

A. Aetna members who feel their privacy rights have been violated may file a complaint by contacting Aetna directly at the toll-free number found on their member ID card. Members may also write to the Secretary of the U.S. Department of Health and Human Services. Members will not be penalized for filing a complaint.

**Q. Will Aetna discipline employees for privacy-related violations?**

A. Yes. Aetna has adopted specific disciplinary procedures and sanctions for employees who violate the company's HIPAA Privacy Policies.

## ***ELECTRONIC TRANSACTIONS AND CODE SETS***

Aetna has established a HIPAA Program Management Office (HIPAA PMO) that is responsible for coordinating our response to the HIPAA Electronic Transaction and Code Sets Regulations (“T&CS Regulations”). The following are questions and answers that reflect our efforts to comply with the T&CS Regulations. Note: Information of interest to Providers and Plan Sponsors is presented separately below.

### **Information for Providers:**

#### **Readiness, Extension Requests, and Timing**

**Q. Has Aetna filed for an extension for compliance with the T&CS Regulations?**

A. The original compliance date for the T&CS Regulations was October 16, 2002. However, Congress has authorized a one-year extension to October 16, 2003 for those covered entities that submitted a Model Compliance Plan to the U.S. Department of Health and Human Services (HHS) on or before October 15, 2002. Aetna filed its own extension on September 3, 2002. As a result, Aetna’s health plans are not required by law to be compliant until October 16, 2003. However, as noted in the following Q&As, Aetna’s actual timetable for compliance with respect to code sets and certain transactions is earlier than October 16, 2003.

**Q. What is Aetna’s schedule for compliance with T&CS Regulations?**

A. Please see Schedule A, attached.

**Q. Will Aetna continue to support transactions in non-HIPAA formats?**

A. We will continue to support non-HIPAA compliant transactions until 10/16/2003.

**Q. Will Aetna continue to support local (home grown) code sets?**

A. At this time, Aetna does not plan to accept claim submissions that contain local (home grown) codes after the end of 2Q 2003.

**Q. Is a trading partner agreement necessary between providers and Aetna?**

A. Currently Aetna does not accept direct submission of transactions from providers. All provider submissions must be routed through an Aetna-contracted clearinghouse. Therefore, because providers do not directly send transactions to Aetna, trading partner agreements are not necessary.

#### **Connectivity**

**Q. How do providers/vendors submit claims to Aetna?**

A. Providers must direct all of their HIPAA transactions to one of Aetna’s designated clearinghouses.

**Q. What clearinghouses are currently connecting to Aetna?**

A. Please see Schedule A, attached, for a list of clearinghouses currently connecting to Aetna.

**Q. Whom should providers/vendors contact with questions pertaining to how transactions are to be transmitted (e.g., individually or in batches, transmission modes, encryption/authentication methods, etc.)?**

A. Please contact your clearinghouse.

### **Formats and Business Processes**

**Q. Are there any changes in Aetna-specific data, coding or documentation requirements for electronic transactions?**

A. All changes will be made in accordance with the HIPAA regulations and the Implementation Guides for each transaction. Aetna-specific data, coding, or documentation requirements will be provided in Companion Guides to clearinghouses, which were developed in conjunction with implementation of the standard transactions. Providers should contact their clearinghouses to obtain the Companion Guides.

**Q. What are Aetna's plans for replacing local (home grown) code sets with standard code sets?**

A. Aetna has cross-walked local codes to HIPAA-compliant standard codes, enabling the replacement of local with compliant codes. Providers with HIPAA non-compliant codes in their contracts have received a 90-day advance notice letter notifying them of the effort. Subsequently, impacted Providers may receive a letter or amendment to their contract identifying the new HIPAA-compliant codes to be substituted for the non-compliant codes by a specified date.

### **Testing**

**Q. What is the process for testing transactions? What is expected of providers/vendors?**

A. Providers and vendors should contact their clearinghouse to arrange testing (Please see Schedule A for a list of clearinghouses currently connecting to Aetna).

### **Certification**

**Q. Will Aetna be certified by a third party agency? How/when will providers/vendors be notified?**

A. The T&CS Regulations do not require covered entities to obtain certification of electronic transactions and code sets compliance. Aetna is in the process of evaluating the benefits of certification, including the services and tools that facilitate the certification process.

**Q. Will Aetna require providers/vendors to be certified by a third party agency?**

A. No. If a vendor or provider wishes to become certified, they will need to work directly with a certification agency.

# ***ELECTRONIC TRANSACTIONS AND CODE SETS***

## **Information for Plan Sponsors:**

### **Readiness, Extension Requests, and Timing**

#### **Q. Has Aetna filed for an extension with the U.S. Department of Health and Human Services (HHS)?**

- A. The original compliance date for the T&CS Regulations was October 16, 2002. However, Congress has authorized a one-year extension to October 16, 2003 for those covered entities that submitted a Model Compliance Plan to the U.S. Department of Health and Human Services (HHS) on or before October 15, 2002. Aetna filed its own extension on September 3, 2002. As a result, the T&CS compliance date for Aetna health plans is now October 16, 2003.

#### **Q. What is Aetna's schedule for transactions compliance?**

- A. Please see Schedule A, attached.

### **Formats and Business Processes**

#### **Q. Which of the standard transactions apply to plan sponsors?**

- A. The Health Plan Premium Payments (820) and Benefit Enrollment and Maintenance (834) transactions pertain to plan sponsors or their third party administrator.

#### **Q. What is expected of plan sponsors for HIPAA compliance with these (Health Plan Premium Payments and Benefit Enrollment and Maintenance) transactions?**

- A. Plan sponsors, whether fully-insured or self-funded, are not “covered entities” for the purposes of the HIPAA Regulations, and, therefore, are **not** required to utilize the T&CS standards when conducting these transactions. A plan sponsor may, however, voluntarily choose to use the T&CS standards, and Aetna would be required to accommodate that election. **Note:** The self-funded health plan created by a plan sponsor is a covered entity under the HIPAA T&CS Regulations and is subject to all HIPAA mandates. A plan sponsor may, however, voluntarily choose to use the T&CS standards and Aetna would be required to accommodate that election.

#### **Q. What is Aetna's preferred format for receiving electronic enrollment information from a plan sponsor?**

- A. Aetna's preferred format for receiving electronic enrollment information from a plan sponsor is the 1000-Byte layout.

#### **Q. What is Aetna's preferred format for receiving premium payment information from a plan sponsor?**

- A. Aetna's preferred format for receiving premium payment information is in an electronic spreadsheet that can easily be converted to a Comma Separated Value (CSV) format.

**Q. Will Aetna accept electronic premium payment or electronic enrollment information using the HIPAA T&CS standard?**

- A. If a plan sponsor chooses to send Aetna either electronic premium payment information using the T&CS standard Health Plan Premium Payments (820) format or electronic enrollment information using the T&CS standard Benefit Enrollment and Maintenance (834) format, Aetna will accept the transaction (subject to Aetna's standard connectivity setup process).

**Q. Are Aetna's Implementation Guides for transactions available?**

- A. An Aetna Implementation Guide for the HIPAA-compliant version of each transaction (Health Plan Premium Payment (820) and Benefit Enrollment and Maintenance (834)) has been developed and is available to facilitate the installation of either transaction upon request by a plan sponsor or its third party administrator. New plan sponsors should contact their Account Executive and existing plan sponsors should contact their Eligibility and/or Premium consultant to receive copies of Implementation Guides and to initiate testing and set-up of either transaction.

**Connectivity and Testing**

**Q. How do plan sponsors submit/test electronic premium payment or electronic enrollment information to Aetna?**

- A. This type of electronic information can be sent directly to Aetna by following Aetna's standard connectivity setup process.

## Schedule A

The following schedule represents our work with respect to electronic transactions.

Transaction Name	Anticipated Readiness Date	Clearinghouses connecting to Aetna **
270/271 – Eligibility Benefit Inquiry and Reponse	Compliant	WebMD, MedUnite, DentalExchange, Proxymed, HDX, Health Fusion
276/277 – Claim Status Inquiry and Response	Compliant	WebMD, MedUnite, Proxymed, Health Fusion
278 – Referral Authorization and Precertification	3Q 2003*	WebMD, MedUnite, Health Fusion
820 – Payment Order/Remittance Advice	Compliant	N/A – Plan Sponsor direct connection
834 – Benefit Enrollment/Disenrollment	Compliant	N/A – Plan Sponsor direct connection
835 – Payment and Remittance Advice	2Q 2003	WebMD, MedUnite, Proxymed, NDC, HDX
837 – Institutional Claim	Compliant	WebMD, ProxyMed, NDCHealth
837 – Professional Claim	Compliant	WebMD, MedUnite, Health Fusion, Proxymed, NDC
837 – Dental Claim	Compliant	WebMD, DentalExchange
NCPDP – Retail Pharmacy Claim	Compliant	WebMD, NDC

\* Aetna currently supports medical Referral Authorization and Precertification transactions. Aetna plans to support Precertification requests for appeals and extensions by 3Q 2003.

\*\*Additional clearinghouses may be contracted during 2003.

- These dates are based on our current project plans and are subject to change without notice.
- The original compliance date for the HIPAA Electronic Transactions and Code Sets Regulations (“T&CS Regulations”) was October 16, 2002. However, Congress has authorized a one-year extension to October 16, 2003 for those covered entities that submitted a Model Compliance Plan to the U.S. Department of Health and Human Services (HHS) on or before October 15, 2002. Aetna filed its own extension on September 3, 2002. As a result, the T&CS compliance date for Aetna health plans is now October 16, 2003.