HIPAA PRIVACY & SECURITY

POLICIES & PROCEDURES

FOR HEALTH PLANS SPONSORED BY

AMERICAN AIRLINES, INC.

Table of Contents

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 A.

- 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 HEATH 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 Redisclosure
    - 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).

Participant	**Person requesting PHI**	**Personal representative?**
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

Participant	Person requesting PHI	Personal representative?
		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:

	Protection Procedures
Printed/ hard copy documentation	Limit the number of photocopies made of PHI. 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. 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. Copies printed to a common printer should be retrieved expeditiously. "Lock" files after hours or when leave desk (whether physical or computer).

	Protection Procedures
E-mail and electronic storage	Destroy electronic PHI that is no longer needed. 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). Encrypt e-mail information as needed. Use "locking" screensavers to limit access. Maintain and periodically update network monitoring software, including intrusion detection and reporting. Maintain and periodically update systems for backing up data and contingency plans for data recovery in the event of a disaster. Maintain and periodically review procedures for ending data access for staff (e.g., after they terminate employment). Follow company IT guidelines regarding electronic data. Limit remote access to systems to secure methods.
Facsimiles	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. When PHI is faxed, a cover sheet marked "Confidential" and addressed to the party authorized to receive the PHI should be used.
Oral conversations / Telephone	Limit the content of PHI in conversations (e.g., with vendors and other staff) to the Minimum Necessary. Verify the identity of individuals on the phone (such as by asking for ID number). Never leave PHI on a voicemail message.
PHI mailed externally	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. The sender's return address should be displayed so that the mail containing the PHI may be returned to the sender, if needed.

	Protection Procedures
PHI sent internally	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. Misdirected mail should be routed to the appropriate party using the same procedure as noted in the previous sentence.

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:

Exception
Secure PHI PHI was encrypted or destroyed under HHS standards (may need additional information).
Unintentional Access by Covered Entity / Business Associate Employee 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).
Inadvertent Disclosure from One Employee to Another Similarly Situated Employee at Same Covered Entity/Business Associate 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).
Recipient Not Reasonably Able to Retain Information For example, information returned in unopened envelope, immediately taking back papers given in error.

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

Factor
1. Nature and extent of PHI Involved 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 I manner adverse to individual.
2. Unauthorized person who used PHI or to whom disclosure made 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.
3. Whether PHI actually acquired or viewed Preamble gives example of being able to determine that information on recovered laptop was not accessed or returned envelope was unopened.
4. Extent to which risk has been mitigated Preamble gives examples of obtaining recipient's assurance that information will not be further used or disclosed or will be destroyed

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 1st 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 for the Plan is:

Jennifer Stojak

Phone: 817-931-2390

jennifer.stojak@aa.com

The Security Officer for the Plan is:

Shawn Irving

Phone: 214-403-1100

Shawn.Irving@aa.com

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

APPENDIX C –

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: _____

Please submit the form to the HIPAA Privacy Officer.

APPENDIX D

HIPAA AUTHORIZATION FORM

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 not 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

APPENDIX E – SECURITY RISK ASSESSMENT

Overall Checklist:

- ❒ Risk Assessment
- ❒ Appoint Security Official
- ❒ Training
- ❒ Amend Business Associate Agreement
- ❒ Amend Plan Document (if applicable)
- ❒ New Procedures
- ❒ Documentation

Factors to Determine Security Measures (as listed in regulations):

- ❒ Size, complexity, and capabilities of Covered Entity;
- ❒ Covered Entity's technical infrastructure, hardware, and software capabilities;
- ❒ Costs of security measures; and
- ❒ Probability and criticality of potential risks to EPHI.

ADMINISTRATIVE SAFEGUARDS

	STANDARD	IMPLEMENTATION SPECIFICATION	DESCRIPTION / EXAMPLES	PLAN PROCEDURE
(1)	**Security Management Process** – Procedures to prevent, detect contain, and correct security violations.	Risk Analysis **(REQUIRED)**	Assess potential risks and vulnerabilities to confidentiality, integrity, and availability of EPHI.	**Vulnerability Management** The Vulnerability Management Policy and Standard are focused on identifying, assessing, and addressing vulnerabilities within the systems. They help ensure that any risks, like unauthorized access or system tampering, are mitigated. Regular vulnerability scans and penetration tests are conducted to catch weaknesses before they can be exploited. *(Referenced from: Doc 1 -*

	STANDARD	IMPLEMENTATION SPECIFICATION	DESCRIPTION / EXAMPLES	PLAN PROCEDURE
				Vulnerability Management Policy and Doc 3 - Vulnerability Management Standard) **Cybersecurity Risk Management Program** The Cybersecurity Risk Management Program ensures a structured approach to identifying and mitigating risks to confidentiality, integrity, and availability. For example, risk questionnaires and scoring methods are used to analyze applications and third-party vendors. They assess potential risks like data disclosure (for confidentiality), operational disruptions (for availability), and system vulnerabilities (for integrity). This helps prioritize actions based on the level of risk. *(Referenced from: Doc 8 - Cybersecurity Risk Management Program) Incident Management* **Cyber Incident Response and Incident Management Policy** Outline procedures for handling incidents that could impact PHI. They emphasize quick detection, response, and recovery to minimize the damage from incidents, whether it's a breach of confidentiality or system downtime. Incidents are classified based on severity, and lessons learned from incidents are used to strengthen processes, ensuring future incidents are less likely. *(Referenced from: Doc 30 - Cyber Incident Response*

	STANDARD	IMPLEMENTATION SPECIFICATION	DESCRIPTION / EXAMPLES	PLAN PROCEDURE
				Policy and Doc 38 - Incident Management Policy) **IT Policies and Standards** The IT Policies and Standards, such as the Application Security, Network Security, and Endpoint Security policies, provide the technical controls needed to secure systems that store or process PHI. These policies ensure that the confidentiality, integrity, and availability of PHI are maintained through secure configurations, regular updates, and ongoing monitoring. *(Referenced from: Doc 10 - IT Policies and Standards)*
		Risk Management **(REQUIRED)**	Implement sufficient security measures to reduce risk and vulnerabilities to a reasonable and appropriate level.	**Vulnerability Management Measures** The Vulnerability Management Policy and Standard outline clear actions to manage vulnerabilities effectively. These include regular vulnerability scans, patch management, and penetration testing to identify and resolve issues promptly, which is intended to . ensure that any known vulnerabilities are addressed within specific timelines based on severity (e.g., critical vulnerabilities must be patched within a certain time period, see SLA for reference). This structured approach helps keep risks at a reasonable level by applying timely and appropriate remediation. *(Referenced from: Doc 1 - Vulnerability Management Policy and Doc 3 -*

	STANDARD	IMPLEMENTATION SPECIFICATION	DESCRIPTION / EXAMPLES	PLAN PROCEDURE
				Vulnerability Management Standard) **Risk-Based Security Controls** The Cybersecurity Risk Management Program ensures that risks are treated based on their potential impact. This includes conducting risk assessments to identify high-risk areas and then implementing targeted controls to mitigate those risks. For example, inherent risk scoring helps determine which systems and third-party vendors require additional controls, such as encryption or multi-factor authentication, based on their level of exposure. This risk-based approach ensures that resources are focused where they are needed most, helping to reduce vulnerabilities to an acceptable level. *(Referenced from: Doc 8 - Cybersecurity Risk Management Program)* **Incident Response and Mitigation** The Cyber Incident Response and Incident Management policies are designed to quickly contain and mitigate the impact of incidents. By having predefined processes for identifying, reporting, and resolving incidents, these policies help reduce the potential damage from security breaches or system failures. The policies also mandate lessons learned from past incidents to further refine security measures and prevent reoccurrence, helping maintain

	STANDARD	IMPLEMENTATION SPECIFICATION	DESCRIPTION / EXAMPLES	PLAN PROCEDURE
				an appropriate level of risk. *(Referenced from: Doc 30 - Cyber Incident Response Policy and Doc 38 - Incident Management Policy)*
		Sanction Policy **(REQUIRED)**	Apply appropriate sanctions to workforce members who fail to comply with security policies and procedures.	**Sanctions for Non-Compliance** Workforce members who fail to comply with security policies and procedures will face disciplinary actions, up to and including termination of employment. The severity of the sanction will be determined based on the seriousness of the violation. *(Referenced from: AA HIPAA Policies Revisions FINAL 1-23-2018.DOCX)*
		Information System Activity Review **(REQUIRED)**	Regularly review records of IS activity, such as audit logs, access reports, and security incident tracing reports.	**Security Log Management Policy** The Security Log Management Policy requires that all security-related events, including audit logs and access reports, be generated, tracked, and reviewed systematically. This document mandates logging mechanisms for user activities, authentication attempts, and security incidents. Logs must be reviewed regularly, and any anomalies must be reported to the Incident Response Team. The policy also states that logs must be retained for at least one year, with the last three months available for immediate restoration if needed *(Referenced from: Doc 20 - Security Log Management).* **Security Log Management Standard**

	STANDARD	IMPLEMENTATION SPECIFICATION	DESCRIPTION / EXAMPLES	PLAN PROCEDURE
				The Security Log Management Standard emphasizes the requirement to review security event logs, ensuring continuous monitoring of system activities. The Security Analytics platform plays a key role in log analysis and event detection, enabling real-time monitoring of access reports and incident tracing. The document outlines specific log generation and retention processes, ensuring that logs are reviewed and monitored by independent personnel for potential security threats *(Referenced from: Doc 41 - Security Log Management Standard).* **Access Control Standard** The Access Control Standard mandates that access to systems and data must be regularly reviewed and audited to prevent unauthorized access. This includes reviewing access logs, conducting user access audits, and verifying privileged access rights. The document highlights the need for regular access right reviews, particularly for privileged users, and requires managers to ensure that user access is aligned with job responsibilities *(Referenced from: Doc 34 - Access Control Standard)* **Cyber Incident Response Policy** The Cyber Incident Response Policy outlines a structured approach to tracking incidents through a case management

	STANDARD	IMPLEMENTATION SPECIFICATION	DESCRIPTION / EXAMPLES	PLAN PROCEDURE
				system. This system is used to capture all details related to cybersecurity incidents, including the actions taken to resolve them. The policy mandates that all incidents be documented, tracked, and reviewed to ensure prompt remediation and that post-incident analyses are performed to identify root causes. Lessons learned from severe incidents (SEV 1 and SEV 2) must be documented and retained to prevent future occurrences *(Referenced from: Doc 30 - Cyber Incident Response Policy)*
(3)	**Workforce Security** – Procedures to ensure employees have appropriate access to EPHI, and to prevent those without access from obtaining access.	Authorization and/or Supervision **(ADDRESSABLE)**	Authorize or supervise workforce members who work with EPHI.	**Authorization and Supervision of Workforce Members** Workforce members who work with electronic protected health information (EPHI) must be authorized and supervised by the Privacy Officer and Security Officer. These officers are responsible for ensuring that only properly trained and authorized personnel have access to EPHI, in compliance with the Plan's privacy and security policies. *(Referenced from: Doc 50 - AA HIPAA Policies Revisions FINAL 1-23-2018)*
		Workforce Clearance Procedure **(ADDRESSABLE)**	Determine whether workforce members' access to EPHI is appropriate.	**Appropriateness of Workforce Members' Access to EPHI** The Privacy Officer and Security Officer are responsible for ensuring that workforce members have appropriate access to EPHI based on their job functions.

	STANDARD	IMPLEMENTATION SPECIFICATION	DESCRIPTION / EXAMPLES	PLAN PROCEDURE
				Access is granted according to the minimum necessary standard, ensuring that employees only access the information required to perform their duties. *(Referenced from: Doc 50 - AA HIPAA Policies Revisions FINAL 1-23-2018)*
		Termination Procedures **(ADDRESSABLE)**	Terminate access to EPHI when employment ends or where access is determined not be appropriate.	**Termination of Access to EPHI** When employment ends or when access is no longer appropriate, the Privacy Officer and Security Officer are responsible for terminating a workforce member's access to EPHI. This process includes deactivating login credentials and ensuring no further access to systems containing sensitive information. *(Referenced from: Doc 50 - AA HIPAA Policies Revisions FINAL 1-23-2018)*
(4)	**Information Access Management** – Procedures to authorize access to EPHI consistent with Privacy rules.	Isolating Health Care Clearinghouse **(REQUIRED)**	If clearinghouse is part of larger organization, must have procedures to protect EPHI from unauthorized access by larger organization.	The plan does not contract with a clearinghouse and does not have a Clearinghouse as part of the org.
		Access Authorization **(ADDRESSABLE)**	Procedures for granting access to workstations, transaction, program, or process.	**Access Control Standard** Procedures for granting access to workstations, transactional systems, programs, or processes are defined by the Business Unit and System Owner. These procedures ensure that access is granted based on job function and responsibilities, and that users only have access to necessary resources. *(Referenced from:*

	STANDARD	IMPLEMENTATION SPECIFICATION	DESCRIPTION / EXAMPLES	PLAN PROCEDURE
				Doc 34 - Access Control Standard). **Identity Management Standard** Roles & responsibilities for user account management including creation, modification, review, and deletion are clearly defined. This includes managers being responsible for reviewing and approving User access aligned with job function and responsibilities. *(Referenced from: Doc 35 - Identity Management Standard).*
		Access Establishment and Modification **(ADDRESSABLE)**	Procedures to establish, document, review and modify a user's right to access to a workstation, transaction , program, or process.	**Access Control Standard** The organization has established procedures for granting access to workstations, transactional systems, programs, or processes *(Referenced from: Doc 34 - Access Control Standard).* **Identity Management Standard** Roles & responsibilities for user account management including creation, modification, review, and deletion are clearly defined. This includes the procedure for establishing, documenting, reviewing, and modifying a User's right to access *(Referenced from: Doc 35 - Identity Management Standard).* **Information Security Policy** The organization has established procedures for granting and revoking access to information systems based

	STANDARD	IMPLEMENTATION SPECIFICATION	DESCRIPTION / EXAMPLES	PLAN PROCEDURE
				on job function and responsibilities, as well as periodic review of user accounts to ensure that all access is still necessary *(Referenced from: Doc 32 - Information Security Policy).*
(5)	**Security Awareness & Training** – Train workforce members.	Security Reminders **(ADDRESSABLE)**	Periodic security updates.	**Cybersecurity Compliance Policy** The organization provides regular Security Awareness Training (SAT) for all Users and third-party vendors that have access to our systems, data or networks. This includes annual training for Employees, and periodic training for Contractors. Additionally, users receive security reminders periodically *(Referenced from: Doc 13 - Cybersecurity Compliance Policy).*
		Protection from Malicious Software **(ADDRESSABLE)**	Guard against, detect, and report malicious software.	**Malicious Code** Systems that connect to enterprise American networks and systems have malware protection configured to perform the following activities: - Block / quarantine malicious code, based on the malware severity *(Referenced from: Doc 17 - Malicious Code).* ***Endpoint Security*** To safeguard against malicious software, endpoint devices must have centrally managed protection, including anti-malware, personal firewalls, and intrusion detection systems. These devices are configured to run approved operating systems with the latest security patches and anti-virus software to prevent

	STANDARD	IMPLEMENTATION SPECIFICATION	DESCRIPTION / EXAMPLES	PLAN PROCEDURE
				unauthorized access. Any incidents involving potential threats or compromised devices must be reported immediately in accordance with the organization's security incident reporting policy. *(Referenced from: Doc 12 - Endpoint Security Policy).*
		Log-In Monitoring **(ADDRESSABLE)**	Monitor log-in attempts and report discrepancies.	**Security Log Management** The Security Log Management infrastructure are used to monitor login attempts and track suspicious activity. American will configure the SA system to capture failed login attempts to include username, IP address of attempt source, date/time, and other relevant fields *(Referenced from: Doc 20 - Security Log Management).*
		Password Management **(ADDRESSABLE)**	Create, change, and safeguard passwords.	**Password Management Standard** Passwords must be created with complexity requirements, changed regularly, and safeguarded through encryption and restricted access. *(Referenced from: Doc 37 - Password Management Standard)*
(6)	**Security Incident Procedures** – Procedures to address security incidents.	Response & Reporting **(REQUIRED)**	Identify and respond to suspected or known security incidents; mitigate harmful effects; document security incidents and outcomes.	**Incident Response Cybersecurity Incident Response Plan (ECIRP and CIRP)** To identify and respond to suspected and known security incidents, American Airlines' Cybersecurity Incident Response Plan (CIRP) that aligns with its Enterprise Cybersecurity Incident Response Plan (ECIRP). This plan ensures the detection,

	STANDARD	IMPLEMENTATION SPECIFICATION	DESCRIPTION / EXAMPLES	PLAN PROCEDURE
				analysis, containment, and recovery from incidents, minimizing impacts on confidentiality, integrity, and availability. The ECIRP outlines the communication process for incident reporting to stakeholders, while post-incident analysis is conducted to uncover root causes, with lessons learned documented to strengthen future response efforts and reduce risks. *(Referenced from: Doc 30 - Cyber Incident Response Policy)* **Incident Management** The Incident Management policy outlines procedures for handling security incidents that could impact an organization's operations. This includes documenting security incidents and outcomes. *(Referenced from: Doc 38 - Incident Management Policy)*
(7)	**Contingency Plan** – Procedures to respond to emergencies that may damage systems.	Data backup Plan **(REQUIRED)**	Create and maintain retrievable exact copies of EPHI.	**Retrievable copies** The plan ensures that retrievable exact copies of electronic protected health information (EPHI) are created and maintained through secure backup processes. This includes safeguarding backup media and ensuring data integrity during the backup and retrieval process. *(Referenced from: Doc 50 - AA HIPAA Policies Revisions FINAL 1-23-2018)* **Backup and Recovery** The Backup and Recovery policy outlines procedures for creating backup copies of user-level information, system-level

	STANDARD	IMPLEMENTATION SPECIFICATION	DESCRIPTION / EXAMPLES	PLAN PROCEDURE
				information, and information system documentation. This ensures that critical data can be restored in case of a disaster or data loss. *(Referenced from: Doc 27 - Information Systems Policy)*
		Disaster Recovery Plan **(REQUIRED)**	Procedures to restore loss of data.	**Data Restoration** The Information Backup and Restore policy outlines procedures for restoring lost or corrupted data. This includes steps for identifying the type of backup needed, accessing backup media, and executing restoration processes. *(Referenced from: Doc 27 - Information Backup and Restore Policy)*
		Emergency Mode Operation Plan **(REQUIRED)**	Procedures to enable continuation of critical business processes for protection of EPHI while in emergency mode.	**Business Continuity Plan** The recovery governance policies emphasize establishing procedures to ensure the continuation of critical business processes, specifically safeguarding EPHI. These procedures include defining essential systems, developing recovery plans, and maintaining data integrity during recovery operations to minimize disruption during emergencies. *(Referenced from: Doc 43 - Recovery Governance.pdf, Doc 44 - Recovery Governance Policy.pdf)*
		Testing & Revision Procedures **(ADDRESSABLE)**	Procedures for periodic testing and revision of contingency plan.	**Contingency Plan Testing** The Contingency Planning policy outlines procedures for periodic testing and revision of the Business Continuity Plan. This includes steps for identifying test objectives, scheduling regular tests, and verifying successful execution of recovery strategies.

	STANDARD	IMPLEMENTATION SPECIFICATION	DESCRIPTION / EXAMPLES	PLAN PROCEDURE
				(Referenced from: Doc 27 - Information Backup and Restore)
		Applications & Data Criticality Analysis **(ADDRESSABLE)**	Assess relative criticality of applications and data in support of contingency plan.	**Application Criticality Standards,** Applications and data must be categorized based on their impact on business operations. This involves evaluating each application's role in supporting critical functions, its downtime tolerance, and recovery priority. The contingency plan will prioritize applications deemed critical to maintaining essential operations, ensuring minimal disruption during emergencies. *(Referenced from: Doc 45 - Application Criticality Standards.pdf)*
(8)	**Evaluation** – Ongoing evaluation of procedures.	Evaluation **(REQUIRED)**	Periodic technical and nontechnical evaluations of compliance with HIPAA standards in response to environmental and operational changes affecting security.	**Audit and Compliance** Periodic audits and compliance reviews are performed to evaluate the effectiveness of organizational procedures and policies to support all necessary Compliance frameworks applicable to American Airlines. This includes assessing adherence to regulatory requirements, industry standards, and internal controls. *(Referenced from: Doc 42 - Cybersecurity Compliance Policy)* **HIPAA Plan** The HIPAA document mandates that ongoing evaluations of both technical and nontechnical procedures must be conducted to ensure continuous compliance with HIPAA standards. This includes regularly assessing the effectiveness of current

	STANDARD	IMPLEMENTATION SPECIFICATION	DESCRIPTION / EXAMPLES	PLAN PROCEDURE
				security measures in response to any changes in the operational or environmental landscape that may affect the security of EPHI. *(Referenced from: Doc 50 - AA HIPAA Policies Revisions FINAL 1-23-2018)*

PHYSICAL SAFEGUARDS

	STANDARD	IMPLEMENATION SPECIFICATION	DESCRIPTION /EXAMPLES	PLAN PROCEDURE
(1)	**Facility Access Controls** – Procedures to limit physical access to system and facility in which housed, while ensuring authorized access.	Contingency Operations **(ADDRESSABLE)**	Allow facility access to restore lost data under disaster recovery plan and emergency mode operations plan.	**Access Control** Physical access to systems and facilities must be limited by using techniques such as RFID access cards or physical lock and key. This includes restricting access to hardware, network jacks, wireless access points, and gateways. *(Referenced from: Doc 34 - Access Control Standard)*
		Facility Security Plan **(ADDRESSABLE)**	Safeguard facility and equipment from unauthorized physical access, tampering, and theft.	**Physical Security** Facilities and equipment are safeguarded through strict access controls managed by the Enterprise Physical Access Control System (EPACS), which monitors all access points, including critical areas such as server rooms and data centers. Alarms are triggered and responded to immediately if

	STANDARD	IMPLEMENTATION SPECIFICATION	DESCRIPTION /EXAMPLES	PLAN PROCEDURE
				unauthorized access, tampering, or theft is detected. Regular audits and monitoring help ensure these safeguards are functioning correctly. *(Referenced from: Doc 34 - Access Control Standard.pdf,* and *Doc 48 - AA SCC Physical Access Control System Monitoring and Response_V3.5.pdf*
		Access Control and Validation **(ADDRESSABLE)**	Control and validate access to facilities based on role or function, including visitor control and control of access to software programs for testing and revision.	**Physical Security** Access to facilities is controlled and validated through the use of role-based access provisioning via the Enterprise Physical Access Control System (EPACS). Access is granted based on the individual's role or function, and visitor control is enforced through pre-registration and escort requirements. For software testing and revisions, restricted access is granted only to authorized personnel, and all access must be properly approved and documented. *(Referenced from: Doc 47 - Badging Access Procedures and Responsibilities V_6.pdf* and *Doc 48 - AA SCC Physical Access Control System Monitoring and Response_V3.5.pdf)*
		Maintenance Records **(ADDRESSABLE)**	Document repairs and modifications to physical facility	**Physical Security** Repairs and modifications to physical security infrastructure are documented within the

	STANDARD	IMPLEMENTATION SPECIFICATION	DESCRIPTION /EXAMPLES	PLAN PROCEDURE
			related to security (e.g., hardware, walls, doors, locks).	Enterprise Physical Access Control System (EPACS). These records are maintained for auditing purposes, and all service ticket information is tracked to ensure that repairs and modifications are completed securely and logged appropriately for future reference. *(Referenced from: Doc 48 - AA SCC Physical Access Control System Monitoring and Response_V3.5.pdf)*
(2)	**Workstation Use** – Procedures to specify physical attributes of workstation that can access EPHI.	Workstation Use **(REQUIRED)**	Procedures that specify workstations that can access EPHI.	**Access Control Standard and Information Access Policy** Workstations that can access sensitive information are controlled through physical and logical access mechanisms. Physical attributes of workstations include location in secure areas, restricted access via badges or keys, and placement within controlled zones such as server rooms or restricted access facilities. Additionally, workstations must have appropriate security controls such as encryption, screen locks, and restricted network access to ensure compliance with security policies. *(Referenced from: Doc 34 - Access Control Standard.pdf* and *Doc 32 - Information Access Policy.pdf)*

	STANDARD	IMPLEMENATION SPECIFICATION	DESCRIPTION /EXAMPLES	PLAN PROCEDURE
(3)	**Workstation Security** – Implement physical safeguards for workstations that access EPHI.	Workstation Security **(REQUIRED)**	For example, password protection, keeping computers with EPHI in locked rooms.	**Workstation Security** Workstations that access sensitive data must be physically secured in controlled areas, such as locked rooms or restricted zones, to prevent unauthorized access. Safeguards include the use of badge access systems, physical barriers (e.g., locks and secure enclosures), and surveillance to ensure that only authorized personnel can use these workstations. Additionally, workstations must be positioned to avoid unauthorized viewing of sensitive information. *(Referenced from: Doc 34 - Access Control Standard.pdf, Doc 32 - Information Access Policy.pdf)*
(4)	**Device & Media Controls** – Procedures to govern receipt and removal of hardware and electronic media that contain EPHI within facility and outside.	Disposal **(REQUIRED)**	Procedures to dispose of PHI and hardware or electronic media on which it is stored.	**Information Handling and Disposal Standard** Outlines strict procedures for the receipt and removal of hardware and electronic media containing sensitive data. Upon receipt, hardware and media must be logged, inspected, and stored securely to prevent unauthorized access. When removing or disposing of such items, they must be sanitized, decommissioned, or destroyed using approved methods to ensure that sensitive data is irretrievable. All movements of hardware and

	STANDARD	IMPLEMENATION SPECIFICATION	DESCRIPTION /EXAMPLES	PLAN PROCEDURE
				media are tracked and logged to ensure accountability. *(Referenced from: Doc 49 - Information Handling and Disposal Standard.pdf)*
		Media Re-Use **(REQUIRED)**	Procedures for removal of EPHI from electronic media before available for re-use.	**Information Handling and Disposal Standard** Specifies that before electronic media containing sensitive data is made available for re-use, all sensitive information must be securely removed through a process called sanitization. This includes techniques such as data wiping, degaussing, or cryptographic erasure to ensure the data is irrecoverable. Media must be verified post-sanitization to confirm the data has been fully removed before being repurposed. *(Referenced from: Doc 49 - Information Handling and Disposal Standard.pdf)*
		Accountability **(ADDRESSABLE)**	Maintain record of movements of hardware and electronic media and any person responsible.	**Information Handling and Disposal Standard** Mandates that all movements of hardware and electronic media containing sensitive data must be logged and tracked. This includes detailed records of when and where the items are moved, as well as identifying the individuals responsible for their handling at each stage. This ensures accountability and transparency throughout the

	STANDARD	IMPLEMENATION SPECIFICATION	DESCRIPTION /EXAMPLES	PLAN PROCEDURE
				lifecycle of the hardware and media, from receipt to disposal or reuse. *(Referenced from: Doc 49 - Information Handling and Disposal Standard.pdf)*
		Data Backup & Storage **(ADDRESSABLE)**	Create retrievable, exact copy of EPHI, when needed, before movement of equipment.	**Backup and Storage** Before moving any equipment containing sensitive data, the Information Handling and Disposal Standard requires that exact, retrievable copies of the sensitive data be created and securely stored. This ensures that, in case of data loss during the movement of equipment, an identical copy is available for restoration. Backup procedures must comply with security requirements to maintain the integrity and confidentiality of the sensitive data. *(Referenced from: Doc 49 - Information Handling and Disposal Standard.pdf, Doc 43 - Recovery Governance)*

TECHNICAL SAFEGUARDS

	STANDARD	IMPLEMENTATION SPECIFICATION	DESCRIPTION / EXAMPLES	PLAN PROCEDURE
(1)	**Access Control** – Procedures to allow access	Unique User Identification **(REQUIRED)**	Assign unique name or number for identifying	**Identity Management Standard** Mandates that each user must be assigned a unique

	STANDARD	IMPLEMENTATION SPECIFICATION	DESCRIPTION / EXAMPLES	PLAN PROCEDURE
	only to authorized persons or programs.		and tracking user identity.	identifier, such as a name or number, to track and manage user identity within systems. This unique identifier ensures accountability and proper tracking of all user actions within the information systems, and it is required for access provisioning, authentication, and auditing purposes. *(Referenced from: Doc 35 - Identity Management Standard.pdf)*
		Emergency Access procedures **(REQUIRED)**	Establish procedures to obtain necessary EPHI during an emergency.	**Access Control Standard and Identity Management Standard** Documents outline procedures to ensure that, in the event of an emergency, authorized personnel can gain necessary access to sensitive data. These procedures include setting up emergency accounts with pre-approved access, ensuring they are only activated during emergency situations, and ensuring all actions are logged and tracked for audit purposes. The procedures guarantee that sensitive data is accessible when critical decisions need to be made, while maintaining security controls. *(Referenced from: Doc 34 - Access Control Standard.pdf, Doc 35 - Identity Management Standard.pdf)*

	STANDARD	IMPLEMENTATION SPECIFICATION	DESCRIPTION / EXAMPLES	PLAN PROCEDURE
		Automatic Logoff **(ADDRESSABLE)**	Procedures to terminate electronic session after predetermined time of inactivity.	**Session Timeout** Electronic sessions are terminated automatically after a predetermined period of inactivity to prevent unauthorized access (15 minutes). This can be achieved through idle timeout settings, which close or log out users who have been inactive for a specified duration. *(Referenced from: Doc 34 - Access Control Standard)*
		Encryption and Decryption **(ADDRESSABLE)**	Mechanism to encrypt or decrypt EPHI.	**Encryption** A mechanism for encrypting and decrypting data must be in place to protect sensitive information. This includes implementing cryptographic protocols such as encryption algorithms, decryption keys, and secure key management practices. *(Referenced from: Doc 26 - Cryptographic Usage)*
(2)	**Audit Controls** – Procedures to examine activity of systems.	Audit Controls **(REQUIRED)**	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain EPHI.	**Monitoring** Activity monitoring and auditing mechanisms track access, modifications, and other interactions with sensitive information. These mechanisms can include log analysis tools, intrusion detection systems, and audit trails that provide a record of system activity, including login attempts, data access, and changes made to sensitive information.

	STANDARD	IMPLEMENTATION SPECIFICATION	DESCRIPTION / EXAMPLES	PLAN PROCEDURE
				(Referenced from: Doc 34 - Access Control Standard, Doc 41 - Security Log Management Standard)
(3)	**Integrity** – Procedures to protect EPHI from improper alteration or destruction.	Mechanism to authenticate EPHI **(ADDRESSABLE)**	Implement electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner.	**Data Integrity** Electronic mechanisms, such as digital signatures and hash functions ensure the integrity of electronic information. These mechanisms can include data checksums, message authentication codes (MACs), and other techniques that verify the accuracy and completeness of data during transmission, storage, or processing. *(Referenced from: Doc 26 - Cryptographic Usage)*
(4)	**Person or Entity Authentication** – Procedures to verify person seeking access if one claimed.	Person or Entity Authentication **(REQUIRED)**	Assign a separate user account to each user in your organization. Train and regularly remind users that they must never share their passwords. Require each user to create an account password that is different from the ones used for personal internet or e-mail access	**Password Management Standard** Unique user accounts with distinct login credentials are assigned to each individual in the organization. Users should be required to create complex passwords that do not reuse or compromise previously used passwords, such as those for personal internet or email services. Regular training and reminders on password security best practices should be provided to users to prevent password sharing and unauthorized access.

	STANDARD	IMPLEMENTATION SPECIFICATION	DESCRIPTION / EXAMPLES	PLAN PROCEDURE
			(e.g., Gmail, Yahoo, Facebook).	*(Referenced from: Doc 37 - Password Management Standard)*
(5)	**Transmission Security** – Measures to guard against unauthorized access to EPHI transmitted over network.	Integrity Controls **(ADDRESSABLE)**	Ensure electronically transmitted EPHI is not improperly modified without detection.	**Cryptographic Usage** Integrity controls ensure that electronic protected health information (EPHI) is accurate, complete, and not altered or destroyed in an unauthorized manner. Data checksums and digital signatures should be used to verify data integrity during transmission and storage. *(Referenced from: Doc 26 - Cryptographic Usage)*
		Encryption **(ADDRESSABLE)**	Mechanism to encrypt or decrypt EPHI whenever deemed appropriate.	**Cryptographic Usage** Access to sensitive information must be protected by implementing robust encryption mechanisms that allow for secure data transmission and storage. A combination of symmetric and asymmetric encryption methods, along with regular key rotation and update policies ensure the confidentiality and integrity of encrypted data. *(Referenced from: Doc 26 - Cryptographic Usage)*

OTHER REQUIREMENTS

	STANDARDS	IMPLEMENTATION SPECIFICATION	DESCRIPTION / EXAMPLES	PLAN PROCEDURE
(1)	**Business Associate Contracts**	Update Business Associate contracts for HIPAA security provisions.	Amend business associate contract to require business associate to: ▪ Implement appropriate security safeguards; ▪ Ensure that any agent to whom it discloses EPHI also implements such safeguards; ▪ Report to covered entity any security incident of which it becomes aware; and ▪ Authorize termination of contract if covered entity determines business associate has violated material term.	**AA HIPAA Policy** The Plan ensures that all Business Associate contracts include language requiring the Business Associate to comply with HIPAA security standards. This includes implementing administrative, technical, and physical safeguards to protect PHI. Contractual Provisions The contract also requires the Business Associate to report any breach of unsecured PHI to the Plan within a specified timeframe. *(Referenced from: Doc 50 - AA HIPAA Policies Revisions FINAL 1-23-2018)*
(2)	**Plan Document**	Update plan document and certification for	Update plan amendment (under HIPAA	**AA HIPAA Policy** The Plan document has been revised to include the

	STANDARDS	IMPLEMENTATION SPECIFICATION	DESCRIPTION / EXAMPLES	PLAN PROCEDURE
		HIPAA security provisions (if applicable).	Privacy Rule) to require plan sponsor to: ▪ Implement administrative, physical, and technical safeguards that reasonably and appropriately protect confidentiality, integrity, and availability of EPHI; ▪ Ensure that the adequate separation among workforce members, as required by HIPAA Privacy Rules, is supported by reasonable and appropriate security measures. ▪ Ensure that any agent to whom it	required HIPAA security provisions, including administrative, technical, and physical safeguards. The Plan sponsor must implement administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of EPHI. This includes ensuring adequate separation among workforce members and implementing reasonable and appropriate security measures. *(Referenced from: Doc 50 - AA HIPAA Policies Revisions FINAL 1-23-2018)*

	STANDARDS	IMPLEMENTATION SPECIFICATION	DESCRIPTION / EXAMPLES	PLAN PROCEDURE
			discloses EPHI also implements such safeguards; and ▪ Report to covered entity any security incident of which it becomes aware.	
(3)	**Policies & Procedures**	Procedures **(REQUIRED)**	Implement "reasonable and appropriate" policies and procedures to comply with these standards, implementation specifications, and other regulation requirements.	**AA HIPAA Policy** The organization has implemented policies and procedures that meet the "reasonable and appropriate" standard for compliance with HIPAA regulations. These include: Implementing administrative safeguards such as workforce training and security awareness programs. *(Referenced from: Doc 50 - AA HIPAA Policies Revisions FINAL 1-23-2018)*
(3)	**Documentation**	Time Limit **(REQUIRED)**	Retain for 6 years from date of creation, or date when last in effect, if later.	**AA HIPAA Policy** All written requests for accounting and responses must be retained for six years. This includes both the request and the response. *(Referenced from: Doc 50 - AA HIPAA Policies Revisions FINAL 1-23-2018)*

	STANDARDS	IMPLEMENTATION SPECIFICATION	DESCRIPTION / EXAMPLES	PLAN PROCEDURE
		Availability **(REQUIRED)**	Make documentation available to those persons responsible for implementing procedures.	**AA HIPAA Policy** The Plan must make its privacy policies and procedures available to all members of its workforce who need to know their contents in order to carry out their duties. This includes making the documents readily available to those responsible for implementing the procedures. *(Referenced from: Doc 50 - AA HIPAA Policies Revisions FINAL 1-23-2018)*
		Updates **(REQUIRED)**	Review and update documentation periodically.	**AA HIPAA Policy** The Plan must review and update its privacy policies and procedures at least annually, or whenever there is a material change in the Plan's practices. *(Referenced from: Doc 50 - AA HIPAA Policies Revisions FINAL 1-23-2018)*