

**HIPAA PRIVACY & SECURITY  
POLICIES & PROCEDURES  
FOR HEALTH PLANS SPONSORED BY  
AMERICAN AIRLINES, INC.**

**Table of Contents**

<b>STATEMENT OF PRIVACY POLICY</b> .....	5
<b>I. ORGANIZED HEALTH CARE ARRANGEMENT</b> .....	6
<b>II. PRIVACY &amp; SECURITY OFFICER</b> .....	7
<b>III. PROTECTED HEALTH INFORMATION</b> .....	8
<b>IV. NOTICES OF PRIVACY PRACTICES</b> .....	10
Distribution of Notice .....	10
Material Changes to the Notice.....	10
Availability of Notice .....	10
Right to Receive a Copy of the Notice .....	10
Content of Notice .....	10
<b>V. USE OR DISCLOSURE OF PHI / HIPAA AUTHORIZATION</b> .....	11
Use & Disclosure of PHI .....	11
Authorization .....	11
Genetic Information .....	12
Claims Assistance .....	12
Marketing & Sale of PHI .....	12
<b>VI. DISCLOSURE TO THE COMPANY</b> .....	13
<b>VII. DISCLOSURE TO FAMILY MEMBERS OR PERSONAL REPRESENTATIVES</b> ..	15
<b>VIII. MINIMUM NECESSARY STANDARD</b> .....	17
<b>IX. PROTECTION OF PHI</b> .....	18
<b>X. CLAIMS ASSISTANCE</b> .....	21
<b>XI. PARTICIPANT’S RIGHT TO ACCESS PHI</b> .....	22
Participant’s Right .....	22
Deadline to Respond .....	22
PHI Held by Business Associate / Insurer .....	22
PHI Held by the Company .....	22
Retention .....	22
<b>XII. PARTICIPANT’S RIGHT TO AMEND PHI</b> .....	23
Participant’s Right .....	23
Deadline to Respond .....	23
PHI Held by Business Associate / Insurer .....	23
PHI Held by the Company .....	23

Retention .....	23
<b>XIII. PARTICIPANT’S RIGHT TO ACCOUNTING OF DISCLOSURES .....</b>	<b>24</b>
Participant’s Right .....	24
Deadline to Respond .....	24
PHI Disclosures by Business Associate / Insurer .....	24
PHI Held by the Company .....	25
Disclosure Log .....	25
Retention .....	25
<b>XIV. PARTICIPANT’S RIGHT TO REQUEST RESTRICTIONS ON PHI .....</b>	<b>26</b>
Participant’s Right .....	26
PHI Held by Business Associate / Insurer .....	26
PHI Held by the Company .....	26
Record Retention .....	26
<b>XV. PARTICIPANT’S RIGHT TO REQUEST CONFIDENTIAL COMMUNICATIONS</b>	
27	
PHI Held by Business Associate/Insurer .....	27
PHI Held by the Company .....	27
Record Retention .....	27
<b>XVI. TRAINING .....</b>	<b>28</b>
Initial Training .....	28
Newly Hired Employees .....	28
Ongoing Training .....	28
<b>XVII. DISCIPLINE FOR VIOLATIONS .....</b>	<b>29</b>
Sanctions .....	29
Mitigation .....	29
Complaints .....	29
<b>XVIII. SECURITY BREACH NOTIFICATION .....</b>	<b>30</b>
Security Breach Rules .....	30
☞ If an exception doesn’t apply, the Plan must consider the following factors: .....	31
Notification of Individual .....	31
Notification of Media .....	32
Notification to HHS .....	32
<b>XIX BUSINESS ASSOCIATE AGREEMENTS .....</b>	<b>33</b>
Business Associate Contract .....	33

Disclosures to Business Associates .....	33
<b>APPENDIX A - PRIVACY OFFICER AND SECURITY OFFICER.....</b>	<b>34</b>
<b>APPENDIX B - APPLICABLE HEALTH PLANS.....</b>	<b>35</b>
<b>APPENDIX C – HIPAA COMPLAINT FORM.....</b>	<b>36</b>
<b>APPENDIX D – HIPAA AUTHORIZATION FORM.....</b>	<b>38</b>

## STATEMENT OF PRIVACY POLICY

American Airlines (the “Company”) has developed these HIPAA Privacy & Security Policy & Procedures (the “Policy”) to comply with the Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164, under the Health Insurance Portability and Accountability Act of 1996 (the “Privacy & Security Rule”), as updated by The Health Information Technology for Economic and Clinical Health Act (“HITECH Act”) and various regulations and guidance.

The Company sponsors the self-funded and fully insured group health plans listed on Attachment A. For purposes of this Policy, the plans listed on Attachment A are referred to collectively and singularly as the “Plan.”

This Policy only applies to the benefits offered by the Plan that are subject to the Privacy & Security Rule, which includes medical benefits, dental benefits, vision benefits, prescription drug benefits, employee assistance programs and health flexible spending accounts. This Policy does not apply to (i) on-site clinics that the Company may operate; (ii) disability, life insurance, or other non-HIPAA covered benefits offered by the Plan or Company; or (iii) workers’ compensation benefits. Note that the vendor that operates an on-site clinic may be considered a “health care provider” under the Privacy & Security Rule if it engages in any of the HIPAA-standardized electronic transactions, such as claims submission and payment, coordination of benefits and eligibility for a health plan. If the vendor is a “health care provider” under the Privacy & Security Rule, the vendor, not the Company, will be responsible for compliance with the Privacy & Security Rule.

The American Airlines Privacy Policy for Employees (“AA Privacy Policy”) provides a global overview of how and why the Company may use employees’ “personal information,” which is information that the Company collects and maintains as a part of an employee’s employment with the Company. In the event of a conflict between this Policy and the AA Privacy Policy, this Policy will control with respect to PHI held by a HIPAA-covered health plan.

Unless otherwise defined herein, the meaning of all terms in this Policy will be consistent with the meanings of these terms in the Privacy & Security Rule.

Any member of a Plan’s workforce who interacts with individually identifiable health information covered under the Privacy & Security Rule (the “Workforce”) must comply with the regulations and this Policy. The Plan also will require any contractors or third parties who act on the Plan’s behalf and who disclose individually identifiable health information covered by the regulations to comply with the Privacy & Security Rule.

The Plan may update this Policy at any time without notice.

**I. ORGANIZED HEALTH CARE ARRANGEMENT**

- The Plan will be considered an organized health care arrangement (“OHCA”) under 45 CFR § 164.501. An organized health care arrangement is made up of health plans that have the same plan sponsor.
- As an OHCA, the Plan will issue a joint notice for all benefits under the Plan.
- The benefits and plans making up the OHCA may disclose PHI to each other for health care operations functions of the OHCA plans.

## **II. PRIVACY & SECURITY OFFICER**

- The Plan has appointed a Privacy Officer who is responsible for developing and implementing the procedures relating to privacy of PHI, including but not limited to this Policy.
- The Plan has appointed a Security Officer who is responsible for ensuring the Plan's compliance with the HIPAA Security Rule and the Plan's security policies and procedures.
- The Privacy Officer will coordinate the Health Plan's privacy activities with the Plan's Security Officer.
- The Privacy Officer and the Security Officer are listed at Appendix B.
- The Privacy Officer and the Security Officer shall be responsible for establishing and implementing these procedures and shall periodically review these procedures and make revisions as necessary.
- The Privacy Officer and the Security Officer shall be responsible for ensuring that the applicable members of the Workforce are properly trained on this Policy.
- The Privacy Officer has also been appointed by the Plan to serve as the contact person for receiving complaints in accordance with the complaint procedures discussed in this Policy.

### III. PROTECTED HEALTH INFORMATION

For purposes of this Policy, PHI is health information created or received by the Plan that identifies an individual and relates to the individual's past, present or future health, treatment or payment for health care services.

PHI encompasses a broad array of information. For example, it could be a single piece of data that directly identifies an individual or a summary of information that can be used to identify an individual.

For purposes of this Policy, PHI does not include the following information:

- Summary health information, as defined by the Privacy & Security Rule, that is disclosed to the Company solely for purposes of obtaining premium bids, or modifying, amending, or terminating the Plan;
- Enrollment and disenrollment information concerning the Plan that does not include any substantial clinical information; and
- PHI disclosed to the Plan or the Company under a signed authorization that meets the requirements of the Privacy & Security Rule.

The above types of disclosures are subject to the procedures under Section VI.

The Privacy & Security Rule does not apply to "de-identified" information, where the identifiers listed below are removed. If all of these identifiers are not removed, the information will still be considered PHI and subject to the Privacy & Security Rule and this Policy.

- Name
- Geographic subdivisions smaller than a state (including address and zip code). Note that the first three digits of a zip code may be retained if census records indicate that this area would have more than 20,000 people.
- All dates, including birth date or employment date (however, years may be retained). Also, for those age 90 and over, all data must be aggregated.
- Telephone number
- Fax number
- E-mail
- Social Security Number
- Medical Record Number
- Health plan beneficiary number
- Account numbers
- Certificate/license numbers



- Vehicle identifiers and serial numbers, such as license plate number
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, such as finger and voice prints
- Full face photographic and comparable images
- Any other unique identifying number, characteristic, or code.

In addition, the Plan must not have actual knowledge that the information retained can be used alone, or in combination with other information, to identify an individual.

Alternatively, information may be considered de-identified if a person with appropriate knowledge of an experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable applies these methods to determine that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information. The expert must document the method and results of the analysis that justify the determination.

#### **IV. NOTICES OF PRIVACY PRACTICES**

##### Distribution of Notice

- The Plan has prepared and distributed to all Plan participants a Notice of Privacy Practices (“Notice”) describing the Plan’s privacy practices regarding PHI.
- A single Notice has been provided to each of the named enrollees that is effective for all covered dependents.
- Individuals must receive a copy of the Notice at the time of their enrollment in a Plan.

##### Material Changes to the Notice

- If the Notice is materially changed, all Plan participants will be provided with a copy of the Notice as revised within 60 days.

##### Availability of Notice

- The Notice shall be placed on the Plan’s website (if applicable).
- The Notice will also be provided:
  - At the time of an individual’s enrollment in the Plan; and
  - To a person requesting the Notice.
- The Plan will also provide notice of availability of the Notice (or a copy of the Notice) at least once every three years in compliance with the Privacy & Security Rule.

##### Right to Receive a Copy of the Notice

- An individual has the right to receive a paper copy of the Notice.
- All requests for a paper copy of the Notice must be made in writing and forwarded to the Privacy Officer.

##### Content of Notice

- The Plan’s Notice shall comply with the content requirements of 45 CFR § 164.520.
- The Plan will, on a reasonably ongoing basis, determine whether the contents of its Notice are consistent with its practices and uses and disclosures of PHI.

## V. USE OR DISCLOSURE OF PHI / HIPAA AUTHORIZATION

### Use & Disclosure of PHI

The Plan only will use or disclose PHI in the following circumstances:

- If the disclosure is to the individual involved or their personal representative.
- If the use or disclosure is for the purposes of treatment, payment, or health care operations, as defined in the Privacy & Security Rule.
- If the use or disclosure is permitted under an exception listed in the Privacy & Security Rule, such as disclosures with respect to law enforcement, pursuant to a subpoena, or where required by law.
- To the Company for plan administrative functions or as otherwise permitted under the Privacy & Security Rule.
- To a family member or other individual involved in the individual's care or payment for care, as permitted under the Privacy & Security Rule.
- If the use or disclosure is pursuant to a valid Authorization.

### Authorization

- PHI should not be used or disclosed on the basis of an Authorization, unless it is verified that the Authorization:
  - Has not expired;
  - Has not been revoked; and
  - Includes all required information.
- The Authorization must contain the following:
  - Information to be Disclosed
  - Persons Making Disclosure
  - Persons to Whom Disclosure is to be Made
  - Purpose of Disclosure
  - Right to Revoke Authorization
  - Whether Plan Can Condition Benefits Upon Providing Authorization
  - Potential for Rediscovery

- Remuneration /Marketing (if use or disclosure will result in direct or indirect remuneration to plan from a third party, such as for marketing)
- Expiration
- Signature (or signature of Personal Representative)

See Appendix D for a copy of the Plan's template HIPAA Authorization Form.

- Revocation of Authorization
  - Individuals may revoke an Authorization at any time. Note that the revocation will not apply to disclosures where the Plan already has relied on the Authorization.
  - The individual must contact the party to whom the Authorization applies in order to revoke the authorization.

#### Genetic Information

- The Plan will not use or disclose PHI that is genetic information for underwriting purposes in accordance with 45 CFR § 164.502(a)(5)(i). Underwriting purposes includes, but is not limited to, determinations of eligibility, or determinations of benefits under the Plan, the computation of premium, the application of any pre-existing condition exclusion under the Plan and other activities related to the creation, renewal or replacement of a contract of health insurance.

#### Claims Assistance

- Where an individual has asked the Plan or the Company to act on his or her behalf in interacting with a business associate or another third party, the Plan shall follow the procedures in the Claims Assistance section.

#### Marketing & Sale of PHI

- The Plan will obtain authorization prior to disclosing PHI for any marketing activities or related to the sale of PHI, where required under the Privacy & Security Rules.

## **VI. DISCLOSURE TO THE COMPANY**

- The Plan may disclose to the Company information on whether an individual is participating in the Plan, or is enrolled in or has disenrolled from a health plan option, a health insurance issuer, or an HMO offered by the Plan.
- The Plan may disclose summary health information to the Company to obtain premium bids for providing health insurance coverage or to modify, amend or terminate the Plan. Summary health information is individually identifiable health information from which individual identifiers have been deleted, except for a five-digit zip code.
- The Plan may disclose de-identified information that meets the standards for de-identification set out in Section III.
- Other than above, the Plan only will disclose PHI to the Company for plan administration functions or as otherwise permitted under the Privacy & Security Rules.
- The Plan may not disclose PHI to the Company for employment-related actions or in connection with any other non-HIPAA-covered benefit or employee benefit plan of the Company.
- The plan document that governs the Plan shall include provisions to describe the permitted and required uses by, and disclosures to, the Company of PHI for plan administrative or other permitted purposes. Specifically, the Plan document shall require the Company to:
  - Not use or further disclose PHI other than as permitted or required by the Plan documents or as required by law;
  - Ensure that any subcontractors or agents to whom it provides PHI agree to the same restrictions and conditions that apply to the Company;
  - Not use or disclose the PHI for employment-related actions or in connection with any other benefit or employee benefit plan of the Company;
  - Report to the Plan any use or disclosure of which the Company becomes aware that is inconsistent with the Plan documents or the Privacy & Security Rule;
  - Make PHI accessible to individuals in accordance with the Privacy & Security Rule;
  - Allow individuals to amend their information in accordance with the Privacy & Security Rule;
  - Provide an accounting of its disclosures in accordance with the Privacy & Security Rule;
  - Make the Company's internal practices and records relating to the use and disclosure of PHI received from the Plan available to the Department of Health & Human Services ("HHS") upon request;
  - Return and destroy all PHI when no longer needed, if feasible; and

- Ensure that adequate separation exists between the Company's Plan administration activities and all other activities.

The Plan document must require the Company to certify that its Plan documents have been amended to include the above restrictions and that the Company agrees to those restrictions.

## VII. DISCLOSURE TO FAMILY MEMBERS OR PERSONAL REPRESENTATIVES

- The Plan will treat a “personal representative,” as described below, the same as an individual covered under the Plan. The personal representative will have the same rights as the individual with respect to his or her PHI, including the right to provide authorization and the individual rights described in this Policy above.
- If a person has authority under applicable law to act on behalf of an individual in making decisions related to health care, the Plan will treat that person as a personal representative.
- Where an individual is exercising a right related to PHI held by a business associate, the Plan will direct the individual to contact the business associate to verify the person’s status as a personal representative.
- Where an individual is exercising a right related to PHI held by the Company or the Plan, the Plan will obtain documentation verifying a person’s status as a personal representative before making any disclosures to the personal representative. The Plan shall follow the procedures below.
- Upon proper documentation, and consistent with the Privacy & Security Rule and other applicable law, the Plan generally will treat the following persons as personal representatives (note that this list provides examples of persons who will be considered personal representatives and is not exhaustive).

<b>Participant</b>	<b>Person requesting PHI</b>	<b>Personal representative?</b>
Minor child	Parent or guardian	Yes, but must provide proof of relationship.
Adult child	Parent or guardian	Yes, but only upon proof of legal authority (e.g., court order) or voluntary agreement (e.g., power of attorney).
Adult	Spouse or other adult	Yes, but only upon proof of legal authority (e.g., court order) or voluntary agreement (e.g., power of attorney).
Deceased	Executor or Administrator	Yes, but only upon proof of legal authority (e.g., provisions of a will or court documents of executor/executrix appointment).
Family Member or Other Party involved in the Participant’s care	Family Member or Close Party	Yes, but limited disclosure and only with approval of the Privacy Officer. The Plan may disclose PHI to an individual’s family member or other party who is assisting in care or payment of care upon proof of the relationship or intent of individual to involve the third party if certain conditions are met. Only information directly

<b>Participant</b>	<b>Person requesting PHI</b>	<b>Personal representative?</b>
		relevant to that person's involvement may be disclosed. Contact the Privacy Officer.



## **VIII. MINIMUM NECESSARY STANDARD**

- The Plan will use or disclose PHI only to the minimum amount necessary to accomplish the intended purpose. This standard applies both to the Plan's requests for PHI from other covered entities, as well as requests for PHI made to the Plan.
- In accordance with this minimum necessary standard, the Plan will not use, disclose or request an individual's entire medical record unless the use, disclosure or request is specifically justified.
- The minimum necessary standard does not apply to disclosures to a health care provider for treatment; disclosures to the individual; disclosures pursuant to a valid Authorization; disclosures to the Secretary of HHS; or disclosures required by law or required to comply with the Privacy & Security Rule.
- In accordance with this minimum necessary standard, the Plan has identified the members of the Workforce as the only persons who need access to PHI to carry out their duties.

**IX. PROTECTION OF PHI**

- The Plan will develop and implement administrative, technical, and physical safeguards that will reasonably protect PHI, including electronic PHI, from intentional and unintentional uses or disclosures that violate the Privacy & Security Rule.
- The Plan will institute procedures to verify the identity of any person or entity requesting PHI and the authority of that person or entity to have access to PHI.
- Such safeguards shall include, where appropriate and feasible:

	<b>Protection Procedures</b>
Printed/ hard copy documentation	<p>Limit the number of photocopies made of PHI.</p> <p>Implement a “clean desk” practice. PHI should be put away if the employee is away from his or her desk throughout the day and PHI will be placed in closed and locked drawers or cabinets when the employee is not in the office.</p> <p>PHI in paper format should be destroyed when it is obsolete or is not required to be retained for storage purposes, with shredding the preferred method of destruction.</p> <p>Copies printed to a common printer should be retrieved expeditiously.</p> <p>“Lock” files after hours or when leave desk (whether physical or computer).</p>

	<b>Protection Procedures</b>
E-mail and electronic storage	<p>Destroy electronic PHI that is no longer needed.</p> <p>Limit the use of PHI in e-mails to the Minimum Necessary (e.g., refrain from forwarding strings of e-mail messages containing PHI. Instead, prepare a new message, with only the Minimum Necessary information).</p> <p>Encrypt e-mail information as needed.</p> <p>Use “locking” screensavers to limit access.</p> <p>Maintain and periodically update network monitoring software, including intrusion detection and reporting.</p> <p>Maintain and periodically update systems for backing up data and contingency plans for data recovery in the event of a disaster.</p> <p>Maintain and periodically review procedures for ending data access for staff (e.g., after they terminate employment).</p> <p>Follow company IT guidelines regarding electronic data.</p> <p>Limit remote access to systems to secure methods.</p>
Facsimiles	<p>Areas receiving PHI by fax should take reasonable measures to ensure the privacy of the faxed PHI, including notifying parties sending PHI of the proper fax number to which the information may be sent.</p> <p>When PHI is faxed, a cover sheet marked “Confidential” and addressed to the party authorized to receive the PHI should be used.</p>
Oral conversations / Telephone	<p>Limit the content of PHI in conversations (e.g., with vendors and other staff) to the Minimum Necessary.</p> <p>Verify the identity of individuals on the phone (such as by asking for ID number).</p> <p>Never leave PHI on a voicemail message.</p>
PHI mailed externally	<p>Mail containing PHI will be addressed to an authorized party. Reasonable efforts should be made to ensure the party to whom mail is directed is authorized to receive PHI.</p> <p>The sender’s return address should be displayed so that the mail containing the PHI may be returned to the sender, if needed.</p>

	<b>Protection Procedures</b>
PHI sent internally	<p>PHI sent through the internal mail routing system should be placed in an inter-office envelope and sealed with “Confidential” marked on the envelope. The recipient’s name should be clearly marked on the envelope.</p> <p>Misdirected mail should be routed to the appropriate party using the same procedure as noted in the previous sentence.</p>

**X. CLAIMS ASSISTANCE**

- If an individual contacts a representative of the Benefits Department with a question about a claim for benefits, the Benefits Department representative may discuss the individual's PHI with an insurer, TPA, or business associate provided the Benefits Department employee has been trained as a member of the Plan's Workforce.
- The Benefits Department employee may not disclose any PHI to an individual or entity that is not (i) a member of the Workforce or (ii) the Plan's insurer, TPA or business associate.
- The Benefits Department employee should keep this information confidential and not use it for any function on behalf of the Company (other than assisting the individual with his or her claim).

## **XI. PARTICIPANT'S RIGHT TO ACCESS PHI**

### Participant's Right

- A participant has the right to access, inspect, and copy his or her PHI within a Designated Record Set for as long as the PHI is maintained in the Designated Record Set. The Plan will provide the information in the format requested where "readily producible" and may charge any applicable cost-based fee, as permitted under the Privacy & Security Rule.
- A Designated Record Set is a group of records that the Plan maintains for enrollment, payment, claims adjudication, case management or medical management, or that the Plan uses, in whole or in part, to make decisions about participants.

### Deadline to Respond

- The Plan must respond to a participant's request within thirty (30) days of the receipt of the request.
- If the Plan is unable to respond within this timeframe, this time may be extended for thirty (30) days.

### PHI Held by Business Associate / Insurer

- All requests to inspect or obtain copies of PHI under 45 CFR § 164.524 should be directed to the applicable business associate or insurer.

### PHI Held by the Company

- Requests to inspect or obtain copies of PHI held by the Company should be directed to the Privacy Officer.

### Retention

- A copy of all written requests for access and responses must be maintained for six years.

## **XII. PARTICIPANT'S RIGHT TO AMEND PHI**

### Participant's Right

- A participant has the right to request that the Plan amend his or her PHI held in a Designated Record Set. The Plan must generally honor these rights, except in certain circumstances. When a Plan amends PHI, it must communicate the Amendment to other persons to whom it has disclosed the PHI.
- A Designated Record Set is a group of records that the Plan maintain for enrollment, payment, claims adjudication, case management or medical management, or that the Plan uses, in whole or in part, to make decisions about participants.

### Deadline to Respond

- The Plan must respond to a participant's request within sixty (60) days of the receipt of the request.
- If the Plan is unable to respond within this timeframe, this time may be extended for thirty (30) days.

### PHI Held by Business Associate / Insurer

- All requests to amend PHI under 45 CFR § 164.526 should be directed to the applicable business associate or insurer.

### PHI Held by the Company

- Requests to amend PHI held by the Company should be directed to the Privacy Officer.

### Retention

- A copy of all written requests for amendment, responses, written statements of disagreement and rebuttals must be maintained for six years.

### **XIII. PARTICIPANT'S RIGHT TO ACCOUNTING OF DISCLOSURES**

#### Participant's Right

- A participant has the right to request an accounting of certain disclosures of PHI by the Plan for the six years prior to the request.
- The accounting rule does not apply to:
  - PHI disclosed for treatment, payment, or health care operations of the Plan;
  - PHI disclosed to the individual who is the subject of the PHI, or their personal representative;
  - PHI disclosed incident to a use or disclosure otherwise permitted or required by the Privacy & Security Rule;
  - PHI disclosed pursuant to an authorization;
  - PHI disclosed to persons involved in the individual's care or payment for the individual's care or for certain other notification purposes;
  - PHI disclosed for a facility directory, as permitted under the Privacy & Security Rule;
  - PHI disclosed for national security or intelligence purposes under the Privacy & Security Rule, 45 CFR § 164.512(k)(2);
  - PHI disclosed to correctional institutions or law enforcement officials under the Privacy & Security Rule, 45 CFR § 164.512(k)(5);
  - PHI disclosed before April 14, 2003; and
  - PHI disclosed under a limited data set.

#### Deadline to Respond

- The Plan must respond to a Participant's request within sixty (60) days of the receipt of the request.
- If the Plan is unable to respond within this timeframe, this time may be extended for thirty (30) days.

#### PHI Disclosures by Business Associate / Insurer

- All requests for accountings of PHI disclosed by the Plan's business associate, such as third party administrator, or an insurer should be directed to the applicable business associate or insurer.
- All other requests for accountings of PHI disclosed by the Plan should be directed to the Privacy Officer.



### PHI Held by the Company

- Requests for an accounting of PHI disclosed by the Company should be directed to the Privacy Officer.

### Disclosure Log

- The Plan will maintain a log of any uses and disclosures of PHI in its paper and electronic systems, consistent with the Privacy & Security Rule.
- The accounting must include the following information for each disclosure:
  - the date of the disclosure;
  - the name of the entity or person who received the PHI and the address, if known;
  - a brief description of the PHI; and
  - a brief statement of the disclosure purpose, or a copy of the individual's written authorization or disclosure request.
- The Plan will document the written accounting that is provided to the individual and maintain this documentation for six years.
- The first accounting requested by an individual in any 12-month period is free. For additional lists, a Plan may charge its reasonable costs of providing an accounting. The Plan must first provide advance notice of the fee that will be charged and allow the individual the right to withdraw or modify his or her request to reduce the charges before any costs are incurred.

### Retention

- A copy of all written requests for accounting and responses must be maintained for six years.

#### **XIV. PARTICIPANT'S RIGHT TO REQUEST RESTRICTIONS ON PHI**

##### Participant's Right

- An individual has the right to request that the Plan restrict the use and disclosure of his or her PHI for treatment, payment or health care operations, or to individuals involved in his or her care or payment for care. The Plan is generally not required to agree to a restriction, but it must abide by an agreed to restriction except in certain circumstances.
- If a participant has paid out of pocket in full for services, the participant's provider may be required to comply with a request to restrict use or disclosure of PHI related to such service.
- All requests for restrictions must be made in writing to the Privacy Officer.

##### PHI Held by Business Associate / Insurer

- All requests to restrict PHI under 45 CFR § 164.522(a) should be directed to the applicable business associate or issuer.

##### PHI Held by the Company

- Requests to restrict PHI held by the Company should be directed to the Privacy Officer.

##### Record Retention

- A copy of all requests for restrictions and responses must be maintained for six years.

## **XV. PARTICIPANT'S RIGHT TO REQUEST CONFIDENTIAL COMMUNICATIONS**

- An individual has the right to request that a Plan communicate with him or her in a certain way or at a certain location.
- A Plan must honor reasonable requests if the individual clearly states that the disclosure of PHI by the usual means could endanger the individual.
- All requests for confidential communications must be made in writing to the Privacy Officer.

### PHI Held by Business Associate/Insurer

- Where appropriate, requests to request confidential communications of PHI under 45 CFR § 164.522(b) should be directed to the applicable business associate/insurer.

### PHI Held by the Company

- If any communications of PHI are made by the Workforce on behalf of the Plan or the Company, such information is subject to the right to request the confidential communications requirements listed in 45 CFR § 164.522(b).

### Record Retention

- A copy of all requests for confidential communications and responses must be maintained for six years.

## **XVI. TRAINING**

### Initial Training

- The Plan provides ongoing training on the Privacy & Security Rule and this Policy to all members of the Workforce who perform administration functions for the Plan.
- The Privacy Officer is charged with developing training schedules and programs so that all members of the Workforce receive the necessary and appropriate training to permit them to carry out their Plan functions in compliance with the Privacy & Security Rule.
- Workforce training will be updated as necessary to reflect any changes in policies or procedures and to ensure that workforce members are appropriately aware of their obligations.
- Records of this training will be maintained for six years.

### Newly Hired Employees

- Newly hired employees who will interact with PHI from the Plan must receive privacy training appropriate to their involvement with PHI within a reasonable time from the date of hire.
- Newly hired employees who receive training must be recorded on a certification, which must be maintained for six years.

### Ongoing Training

- The Privacy and Security Officer shall be responsible for identifying material changes in this Policy that would necessitate additional or “refresher” training.
- The Privacy and Security Officer shall identify any members of the Workforce who should undergo additional training.
- Members of the Workforce who receive additional training must be recorded on a certification, which must be maintained for six years.

## **XVII. DISCIPLINE FOR VIOLATIONS**

The Privacy Officer and the Security Officer is responsible for addressing all violations of the Privacy & Security Rule or this Policy. The Privacy Officer and the Security Officer shall document the facts of the violation, actions that have been taken to discipline the offending party and the steps taken to prevent future violations. Such records shall be kept for six years.

### Sanctions

- If the Privacy Officer and the Security Officer determines that any member of the Workforce has acted in noncompliance with the Privacy & Security Rule or this Policy, then the Privacy Officer shall take or seek to have taken appropriate disciplinary action with respect to that person, up to and including termination of employment.
- Violations will be dealt with according to the seriousness of the offense.

### Mitigation

- A Plan will mitigate any harmful effects of known violations of the Privacy & Security Rule or of this Policy.
- Mitigation may include informing the person whose PHI has been disclosed, if appropriate.

### Complaints

- The Plan will establish procedures for individuals to make complaints concerning the Plan's privacy procedures.
- In order to file a complaint, an individual must complete a complaint form ("HIPAA Complaint Form") and file the form with the Plan's Privacy Officer. See Attachment C for a template of the HIPAA Complaint Form.
- The Privacy Officer will investigate all complaints within an appropriate time period and respond to the reporting party as appropriate regarding the status of the investigation and any corrective action taken.
- Members of the Workforce are required to cooperate in any investigation by the Privacy Officer.
- The Privacy Officer shall take reasonable corrective steps to respond appropriately to any privacy breach detected or reported and to prevent future similar offenses.
- The Plan will retain a record of all complaints submitted to the Plan and their resolutions for six years.

## XVIII. SECURITY BREACH NOTIFICATION

### Security Breach Rules

- Any suspected or potential breaches of PHI or violations of the Privacy & Security Rule must be reported to a Privacy Officer immediately.
- The Privacy Officer will conduct a risk assessment to determine if the potential breach should be considered a “breach” for purposes of the HITECH Act requirements. This risk assessment will include an evaluation of:
  - Whether the data was unsecured PHI,
  - Whether the information was used or disclosed in an unauthorized manner; and
  - For potential breaches **prior** to 9/23/13, whether the use or disclosure poses a significant risk of financial, reputational, or other harm to the individual.
  - For potential breaches **on or after** 9/23/13, the probability that the PHI has been compromised under the factors set out in guidance issued by HHS.
    - HHS has outlined certain exceptions whereby a non-permitted disclosure will not be considered a “breach” under HIPAA:

<b>Exception</b>
<p><b>Secure PHI</b></p> <p>PHI was encrypted or destroyed under HHS standards (may need additional information).</p>
<p><b>Unintentional Access by Covered Entity / Business Associate Employee</b></p> <p>Access must be in good faith, within employee’s course and scope of employment, and not result in further use or disclosure (e.g., nurse sends record to hospital billing employee, who opens in normal course of business, realizes mistake, deletes email, and notifies nurse).</p>
<p><b>Inadvertent Disclosure from One Employee to Another Similarly Situated Employee at Same Covered Entity/Business Associate</b></p> <p>Where both employees authorized to access information and information not further used (e.g., doctor providing PHI to nurse who would otherwise be authorized to see, even if not in this instance).</p>
<p><b>Recipient Not Reasonably Able to Retain Information</b></p> <p>For example, information returned in unopened envelope, immediately taking back papers given in error.</p>

- If an exception doesn't apply, the Plan must consider the following factors:

<b>Factor</b>
<p><b>1. Nature and extent of PHI Involved</b></p> <p>Preamble says covered entity should consider whether information disclosed was more "sensitive" in nature, such as financial or clinical information and whether information could be used by unauthorized recipient in manner adverse to individual.</p>
<p><b>2. Unauthorized person who used PHI or to whom disclosure made</b></p> <p>Preamble says covered entity should consider whether person receive PHI also has an obligation to protect the information or has the ability to identify individuals involved (i.e., if the recipient may know these individuals). Preamble also says covered entity may take into account whether PHI was disclosed internally or outside organization.</p>
<p><b>3. Whether PHI actually acquired or viewed</b></p> <p>Preamble gives example of being able to determine that information on recovered laptop was not accessed or returned envelope was unopened.</p>
<p><b>4. Extent to which risk has been mitigated</b></p> <p>Preamble gives examples of obtaining recipient's assurance that information will not be further used or disclosed or will be destroyed</p>

#### Notification of Individual

- If there is a breach, the Plan must notify the individual without unreasonable delay, but no later than 60 days after discovery of the breach.
- The breach will be considered discovered on the first day it is known to any member of the Workforce (other than the person who committed the breach), or the date it would have been known if the Plan exercised reasonable diligence.
- The notice must be written in plain language and contain:
  - A brief description of what happened, including the date of the breach and date of discovery;
  - The types of PHI involved (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
  - Any steps individuals should take to protect themselves from potential harm;
  - A brief description of steps the Plan is taking to investigate, mitigate losses, and protect against further breaches; and

- Contact information for individuals to ask questions, including a toll-free telephone number, email address, website, or postal address.

#### Notification of Media

- The Plan must notify the media where the breach involves more than 500 residents in a state.
- The Plan also may need to notify the media if insufficient or out-of-date contact information precludes individual notice.

#### Notification to HHS

- Where a breach involves 500 or more people, the Plan must notify the Secretary of HHS immediately.
- Where a breach involves fewer than 500 people, the Plan must maintain a log of security breaches and submit it to HHS on an annual basis by March 1<sup>st</sup> for breaches from the prior year.



## **XIX BUSINESS ASSOCIATE AGREEMENTS**

### Business Associate Contract

- The Plan will enter into any necessary contracts with its business associates, in accordance with 45 CFR § 164.505(c). A business associate is any party acting on behalf or for the Plan in a function involving PHI.
- For an approved sample business associate contract, contact the Privacy & Security Officer.

### Disclosures to Business Associates

- The Plan will comply with the Minimum Necessary Standard to ensure only the minimum necessary information is disclosed to business associates.
- The Plan only may disclose PHI for the purposes of treatment, payment, or health care operations, or under another exception in the Privacy & Security Rule, except where authorization has been obtained.
- If the Plan become aware of a pattern of activity or practice that constitutes a material breach of the business associate contract, the Plan will take reasonable steps to have the business associate end the violation, or if unsuccessful, will terminate the business associate contract.

**APPENDIX A - PRIVACY OFFICER AND SECURITY OFFICER**

The Privacy Officer and Security Officer for the Plan is:

Jennifer Stojak

Messages to the Privacy Officer and/or Security Officer may be sent to:

HIPAA Privacy & Security Officer  
C/O Bobbie Davies  
American Airlines, Inc.  
4333 Amon Carter Boulevard  
Mail Drop 5123  
Fort Worth, Texas 76155

## **APPENDIX B - APPLICABLE HEALTH PLANS**

This Policy applies to the following plans. This list may be updated from time to time:

- American Airlines, Inc. Health & Welfare Plan for Active Employees
- Supplemental Medical Plan for Employees of Participating American Airlines Group Subsidiaries
- American Airlines, Inc. Health and Life Plan for Retirees
- TWA Retiree Health and Life Benefit Plan
- American Airlines, Inc. Health Benefit Plan for Certain Legacy Employees
- American Airlines Inc. Flexible Benefit Plan for Certain Legacy Employees

**APPENDIX C – HIPAA COMPLAINT FORM**

---

See following page

**AMERICAN AIRLINES, INC. HIPAA COMPLAINT FORM**

The Health Insurance Portability and Accountability Act of 1996, as amended, (“HIPAA”) requires health plans to provide individuals an opportunity to file a complaint regarding suspected privacy and security violations. The health plans sponsored by American Airlines, Inc. (the “Plans”) allow covered individuals to file a complaint with the Plans’ HIPAA Privacy Officer. To file a complaint with the HIPAA Privacy Officer, please complete, date, and sign this form. The HIPAA Privacy Officer will review your complaint and may contact you for more information.

Please use the space below to describe the nature and source of the alleged violation of the HIPAA privacy and security rules. Be specific and provide as much information as you can—please attach additional pages if necessary. Your complaint should include any and all information that you believe pertains to your case.

---

---

---

---

---

---

---

---

---

---

**PLEASE PROVIDE THE FOLLOWING INFORMATION**

NAME: \_\_\_\_\_ PHONE NUMBER: \_\_\_\_\_

EMAIL ADDRESS: \_\_\_\_\_ EMPLOYEE ID NUMBER: \_\_\_\_\_

HEALTH INSURANCE MEMBER NUMBER: \_\_\_\_\_

(Please include the number on the front of your ID card)

SIGNATURE: \_\_\_\_\_

Mail a completed form to the address below:

HIPAA Privacy & Security Officer  
C/O Bobbie Davies  
American Airlines, Inc.  
4333 Amon Carter Boulevard  
Mail Drop 5123  
Fort Worth, Texas 76155

**APPENDIX D – HIPAA AUTHORIZATION FORM**

---

See following page

**Authorization for Release of Protected Health Information**

**Instructions:** You must complete all the information below. If incomplete, this authorization form will be returned to you. If you have any questions or need assistance completing this form, please use Chat in the American Airlines Benefits Service Center or call 888-860-6178.

**Purpose:** I authorize the American Airlines Health & Welfare Plan for Active Employees (the "Plan") to disclose the information listed below to the authorized person(s) named below.

---

**Section A:** Employee Information

Employee Name: \_\_\_\_\_ Employee Number: \_\_\_\_\_  
First and Last Name

---

**Section B:** Release of Protected Health Information ("PHI")

Name of person whose PHI is being released: \_\_\_\_\_

Member ID Number of person whose PHI is being released (from the front of the insurance card):  
\_\_\_\_\_

Address: \_\_\_\_\_  
\_\_\_\_\_

Telephone Number: \_\_\_\_\_

Purpose of Disclosure: Check one box

At my request

Other (e.g., respond to inquiries regarding my health benefits, appeal assistance):  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

---

**Section C:** Recipient of Protected Health Information

Name of person or organization allowed to receive PHI \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

---

---

**Section D: Acknowledgment, Authorization and Signature**

I understand that:

- I have the right to revoke this authorization at any time for future disclosures the American Airlines Health & Welfare Plan for Active Employees (the "Plan") may make, unless the Plan has taken action in reliance upon this authorization. I must revoke this authorization in writing directly to the American Airlines Benefits Service Center at the address provided below.
- The Plan may not condition my treatment, payment, enrollment, or eligibility for benefits upon whether I sign this authorization.
- Once my information has been disclosed, as permitted under this authorization, it may no longer be protected under the federal privacy regulations of the Health Insurance Portability and Accountability Act ("HIPAA"), so there is a possibility that the party to whom my information is being disclosed may re-disclose the information.

Unless revoked, this authorization is valid from the date of my signature until the date I am no longer covered by the Plan or until I revoke this authorization.

I authorize the use or disclosure of the PHI as indicated above:

Signature: \_\_\_\_\_

Date Signed: \_\_\_\_\_

If you are a personal representative, such as a Legal Guardian or agent acting under a Power of Attorney, you may be able to sign on behalf of the Member if the supporting paperwork has the required regulatory language. Complete the following and attach documentation (if applicable) supporting such personal representation and the Privacy Officer, or her designee, will determine whether it is sufficient to grant authorization.

Personal Representative's Name: \_\_\_\_\_

Relationship to Member or Authority to act as Personal Representative: \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_

Please keep a copy of this document for your records and mail the completed Authorization to:

American Airlines Benefits Service Center  
P.O. Box 564103  
Charlotte, NC 28256-4103