RYMAN HOSPITALITY PROPERTIES, INC.
HIPAA PRIVACY AND SECURITY
POLICIES AND PROCEDURES

RYMAN HOSPITALITY PROPERTIES, INC.
HIPAA PRIVACY AND SECURITY
POLICIES AND PROCEDURES

Updated September 23, 2013

Revisions Effective August 1, 2016

Purpose

It is the policy of all health plans sponsored by Ryman Hospitality Properties, Inc. ("Ryman") to preserve the availability, integrity and confidentiality of PHI pertaining to its Participants, to comply with the privacy regulations issued by the United States Department of Health and Human Services ("HHS") under the Health Insurance Portability and Accountability Act ("HIPAA") and to comply with other federal and state laws applicable to such PHI. Further, it is the policy of the Plans to use reasonable and appropriate safeguards to protect the integrity, confidentiality and availability of EPHI pertaining to its Participants and to comply with the security regulations issued by HHS.

Section 1. Definitions

The following definitions are applicable to all sections set forth in these Policies and Procedures:

A. "Business Associate" means, with respect to a Plan, a person who:

(1) on behalf of the Plan, but other than in the capacity of a Workforce Member, creates, receives, maintains, or transmits PHI for a function or activity regulated by the HIPAA Rules, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed in 42 CFR 3.20, billing, benefit management, practice management, and repricing; or

(2) provides, other than in the capacity of a Workforce Member, legal, actuarial, accounting, consulting, data aggregation (as defined in 45 CFR § 164.501), management, administrative, accreditation, or financial services to or for the Plan, where the provision of the service involves the disclosure of PHI from the Plan, or from another Business Associate of the Plan, to the person.

B. "Breach" means the acquisition, access, use or disclosure of PHI in a manner not permitted by the privacy provisions of HIPAA and that compromises the security or privacy of the PHI, unless an exception applies as described in Section 11.

C. "Covered Entity" is a health plan, healthcare provider or healthcare clearinghouse that is subject to the HIPAA Rules and is acting in such capacity.

D. "Designated Record Set" means a group of records maintained by or for a Plan that is used, in whole or in part, by or for the Plan to make decisions about Participants. A Plan's

Designated Record Set includes enrollment, payment, claims adjudication, and case or medical management records systems maintained by or for the Plan.

E. "De-identified Information" means information that does not include any of the following identifiers of Participant or the Participant's employer, family members or household members: name; all geographic subdivisions smaller than a state (including street address, city, county, precinct and zip code); all elements of dates related to a Participant (including birth date, admission date and discharge date) except for years (other than year of birth for those over 89); telephone numbers; fax numbers; electronic mail address; social security number; medical record number; health plan beneficiary number; account number; certificate/license number; serial number of a vehicle or other device identifier; internet URL; internet protocol (IP) address number; biometric identifiers, including finger and voice prints; full face photographic images and any other unique information that could reasonably be used alone or in combination with other information to identify a Participant.

F. "EPHI" means PHI that is transmitted by electronic media or maintained in electronic media. The term "electronic media" means: (i) electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or (ii) transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media because the information being exchanged did not exist in electronic form before the transmission.

G. "Genetic Information" means, with respect to a Participant, information about (i) the Participant's genetic tests, (ii) the genetic tests of family members of the Participant, and (iii) the manifestation of a disease or disorder in family members of such Participant. It includes any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the Participant or any family member of the Participant. It does not include information about the sex or age of any Participant.

H. "HIPAA Rules" means the privacy and security regulations issued by HHS and set forth at 45 CFR Part 160 and Part 164, subparts A, C, D and E.

I. "Limited Data Set" means PHI that excludes all of the following direct identifiers of the Participant and of relatives, employers, and household members of the Participant: names; postal address information (other than town or city, State, and zip code); telephone numbers; fax numbers; e-mail addresses; social security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate/license numbers; vehicle identifiers and serial numbers (including license plate numbers); device identifiers and serial numbers; internet URLs; IP address numbers; biometric identifiers (including finger and voice prints); and full face photographic images and any comparable images.

J. "Participant" means any Participant that receives health care coverage from a Plan, including employees, retirees, surviving spouses, or COBRA beneficiaries and any dependents or other individuals receiving health care benefits as a result of their relationship with a Primary Source of Coverage.

K. "Plan" means the Health Care Spending Account Program under the Ryman Hospitality Properties, Inc. Flexible Benefits Plan (a part of the Ryman Hospitality Properties, Inc. Employee Health and Welfare Plan) and the Ryman Hospitality Properties, Inc. Retiree Reimbursement Account, each a "Plan" and collectively the "Plans." Each Plan is a Covered Entity.

L. "Plan Sponsor" means Ryman to the extent Ryman meets the definition of "plan sponsor" set forth at Section 3(16)(B) of ERISA (29 USC 1002(16)(B)).

M. "Personal Representative" means a person who has authority under applicable law to make decisions related to health care on behalf of an adult or an emancipated minor, or the parent, guardian, or other person acting *in loco parentis* who is authorized under law to make health care decisions on behalf of an unemancipated minor, except where the minor is authorized by law to consent, on his/her own or via court approval, to a health care service, or where the parent, guardian or person acting *in loco parentis* has assented to an agreement of confidentiality between the provider and the minor.

N. "Primary Source of Coverage" means the Participant that, due to the Participant's status as an employee, retiree, surviving spouse, or COBRA beneficiary, is the primary source of health care coverage for himself/herself and any other dependents.

O. "Protected Health Information" or "PHI" means any individually identifiable information, whether oral or recorded in any form or medium, that relates to the past, present or future physical or mental health or condition of a Participant, the provision of health care to a Participant, or the past, present or future payment for the provision of health care to a Participant. PHI is "protected" in all forms, including paper records, oral communications and electronic media. PHI includes Genetic Information. PHI pertains to both living and deceased individuals, unless the individual has been deceased for more than fifty (50) years. Ryman will assume that an individual has not been deceased for more than fifty (50) years unless it has received documentation or other reasonable evidence of death of the individual. Information that meets the definition of De-identified Information is not PHI and is not subject to these Policies and Procedures.

P. "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification or destruction of EPHI or interference with system operations in an information system containing or allowing access to EPHI.

Q. "Summary Health Information" means information that summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom a Plan Sponsor

has provided health benefits under a Plan and that is De-identified Information, except that geographic information is only required to be aggregated to the level of a 5 digit zip code.

R. "TPA" means a third party administrator engaged by a Plan or by Ryman on behalf of a Plan under a service agreement to administer the Plan.

S. "Unsecured PHI" means PHI that is not rendered unusable, unreadable or indecipherable to unauthorized individuals through the use of a technology or methodology specified on the HHS website (www.hhs.gov/ocr/privacy). For example, PHI that has been encrypted in accordance with HHS guidance or that has been shredded or destroyed so that the information cannot be read or reconstructed would not be considered Unsecured PHI.

T. "Workforce Member" means employees and other persons whose conduct, in the performance of work for a Plan, is under the direct control of the Plan, whether or not they are paid by the Plan, which includes individuals in Human Resources and Treasury who are responsible for Plan administration and individuals in IT and Legal who provide support to the foregoing individuals. Each Plan's plan document provides that the Workforce Members are allowed access to PHI.

U. Other Terms. Terms contained herein and defined in the HIPAA Rules shall have the meaning given to such terms in the HIPAA Rules.

Section 2. Privacy Officer and Security Officer

A. Privacy Officer

The Privacy Officer for the Plans ("Privacy Officer") is the SVP, General Counsel and Corporate Secretary of Ryman. The Privacy Officer will be responsible for development, implementation, and enforcement of these Policies and Procedures, except for provisions related to the security of EPHI (which are the responsibility of the Security Officer as defined below), and reporting to the Plan Sponsor. The Privacy Officer for the Plans can be contacted at 615-316-6000, HIPAA@RymanHP.com or One Gaylord Drive, Nashville, TN 37214.

The Privacy Officer is the contact person responsible for receiving requests and complaints related to access, privacy, amendment, and accountings of PHI and any other request or complaint relating to Plan privacy issues, as well as maintaining documentation required by these Policies and Procedures. Further, the Privacy Officer shall review and revise these Policies and Procedures as required by applicable law. The Privacy Officer may delegate tasks set forth in these Policies and Procedures to Workforce Members and/or to a TPA.

B. Security Officer

The Security Officer for the Plans ("Security Officer") is the VP, Compensation & Benefits of Ryman. The Security Officer will be responsible for development and implementation of the provisions of these Policies and Procedures related to the security of EPHI. The Security Officer

can be contacted at 615-316-6000, HIPAA@RymanHP.com or One Gaylord Drive, Nashville, TN 37214.

The Security Officer shall be responsible for implementing and monitoring the provisions of these Policies and Procedures related to the security of EPHI and reporting to the Plan Sponsor. The Security Officer is the contact person responsible for receiving complaints related to the security of EPHI. Further, the Security Officer shall review these Policies and Procedures and, in consultation with the Privacy Officer, amend these Policies and Procedures as required by applicable law. The Security Officer may delegate tasks set forth in these Policies and Procedures to Workforce Members.

Section 3. Participant Rights to PHI

A Plan will not require Participants to waive any rights under HIPAA, the HIPAA Rules, or these Policies and Procedures as a condition of the provision of treatment, payment, participation in the Plan, eligibility for benefits or otherwise.

A. Right to Access PHI

Participants have a right to access and copy their PHI and any information in their Designated Record Set, for as long as the PHI is maintained in the Designated Record Set by a Plan, except for as follows: (1) psychotherapy notes; (2) information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding; and (3) PHI maintained that is subject to the Clinical Laboratory Improvements Amendments of 1988 set forth at 42 USC 263(a) ("CLIA"), to the extent the HIPAA Rules permit the PHI to be exempt from the access requirement.

Any requests for access received by a Workforce Member must be forwarded to the Privacy Officer to handle. The Privacy Officer will oversee the response to the access request in compliance with the HIPAA Rules. In most, if not all cases, responding to an access request will require coordination with the applicable Plan's TPA. If provided for under the Plan's contract or arrangement with its TPA, the TPA will handle responding to the request in compliance with the HIPAA Rules.

In order to request access to the Participant's PHI, the Participant must make a written request and indicate how the PHI should be delivered. The Plan will provide a Participant with access to the PHI in the form or format requested by the Participant, if it is readily producible in such form or format. If such form or format is not readily available, another readable, hard copy form will be provided to the Participant. However, if the Participant requests an electronic copy of PHI that is maintained in a Designated Record Set electronically, the Plan will provide the Participant with access to the PHI in the electronic form and format requested by the individual, or if the PHI is not readily producible in the requested form or format, in a readable electronic form and format agreed to by the Plan and the Participant.

A Plan may provide a summary of the PHI in lieu of providing access, or may provide an explanation of the information to which access has been provided, if the Participant agrees in advance to such a summary or explanation and, if applicable, the Participant agrees in advance to the fees associated with providing such summary or explanation.

A Plan may impose a reasonable, cost-based fee for copying, or preparing a summary or explanation of the information. The fee will include only the cost of labor for copying the PHI, whether in paper or electronic form; supplies for creating the paper copy or electronic media if the Participant requests that the electronic copy be provided on portable media; postage, when the Participant has requested the copy, summary or explanation be mailed; and the cost of preparing an explanation or summary of the PHI if a summary or explanation has been agreed to by the Participant.

Access requests will be granted unless a ground for denial permitted by the HIPAA Rules applies to the requested PHI. In the event a Plan denies a Participant access to the Participant's PHI, the Plan will provide a written denial to the Participant within the time frame set forth below. The written denial will include a basis for the denial; a statement detailing the Participant's review rights; a statement how the Participant may exercise such review rights; and a description of how the Participant may file a complaint with the Plan or with HHS.

A Plan may deny a Participant access to the Participant's PHI without providing the Participant an opportunity for a review of the denial if the PHI is exempted from the right of access (see above) or in certain limited situations set forth in the HIPAA Rules. The Privacy Officer will determine whether any exceptions to the right to review apply.

A Plan may deny access in the following situations, provided that the Participant is provided with a right to have the denial reviewed:

- a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the Participant or another person;

- the PHI makes reference to another person other than a health care provider, and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or

- the request for access is made by a Participant's Personal Representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such Personal Representative is reasonably likely to cause substantial harm to the Participant or another person.

If the Participant requests a review of a denial made based on one of the above reviewable reasons, the denial will be reviewed by a licensed health care professional who is designated by the Plan and who did not participate in the original denial decision. The Plan will abide by the determination of the reviewing licensed health care professional.

A Plan will act on a Participant's request for access no later than 30 days after receiving the request. The Plan may be permitted to extend the time for acting on the request by 30 days, provided the Plan provides the Participant with a written statement detailing the reasons for the delay and the date by which the Plan will complete its action on the request. The Plan may only have one such extension of time for action on a Participant's request for access.

If the Participant's request for access directs the Plan to transmit the copy of PHI directly to another person, the Plan will provide the copy to the person designated by the Participant, provided that the request is in writing, is signed by the individual and clearly identifies the recipient and where to send the PHI. Section 4(E) addresses requirements for a compliant authorization to use or disclose PHI. A request for access/designation of a third party recipient does not have to meet all of the requirements for a complaint authorization. If a Participant requests PHI to be sent to a third party (without including an authorization that includes the elements set forth at Section 4(E)), the Privacy Officer will be consulted regarding whether additional documentation is required before responding to the request (i.e., does the request require an authorization? Or does the request constitute a request to transmit the PHI directly to a third party that is written, signed and clearly identifies the recipient and where to provide the PHI?). Requests for PHI delivered to a Plan by third parties (anyone besides the Participant or the Participant's Personal Representative) must meet the requirements set forth in Section 4(E) unless the Plan determines that the request constitutes an access request (that has been delivered by a third party on behalf of the Participant). If necessary, the Participant will be contacted to clarify whether the Participant is attempting to exercise his or her rights to access PHI and may be requested to complete a more clearly worded access request and, if applicable, a designation of a third party recipient. If a request to disclose PHI directly to a third party is rejected (because it does not contain a valid authorization and the Plan concludes it does not meet the requirements for the Plan to deliver the PHI directly to a third party recipient), the Privacy Officer will notify the Participant of the deficiency and either provide the PHI directly to the Participant (provided no other basis for a denial applies as described above) or instruct the Participant on how to provide an actionable request (such as by sending the Plan's authorization form to the Participant to complete).

The Plans will document and retain for 6 years from the date of its creation the Designated Record Sets subject to access and title of the Workforce Members responsible for receiving and processing such requests (the Privacy Officer).

B. **Right to Amend PHI**

A Participant may request a Plan amend PHI contained in a Designated Record Set for as long as the PHI is maintained in the Designated Record Set. A Participant may request such an amendment by submitting a written request to the Privacy Officer.

Any requests for amendment received by a Workforce Member must be forwarded to the Privacy Officer to handle. The Privacy Officer will oversee the response to the amendment request in compliance with the HIPAA Rules. In most, if not all cases, responding to an amendment request will require coordination with the applicable Plan's TPA. If provided for under the Plan's contract or arrangement with its TPA, the TPA will handle responding to the request in compliance with the HIPAA Rules.

A Plan will act on the Participant's request for an amendment no later than 60 days after receiving such a request. If the Plan is unable to act on the amendment within 60 days, the Plan may extend the time for action by no more than 30 days, provided the Plan provides the Participant with a written statement of the reasons for the delay and the date by which the Plan will complete its action on the request.

In the event the Plan accepts the requested amendment, in whole or in part, the Plan will:

- make the appropriate amendment to the PHI or record that is the subject of the request by, at a minimum, identifying the records in the Designated Record Set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment;

- timely inform the Participant that the amendment is accepted and obtain the Participant's identification of, and agreement to have the Plan notify, relevant parties with which the amendment needs to be shared; and

- make reasonable efforts to inform and provide the amendment within a reasonable time to persons identified by the Participant as having received PHI about the Participant and needing the amendment, and/or persons, including the TPA and other Business Associates, that maintain PHI that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the Participant.

The Plan may deny a Participant's request for amendment, if it determines that the PHI record that is subject of the request:

- was not created by the Plan, unless the Participant provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment;

- the information is not part of the Designated Record Set;

- the information is not available for access under the HIPAA Rules (see Section 3(A) above); or

- the information is accurate and complete.

In the event the Plan denies the amendment request, in whole or in part, the Plan will provide the Participant with a written denial that sets forth the basis for the denial; the Participant's right to submit a written statement disagreeing with the denial; a statement explaining how the Participant may file such a statement; and a statement informing the Participant that if the Participant does not submit a statement of disagreement, the Participant may request that the Plan provide the Participant's request for amendment and the Plan's written denial with any future disclosures of the PHI that is the subject of the amendment request. The Plan's written denial will also include a description of how the Participant may file a complaint with the Privacy Officer or HHS.

If the Participant submits a statement of disagreement, the Plan may prepare a written rebuttal to a statement of disagreement filed by a Participant. Whenever the Plan prepares a rebuttal, the Plan will provide a copy to the Participant who submitted the statement of disagreement. If a statement of disagreement has been submitted by a Participant, the Plan will include the material appended or, at the election of the Plan, an accurate summary of any such information, with any subsequent disclosure of the PHI to which the disagreement relates. If the Participant has not submitted a written statement of disagreement, the Plan will include the Participant's request for amendment and the Plan's written denial, or an accurate summary of the information with any subsequent disclosure of the PHI, only if the Participant has requested such action. If the Participant has requested that the information be

included with any subsequent disclosure, and such subsequent disclosure does not permit the additional material to be included with the disclosure, the Plan may separately transmit the material to the recipient of the PHI.

If the Plan is informed by another Covered Entity under the HIPAA Rules of an amendment to a Participant's PHI, the Plan will amend the PHI accordingly in Designated Record Sets maintained by the Plan.

C. Right to an Accounting of Disclosures

A Participant has a right to receive an accounting of disclosures of PHI made by a Plan for any period of time up to 6 years prior to the date on which the accounting is requested. A Participant may request an accounting of disclosures by completing a written request and submitting the request to the Privacy Officer.

Any requests for an accounting of disclosures received by a Workforce Member must be forwarded to the Privacy Officer to handle. The Privacy Officer will oversee the response to the accounting request in compliance with the HIPAA Rules. In most, if not all cases, responding to an accounting request will require coordination with the applicable Plan's TPA. If provided for under the Plan's contract or arrangement with its TPA, the TPA will handle responding to the request in compliance with the HIPAA Rules.

The accounting of disclosures will not include disclosures permitted to be excluded from the accounting under the HIPAA Rules, including (1) disclosures required to carry out treatment, payment and health care operations (subject to a carve out for disclosures made from an electronic health record as described in regulations to be issued at a later date by HHS); (2) disclosures of a Participant's PHI to the Participant; (3) PHI disclosed incident to a use or disclosure otherwise permitted or required by the Privacy Regulations; and (4) PHI disclosed pursuant to an authorization.

The accounting of disclosures will include disclosures to or by Business Associates of the applicable Plan that are not excluded from the accounting under the HIPAA Rules and will include the date of the disclosure; the name of the entity or person who received the PHI and; if known, the address of the entity or person. The accounting of disclosures will also include a brief description of the PHI disclosed and a brief statement of the purpose of the disclosure that reasonably informs the Participant of the basis for the disclosures or, in lieu of such statement, a copy of the written request for a disclosure, if any.

If the Plan has made multiple disclosures of PHI to the same individual or entity during the period for which the accounting is requested, the Plan may, with respect to such multiple disclosures, provide the information set forth above with respect to the first disclosure, describe the frequency or number of the disclosures made during the accounting period, and the date of the last disclosure. Special rules apply to disclosures for research purposes, which the Privacy Officer will follow if applicable.

A Plan must temporarily suspend a Participant's right to receive an accounting of disclosures to a health oversight agency or law enforcement official for the time specified by the agency or official, if the agency provides the Plan with a written statement that indicates an accounting to the Participant

would be reasonably likely to impede the agency's activities and the written notice specifies the time for which a suspension is required. Any such suspensions will be conducted in accordance with the requirements for such suspensions as set forth in the HIPAA Rules at 45 CFR § 164.528(a)(2).

A Plan will act on a Participant's request for an accounting of disclosures within 60 days after receipt of the request. If the Plan is unable to provide the accounting within 30 days of receiving the request, the Plan may extend the time to provide the accounting by an additional 30 days, provided the Plan notifies the Participant in writing of the reasons for the delay and the date by which the Plan will provide the accounting.

The Plan will provide the first accounting to a Participant in any 12-month period without charge. The Plan may impose a reasonable, cost-based fee for each subsequent request for an accounting made by the same Participant within a single 12-month period; provided, however, the Plan will notify the Participant in advance of the fee and provide the Participant with an opportunity to withdraw or modify the request.

The Plan will document and retain the information required to be included in an accounting of disclosures of the Participant's PHI, the written accounting provided to a Participant, and Workforce Members responsible for receiving and processing accounting of disclosure requests (the Privacy Officer) for a period of 6 years from the date of the creation of the information.

D. Right to Request Additional Privacy Restrictions and Confidential Communications

A Participant has the right to request additional privacy restrictions with respect to the Participant's PHI. A Participant may request that a Plan restrict uses or disclosures of the Participant's PHI to carry out treatment, payment or health care operations and other disclosures permitted under 45 CFR § 164.510(b), which include disclosures to family members of the Participant and close personal friends of the Participant. The Plans are not required to agree to a restriction of the Participant's PHI, except for disclosures to another health plan for treatment for which the Participant has paid in full out of pocket ("Out of Pocket Exception"). The Plans will abide by any additional restrictions agreed to by the Plans and will not use or disclose PHI in violation of any agreed-to restrictions, except in the case of an emergency. The additional restriction may be terminated by the Participant orally or in writing. A Plan may terminate its agreement to the restriction at any time by providing written notice to the Participant, but the termination will only apply to PHI created or received after informing the Participant of the termination. Also, for restriction requests covered by the Out of Pocket Exception, a Plan may not terminate the restriction unless the Participant agrees (however, since the Plan is a health plan, it is unlikely to receive restriction requests that would qualify for the Out of Pocket Exception). The Plans will maintain documents related to the restriction for a period of 6 years from the date of the creation of the request.

Additionally, the Plans will accommodate a Participant's request for "confidential communications" --meaning a request that the Plan communicate PHI to the Participant by alternative means or at alternative locations--if the Participant clearly indicates that the disclosure of all or part of the information could endanger the Participant, and the Participant provides an alternative address or other method of contact. The Plans will not require the Participant to provide an explanation as to the basis for the request as a condition of providing communications on a confidential basis.

A Participant may make a request for additional privacy restrictions or confidential communications by submitting a written request to the Privacy Officer. Any requests for restriction or confidential communications received by a Workforce Member must be forwarded to the Privacy Officer to handle. The Privacy Officer will oversee the response to the request in compliance with the HIPAA Rules. In most, if not all cases, responding to a restriction or confidential communication request will require coordination with the applicable Plan's TPA. If provided for under the Plan's contract or arrangement with its TPA, the TPA will handle responding to the request in compliance with the HIPAA Rules. The Privacy Officer will ensure that appropriate steps are taken to implement any granted request, which may include notifying Business Associates of the granted request.

E. Right to Receive a Privacy Notice

The Plans will provide their Participants with a Notice of the Plan's Privacy Practices ("Notice"). The Notice must be written in plain language. It must contain the following statement as a header: "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY." The Notice must contain information related to uses and disclosures of PHI (including a description of the types of uses and disclosures that require an authorization, a statement that other uses and disclosures will be made only with the individual's authorization, and a statement that the individual may revoke an authorization); a statement that the Plan or a health insurance issuer with respect to the Plan may disclose PHI to the Plan Sponsor as permitted by the HIPAA Rules; information about individual rights under the HIPAA Rules; the Plan's duties with respect to the HIPAA Rules; a statement that the Plan is prohibited from using or disclosing Protected Health Information that is Genetic Information for underwriting purposes; information about how individuals may make complaints related to privacy; contact information for the Privacy Officer; a statement regarding the Plan's duty to notify the Participant in the event of a breach affecting the Participant's unsecured PHI; and the effective date of the Notice.

The Plans will make the Notice available to all new Participants at the time of enrollment. If a Plan maintains a website that provides information about its customer services or benefits, it will prominently post the Notice on the web site and make the Notice available electronically through the web site.

The Plans will promptly revise the Notice whenever there is a material change to the uses or disclosures of PHI, the Participant's rights, the Plan's legal duties, or other privacy practices stated in the Notice. If a Plan maintains a website, the Plan will post on its website the revised Notice by the effective date of the material change and will provide the revised Notice (or information about the material change and how to obtain the revised Notice) in its next annual mailing to Participants. If the Plan does not maintain a website, the Plan will provide all Participants with a copy of the Notice within 60 days of any material revision to the Notice. The Plan will also notify its Participants no less frequently than once every 3 years of the availability of the Notice and how to obtain the Notice.

The Plans may provide a Participant with an electronic copy of the Notice, provided the Participant agrees to accept an electronic copy of the Notice. If the Plan becomes aware that the transmission of the electronic Notice has failed, the Plan will mail a paper copy of the Notice to the Participant.

A Participant is entitled to receive a paper copy of the Notice upon request, even if the Participant has previously agreed to accept an electronic copy of the Notice.

Section 4. Uses and Disclosures of PHI

PHI may be used or disclosed as described in this Section 4 and as necessary to provide Participants with the rights described in Section 3. PHI may not be disclosed to the Plan Sponsor for the purpose of employment-related actions or decisions or in connection with any other benefit or employee benefit plan of the Plan Sponsor, unless an authorization that complies with the requirements set forth in Section 4(E) below has been signed by the Participant. Other disclosures to the Plan Sponsor may be made in compliance with Section 4(G).

If a desired use or disclosure is not addressed below, the use or disclosure of PHI may not be made unless the Privacy Officer has reviewed the contemplated use or disclosure in advance and confirmed that it complies with the HIPAA Rules. Any Workforce Member who desires to use or disclose PHI and is not certain whether the use or disclosure is permitted under these Policies and Procedures should consult with the Privacy Officer before making the use or disclosure. All uses and disclosures must comply with the Notice.

In addition to complying with a permitted use or disclosure listed in this Section 4, the use or disclosure must (1) comply with the minimum necessary standard to the extent applicable (see Section 8); (2) be made after verifying the requestor's identity and authority to receive the PHI (see Section 5); (3) be made after confirming a Business Associate Agreement is in place if the recipient is acting as a Business Associate of the Plan (see Section 6); and (4) not involve the use or disclosure of Genetic Information for underwriting purposes (as described in Section 4(F)). Further, unless a disclosure is exempt from right to receive an accounting of disclosures (see Section 3(C)), the disclosure must be recorded. The Privacy Officer must be notified of any disclosures that are made and are subject to the accounting obligation, so that the Privacy Officer can log the disclosure.

A Plan may not use or disclose PHI that is Genetic Information about a Participant for underwriting purposes (as described in Section 4(F)) even if an authorization is obtained.

The Plans will comply with any more stringent requirements of applicable state law.

A. Treatment, Payment and Health Care Operations

A Participant's PHI may be used and disclosed by a Plan for purposes of treatment, payment or health care operations as described in more detail below.

1. Treatment

A Plan may use and disclose PHI to provide, coordinate, or manage a Participant's health care and any related services. This includes the coordination or management of a Participant's health care with the Participant's physician or other third party involved in the Participant's care.

2. Payment

The Participant's PHI may be used and disclosed, as needed, to facilitate and coordinate payment for the Participant's health care services. This may include certain activities that are undertaken before it approves or pays for the Participant's health care services such as making a determination of eligibility or coverage for insurance benefits and payment-related services such as reviewing services provided to the Participant for medical necessity, and undertaking utilization review.

3. Health Care Operations

A Plan may use or disclose, as needed, the Participant's PHI in order to support the Plan's health care operations. "Health care operations" include, but are not limited to, quality assessment and improvement activities, disease management, patient safety activities, and Plan employee review activities. It also includes underwriting, enrollment, premium rating and other activities related to the creation, renewal or replacement of a contract of health insurance or health benefits, except as prohibited under Section 4(F). Disclosures to the Plan Sponsor for health care operations must also comply with Section 4(G).

A Plan may disclose PHI for the health care operations of another Covered Entity if the other Covered Entity has an existing relationship with the Participant that relates to the purpose of the disclosure and the purpose of the disclosure falls within certain sections of the definition of *health care operations* under the HIPAA Rules (such as disease management and quality assessment activities). If a Plan is contemplating disclosing PHI for the health care operations of another Covered Entity, the Privacy Officer must be consulted and must confirm that the disclosure is permissible prior to the disclosure being made.

B. Disclosure of Information to Family Members, Friends and Other Individuals Involved in a Participant's Care

Unless a Participant objects or requests additional privacy restrictions or alternative communications that are accepted by a Plan, the Plan may, in the exercise of professional judgment: (i) disclose to a Participant's family member, other relative, or close personal friend, PHI directly relevant to such person's involvement with the Participant's care or payment related to such care; or (ii) use or disclose PHI to notify, or assist in the notification of (including identifying or locating), a family member, other relative, or other person responsible for the care of the Participant of the Participant's location or general condition. The Plan may reasonably infer from the circumstances surrounding the request, or otherwise utilize the professional judgment of the Plan's Workforce Members and its experience with common practice to make reasonable inferences of, the Participant's best interest in disclosing PHI to an individual on behalf of a Participant.

If the Participant is deceased, the Plan may disclose PHI to the Participant's family member, other relative, or close personal friend if the recipient was involved in the Participant's care or payment for care prior the Participant's death. The PHI must be limited to PHI relevant to the recipient's involvement in care or payment for care. Disclosure may not be made if the disclosure would be inconsistent with the Participant's prior expressed preference that is known to the Plan.

C. Disclosure Incidental to a Permitted Use or Disclosure

An incidental use or disclosure is a use or disclosure that cannot be reasonably prevented, is limited in nature, and that occurs as a by-product of an otherwise permitted use or disclosure of PHI. Incidental uses and disclosures are permissible only to the extent that the applicable Plan has applied reasonable safeguards (see Section 13) and has implemented the minimum necessary standard (see Section 8) where applicable.

D. Permitted and Required Uses and Disclosures That May Be Made Without a Participant's Authorization or Opportunity to Object

A Plan may use or disclose a Participant's PHI in a limited number of situations without the Participant's consent or authorization. Each of these situations contains detailed requirements. Before making a use or disclosure under one of the situations listed below, the Privacy Officer must review the contemplated use or disclosure and confirm that it complies with the HIPAA Rules. These situations are as follows:

1. **Required By Law:** A Plan may use or disclose a Participant's PHI to the extent that the use or disclosure is required by law, including to HHS to investigate or determine the Plan's compliance with the HIPAA Rules and to the Participant in response to an access request as set forth in Section 3(A). The use or disclosure will be made in compliance with the law and will be limited to the relevant requirements of the law. The Participant will be notified, to the extent required by law, of any such uses or disclosures.

2. **Public Health:** A Plan may disclose a Participant's PHI for public health activities and purposes to a public health authority that is permitted by law to collect or receive the information. The disclosure will be made for the purpose of controlling disease, injury or disability. The Plan may also disclose the Participant's PHI, if directed by the public health authority, to a foreign government agency that is collaborating with the public health authority.

3. **Communicable Diseases:** A Plan may disclose a Participant's PHI, if authorized by law, to a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading the disease or condition.

4. **Health Oversight:** A Plan may disclose PHI to a health oversight agency for activities authorized by law, such as audits, investigations, and inspections. Oversight agencies seeking this information include government agencies that oversee the health care system, government benefit programs, other government regulatory programs and civil rights laws.

5. **Abuse or Neglect:** A Plan may disclose a Participant's PHI to a public health authority that is authorized by law to receive reports of child abuse or neglect. In addition, a Plan may disclose the Participant's PHI to the governmental entity or agency authorized to

receive such information if the Plan believes that the Participant has been a victim of abuse, neglect or domestic violence. In this case, the disclosure will be made consistent with the requirements of applicable federal and state laws.

6. **Legal Proceedings (discovery requests, court orders and subpoenas):** In accordance with applicable federal and state law, a Plan may disclose PHI in the course of any judicial or administrative proceeding, in response to an order of a court or administrative tribunal (to the extent such disclosure is expressly authorized) and in certain situations involving notice to the Participant or a special court order, in response to a subpoena, discovery request or other lawful process. Any subpoena, court order, discovery request or other lawful process must be forwarded to the Privacy Officer for review.

7. **Law Enforcement:** In accordance with applicable law, a Plan may also disclose PHI for law enforcement purposes.

8. **Workers' Compensation:** A Plan may disclose PHI as authorized to comply with workers' compensation laws and other similar legally-established programs.

9. **Limited Data Sets:** A Plan may use or disclose PHI that constitutes a Limited Data Set for purposes of research, public health or health care operations. Disclosures of a Limited Data Set for this purpose require a Data Use Agreement that meets requirements specified in the HIPAA Rules. If a Workforce Member wishes to use or disclose PHI that constitutes a Limited Data Set, the Workforce Member must consult with the Privacy Officer first and ensure that a Data Use Agreement is in place. If a third party requests that a Workforce Member sign a Data Use Agreement, the Workforce Member must send the Data Use Agreement to the Privacy Officer for review and approval.

10. **Other Situations:** A Plan may disclose PHI in the following additional situations, which do not typically arise, after the Privacy Officer has confirmed all applicable requirements have been met: to a coroner or medical examiner or funeral director; for cadaveric organ, eye or tissue donation purposes; to researchers when their research has been approved by an institutional review board that has reviewed the research proposal and established protocols to ensure the privacy of the Participant's PHI; to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; for certain military and national security purposes; and if the Participant is an inmate of a correctional facility; and for any other purpose or to any other recipient if the disclosure is permitted by the HIPAA Rules and consistent with the Notice.

E. Authorization

A Plan may use or disclose PHI as permitted by an authorization that complies with the requirements of this Section 4(E).

To be valid, an authorization must be written in plain language and contain at least the following elements:

- A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;
- A name or other specific identification of the person(s), or entity(ies), authorized to make the requested use or disclosure;
- The name or other specific identification of the person(s), or entity(ies), to whom the Plan may make the requested use or disclosure;
- A description of each purpose of the requested use or disclosure (the statement "at the request of the Participant" is a sufficient description of the purpose when a Participant initiates the authorization and does not, or elects not to, provide a statement of the purpose);
- An expiration date or an expiration event that relates to the Participant or the purpose of the use or disclosure;
- Signature of the Participant, or if the authorization is signed by a Personal Representative of the Participant, a description of the Personal Representative's authority to act on behalf of the Participant, and the date;
- A statement describing the Participant's right to revoke the authorization in writing and a reference to the revocation procedure and exceptions to the Participant's right to revoke contained in the Plan's Notice;
- A statement describing the inability of the Plan to condition enrollment or eligibility for benefits on the authorization, unless the authorization is for the Plan's eligibility or enrollment determinations relating to the Participant, or for its underwriting or risk rating determinations; and the authorization is not for the use or disclosure of psychotherapy notes;
- A statement describing the potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer protected by the HIPAA Rules;
- If the Plan will receive direct or indirect financial remuneration (anything of value) from a third party for obtaining an authorization to use or disclose PHI for marketing purposes, a statement that remuneration is involved;
- If the Plan will receive direct or indirect remuneration (including in-kind compensation) in connection with the sale of PHI, a statement that the disclosure will result in remuneration to the Plan; and
- If the disclosure is in exchange for direct or indirect remuneration from or on behalf of the recipient of the PHI, a statement that the disclosure will result in remuneration to the Plan.

A Participant may revoke an authorization at any time, provided that the revocation is in writing, except to the extent that the Plan has already taken action in reliance on the authorization; or if the authorization was obtained as a condition of obtaining insurance coverage and the Plan itself or other law provides the insurer with the right to contest a claim under the Plan.

A Plan must obtain an authorization before using or disclosing PHI for a purpose not otherwise expressly permitted by another subsection of this Section 4. Further, an authorization is required to use or disclose psychotherapy notes, to use or disclose PHI for purposes of marketing as described in Section 9 below or to sell PHI as set forth in Section 9.

An authorization is invalid and may not be relied upon if:

- The expiration date has passed or the expiration event is known by the Plan to have occurred;
- The authorization has not been filled out completely or the authorization does not contain all of the elements required by this Section 4(E) to be included in a valid authorization;
- The authorization is a compound authorization (unless the compound authorization is permitted by 45 CFR § 164.508(b)(3));
- The authorization was provided to the Plan improperly as a condition to the Participant being enrolled in the Plan or the Participant being eligible for benefits; or
- The Plan knows the authorization contains material information that is false.

A sample Authorization form is attached to Exhibit A (note: this sample does *not* contain elements that apply only to marketing and the sale of PHI).

Except for limited situations permitted by the HIPAA Rules, an authorization for use or disclosure of PHI cannot be combined with another document (i.e., any other type of permission) to create a compound authorization.

A Plan will not condition a Participant's enrollment in the Plan or eligibility for benefits on the provision of an authorization, unless the authorization is sought in connection with the Plan's eligibility or enrollment determinations relating to the Participant or for its underwriting or risk rating determinations, and the authorization is not related to the use or disclosure of psychotherapy notes.

An authorization is not required for Participants requesting their own PHI (see Section 3(A)).

See Section 4(F) below for special limitations regarding Genetic Information.

F. Genetic Information

A Plan may not use or disclose PHI that is Genetic Information about a Participant for underwriting purposes even if an authorization is obtained. "Underwriting purposes" include (1) rules for, or determinations of, eligibility (including enrollment and continued eligibility) for, or determination of, benefits under the Plan, coverage, or policy (including changes in deductibles or other cost-sharing mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program; (2) the computation of premium and contribution amounts under the Plan, coverage or policy (including discounts, rebates, payments in-kind or other premium differential mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program); (3) the application of any preexisting condition exclusion under the Plan; and (4) other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits. "Underwriting purposes" does not include determinations of medical appropriateness where an individual seeks a benefit under the Plan.

G. Disclosures to the Plan Sponsor

Disclosures of PHI may be made to the Plan Sponsor without an authorization in the following situations. Disclosures of PHI that is Genetic Information for underwriting purposes do not fall into any of the categories below.

1. **Summary Health Information:** The disclosure of Summary Health Information if the Plan Sponsor requests the Summary Health Information for the purpose of (a) obtaining premium bids from health plans for providing health insurance coverage under the Plan; or (b) modifying, amending or terminating a Plan. Note that Summary Health Information is De-identified Information except that a 5-digit zip code may be included (see Section 1);

2. **Participation and Enrollment:** The disclosure of PHI consisting of information on whether an individual is participating in a Plan, is enrolled in a Plan, or has disenrolled from a Plan.

3. **Other Plan Administration Disclosures:** The disclosure of PHI to the Plan Sponsor for plan administration functions, provided that the applicable Plan's documents have been amended to (a) establish the permitted and required uses and disclosures by the Plan Sponsor (which must be consistent with the HIPAA Rules); (b) provide that the Plan will disclose PHI to the Plan Sponsor only upon receipt of a certification by the Plan Sponsor that the plan documents have been amended to incorporate restrictions required by the HIPAA Rules; and (c) provide for an adequate separation between the Plan and the Plan Sponsor consistent with the HIPAA Rules. As used herein, "plan administration functions" mean administration functions performed by the Plan Sponsor on behalf of a Plan and exclude functions performed by the Plan Sponsor in connection with any other benefit or benefit plan of the Plan Sponsor.

   The Plans' documents have been amended to address the above requirements. A Plan may disclose PHI to the Plan Sponsor to carry out plan administration functions (subject to Section 4(F)). A Plan shall not permit its TPA or any health insurance issuer with respect to the Plan to disclose PHI to the Plan Sponsor except as permitted by this Section 4(G)(3). A Plan shall not disclose, or permit its TPA or any health insurance issuer to disclose, PHI to the Plan Sponsor unless the Notice includes a statement that such disclosure may occur (see Section 3(E)). A Plan shall not disclose PHI to the Plan Sponsor for employment-related actions or decisions or in connection with any other benefit or employee benefit of the Plan Sponsor (unless authorized by the Participant).

Section 5. Verification

Before releasing PHI (when permissible as set forth in Section 4), a Plan will verify the identity and legal authority of any person requesting PHI if such person is not already known to the Workforce Member handling the request. Such verification will comply with the following:

- *Identity of Public Officials.* In verifying the identity of a public official or a person acting on behalf of the public official requesting disclosure of PHI, the Plan may rely on the following, if such reliance is reasonable under the circumstances:
    - Presentation of an agency identification badge, other official credentials, or other proof of government status if the request is made in person;
    - A written statement on appropriate government letterhead that the person is acting under the government's authority; and

- Other evidence or documentation from an agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

- *Authority of Public Officials.* In verifying the authority of a public official or a person acting on behalf of the public official requesting disclosure of PHI, the Plan may rely on the following, if such reliance is reasonable under the circumstances:
  - A written statement of the legal authority under which the information is requested;
  - If a written statement would be impracticable, an oral statement of such legal authority; and
  - A request that is made pursuant to a warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal that is presumed to constitute legal authority.
- *Identity of Other Requestors (Including Personal Representatives).* The Plan will make reasonable efforts to verify the identity of Participants or others requesting PHI. Such efforts may include, as applicable, requesting identification (i.e., a driver's license, passport or similar ID) and requesting the Participant's health plan number/member ID or other information that can be verified in the Plan's records (i.e., address or home phone). If a Personal Representative is making the request, the Plan will also make reasonable efforts to verify that the individual is, in fact, the named Personal Representative, using the methods listed above or other common sense methods of verifying identity.
- *Authority of Other Requestors (Including Personal Representatives).* The Plan will make reasonable efforts to verify the authority of those requesting PHI. The Participant has authority to access his or her own PHI. For other requestors, the Plan will obtain documentation of the requestor's authority. The Plan must obtain any authorization, documents, statements, or representations, whether oral or written, from the person requesting the PHI required by these Policies and Procedures. Documents, statements or representations that are valid on their face may be reasonably relied upon by the Plan.
- *Additional Requirement for Personal Representatives/Deceased Participants.* In the case of Personal Representatives, the Plan should request a copy of the power of attorney, guardianship or other authority, as applicable. In the case of deceased Participants, appropriate documentation includes letters testamentary or court orders recognizing an individual as the executor or other representative of the estate.

Section 6: Business Associates

1. In General. Before allowing any Business Associates to create, receive, maintain or transmit PHI on behalf of a Plan, the Plan will enter into a Business Associate Agreement that establishes the permitted and required uses and disclosures of PHI by the Business Associate and contains all additional provisions required by the HIPAA Rules. The Privacy Officer will review Business Associate Agreements proposed by vendors of the Plan or any changes to the Plan's form requested by vendors prior to the Plan agreeing to them. Whenever possible, the Plan will use its form Business Associate Agreement, which is attached as Exhibit A.

2. Required Components of Business Associate Agreement. The following items are required elements of a Business Associate Agreement (a "BAA"):

i. Requiring the Business Associate to only use or disclose PHI in accordance with the BAA or as required by law. The services and duties of the subcontractor or agent must either be specified in an underlying service agreement or in the BAA.

ii. Requiring the Business Associate to maintain appropriate administrative, technical and physical safeguards to protect the confidentiality of PHI and to comply with the applicable provisions of 45 CFR Part 164, Subpart C of the HIPAA Rules with respect to electronic PHI to prevent any use or disclosure of such information other than as provided by the BAA.

iii. Requiring the Business Associate, to the extent that the Business Associate is to carry out an obligation of the Plan under the HIPAA Rules, to comply with the requirements of the HIPAA Rules that apply to the Plan in the performance of such obligation.

iv. Requiring the Business Associate to report non-permitted uses and disclosures, security incidents and breaches to the Plan.

v. Requiring the Business Associate to obligate agents and subcontractors that create, receive, maintain or transmit PHI on behalf of the Business Associate to agree in writing to be bound by the same restrictions and conditions that apply to the Business Associate with respect to such PHI.

vi. Requiring the Business Associate to make PHI available and to amend PHI to satisfy the patient rights provisions of the HIPAA Rules. If the requested PHI is maintained electronically, the Business Associate must provide a copy of the PHI in the electronic form and format requested by the individual, if it is readily producible, or, if not, in a readable electronic form and format as agreed to by the Plan and the individual.

vii. Requiring the Business Associate to document disclosures required to be reported under the accounting obligation and to provide such documentation to the Plan.

viii. Requiring the Business Associate to provide access to its internal practices, books and records to HHS for purposes of determining compliance with the HIPAA Rules.

ix. Requiring the Business Associate to return or destroy all PHI upon termination of the BAA, if feasible, and to continue to abide by the BAA with respect to any PHI that is infeasible to return or destroy and only use and disclose retained PHI for purposes that make return or destruction infeasible.

x. Authorizing termination of the BAA if the Business Associate violates a material term of the BAA.

xi. Any other items required by the HIPAA Rules, as may be amended from time to time.

The BAA may also expressly address other items such as the minimum necessary standard, restrictions on the use or disclosure of PHI for marketing or fundraising, prohibitions on the sale of PHI, that the Business Associate may be subject to the penalty provisions of the HIPAA Rules and that either party may report the other to HHS if the other party breaches and termination is not feasible.

In the event a Plan knows of a pattern of activity or practice of a Business Associate that constitutes a material breach or violation of the Business Associate's obligations under the applicable BAA or the HIPAA Rules, the Plan will take reasonable steps to cure the breach or end the violation. If such steps are unsuccessful, the Plan will terminate the arrangement with the Business Associate, if feasible. In the event termination is not feasible, the Plan may report the problem to HHS.

Section 7: <u>De-Identification of PHI</u>

A Plan may use PHI to create information that is de-identified in compliance with the HIPAA Rules. When practicable, de-identified information will be used and disclosed. Information is de-identified if it meets the definition of De-Identified Information as set forth in Section 1.

A Plan may assign a code or other means of record identification to allow de-identified information to be re-identified by the Plan provided that: (1) the code or other means of record identification is not derived from or related to information about the Participant and is not otherwise capable of being translated so as to identify the Participant; and (2) the Plan does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

Section 8: <u>Minimum Necessary Standard</u>

This Section 8 does <u>not</u> apply to (1) disclosures to or requests by a health care provider for treatment; (2) uses or disclosures made to the Participant; (3) uses or disclosures made pursuant to an authorization; (4) uses or disclosures required by law; and (5) uses or disclosures that are otherwise required to comply with the HIPAA Rules.

For uses, disclosure and requests subject to this Section 8, when practicable, a Plan will limit is uses, disclosures or requests of PHI to PHI making up a Limited Data Set. When a Limited Data Set is not practicable, a Plan will make reasonable efforts to limit the PHI used, disclosed or requested by the Plan to the minimum necessary required to accomplish the intended purpose of the use, disclosure or request. Accordingly, a Plan will identify those individuals or classes of individuals who are Workforce Members who need access to PHI to carry out their duties and for each such person or class of persons, the category or categories of PHI to which access is needed

and any conditions appropriate to such access. The Plans currently handle a small amount of PHI since its TPA handles most functions of the Plan.

For any disclosure or request for PHI that a Plan makes on a routine and recurring basis, the Plan will implement procedures that limit the PHI disclosed or requested to the amount reasonably necessary to achieve the purpose of the disclosure or request. For all other disclosures or requests for PHI, the Plan will review the disclosures or request for PHI on an individual basis in accordance with the following criteria: (1) what is the purpose of the request or disclosure? (2) what type of PHI is needed for this purpose? (3) how important is the need for the PHI (versus De-Identified Information)? (4) are there reasonable alternatives to requesting PHI? (5) is the request or disclosure limited to the scope of PHI needed for the purpose of the disclosure or request? and (6) any other relevant factors specific to the request or disclosure.

A Plan may reasonably rely on a requested disclosure as the minimum necessary for the stated purpose when:

- making disclosures to public officials (if the public official represents that the information requested is the minimum necessary for the stated purpose);
- the information is requested by another covered entity under the HIPAA Rules;
- the information is requested by a professional who is a Business Associate of the Plan for the purpose of providing professional services to the Plan, provided the professional represents that the information requested is the minimum necessary for the stated purpose; or
- documentation or representations that comply with the applicable requirements have been provided by a person requesting the information for research purposes.

A Plan will not use, disclose or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

Section 9: Marketing and Sale of PHI

An authorization that complies with Section 4(E) (including a statement regarding remuneration, if applicable) is required in order to use or disclose PHI for marketing or to sell PHI. However, there are exceptions to what is considered marketing or the sale of PHI as described below. Prior to using or disclosing PHI for marketing, selling PHI or engaging in any activities that may be fairly considered to be using or disclosing marketing or selling PHI, Workforce Members will consult with, and receive the approval of, the Privacy Officer.

A. Marketing

The HIPAA Rules prohibit the use or disclosure of PHI for marketing purposes without an authorization, with limited exceptions. The Privacy Officer will confirm that the applicable requirements set forth in the HIPAA Rules are met before approving a use or disclosure of PHI for marketing purposes.

"Marketing" means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. It does not include the following communications:

1. face-to-face communications made by a Plan to a Participant;

2. a promotional gift of nominal value provided by a Plan;

3. communications to provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any remuneration received by a Plan in exchange for making the communication is reasonably related to the Plan's cost of making the communication;

4.. if no remuneration is received by a Plan, communications for treatment of the Participant, including case management or care coordination for the Participant, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual;

5. if no remuneration is received by a Plan, communications to describe a health-related product or service (or payment for such product or service) that is provided by the Plan, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, the Plan; and health-related products or services available only to the Participant that add value to, but are not part of, the Plan's benefits; and

6. if no remuneration is received by a Plan, communications for case management or care coordination, contacting of Participants with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of "treatment" (see Section 4(A)).

As outlined in Section 4(E), in the event the marketing involves financial remuneration to the Plan from a third party, the authorization provided by the Plan to the Participant for signature will include a statement that such remuneration is involved. For purposes of the definition of "Marketing," the term *financial remuneration* means direct or indirect payment from or on behalf of a third party whose product or service is being described. It does not include any payment for treatment of an individual (i.e., payment by the Plan to a provider as payment for health care services provided to Participants).

B. Sale of PHI

A Plan must obtain an authorization before selling PHI. As outlined in Section 4(E), the authorization must include a statement that the disclosure will result in remuneration to the Plan. The "Sale of PHI" is defined as any disclosure of PHI where the Plan or its Business Associate receives, directly or indirectly, remuneration (i.e., anything of value) from or on behalf of the recipient of the PHI in exchange for the PHI, except for the following disclosures: (1) for public health purposes under the public health exception or pursuant to the Limited Data Set rules (see Section 4(D)); (2) for research purposes (see Section 4(D)) pursuant to the research exception or

the Limited Data Set rules if the only remuneration received is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI for such purposes; (3) for treatment and payment purposes (see Section 4(A)); (4) for the sale, transfer, merger or consolidation of all or part of the Plan and for related due diligence as permitted by the definition of *health care operations* (see Section 4(A)); (5) to or by a Business Associate for activities that the Business Associate undertakes on behalf of the Plan and the only remuneration provided is by the Plan to the Business Associate for the performance of such activities (see Section 6); (6) to an individual when requested under the access or accounting provisions of the HIPAA Rules (see Section 3(A) and Section 3(C)); (7) required by law (see Section 4(D)); (8) as otherwise permitted by and in accordance with the applicable requirements of the HIPAA Rules (see Section 3 and 4) where the only remuneration received by the Plan or its Business Associate is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for such purpose or a fee otherwise expressly permitted by other law.

Section 10: Complaints/Responding to Instances of Non-Compliance/Training and Other Administrative Provisions

A. Policies and Procedures

The Plans have established these Policies and Procedures that implement the requirements of the HIPAA Rules. The Privacy Officer and Security Officer will review these Policies and Procedures periodically, and revise these Policies and Procedures as needed, in response to environmental, legal or operational changes affecting PHI and EPHI. The Privacy Officer or Security Officer shall disseminate all official updates to policies and procedures to affected Workforce Members and make all pertinent documentation available to those individuals responsible for implementing the policies and procedures.

B. Training

The Plans will train all Workforce Members on these Policies and Procedures. The Plans will provide such training (1) to each new Workforce Member within a reasonable period of time after the person becomes a Workforce Member; and (2) to each Workforce Member whose functions are affected by a material change in these Policies or Procedures, within a reasonable period of time after the material change becomes effective.

The Privacy Officer will ensure that the above training is provided, except that the Security Officer is responsible for ensuring that Workforce Members receive security awareness training regarding EPHI, that will include, at a minimum, the following topics: (1) overall discussion of threats and vulnerabilities specific to EPHI; (2) security incident reporting; (3) viruses and other forms of malicious software; (4) user log-in; and (5) password management. The Security Officer will periodically send out security reminders to make the Workforce Members aware of security concerns and initiatives.

The Plans will document the training described in these Policies and Procedures, including training materials used and evidence of attendance/completion. The Plans will maintain training documentation for a period of no less than 6 years from the date the documentation was created.

C. Non-compliance/Complaints

Any Workforce Member who witnesses, suspects or knows of a non-permitted use or disclosure of PHI, a Security Incident or a Breach or any violation or breach of these Policies and Procedures must immediately report the incident to the Privacy Officer, or in the case of Security Incidents, the Security Officer. The applicable Plan will investigate the matter and take appropriate action.

Any complaints from a Participant regarding the privacy or security of PHI will be forwarded immediately to the Privacy Officer, who will notify and coordinate, when appropriate given the nature of the complaint, with the Security Officer. All complaints will be investigated by the Plan as described above. Complaints will be kept confidential to the maximum extent possible.

Appropriate steps consistent with Sections 10(D) and 24 and corrective actions will be taken in response to any Security Incidents or instances of non-compliance. The Privacy Officer or Security Officer, as appropriate, will document all complaints, known Security Incidents and reports of potential non-compliance and their resolution.

If a Plan determines that a Workforce Member has violated these Policies and Procedures, appropriate disciplinary action will be taken against the offending staff member, up to and including termination of employment consistent with the human resources policies of Ryman as Plan Sponsor. The type of sanction applied shall vary depending on the severity of the violation, whether the violation was intentional or unintentional, whether the violation indicates a pattern or practice of improper use or disclosure of PHI, and any other relevant factors. The Plan will document sanctions imposed upon a Workforce Member.

The Plans specifically prohibit any form of retaliation against any Workforce Member or Participant for filing a bona fide complaint under these Policies and Procedures or for assisting in a compliance investigation. A Plan may, however, take action against a Workforce Member or Participant who filed a complaint if, after investigating the complaint, the Plan determines the complaint was not made in good faith or that the individual provided false information regarding the complaint.

D. Mitigation

If any Workforce Member becomes aware that any harmful effect has or may occur as the result of a use or disclosure of PHI in violation of these Policies and Procedures, such individual shall report the occurrence to the Privacy Officer. The Privacy Officer shall investigate the report and to the extent practicable take such actions as he/she deems necessary to mitigate the harmful effect. All actions of mitigation shall be documented by the Privacy Officer. Where applicable (see Section 11), mitigation will include providing notice to affected Participants and other parties required by law.

The Security Officer will take immediate action to minimize the impact of any Security Incident and to determine the cause of the incident as set forth in Section 24.

Section 11: Breach Notification

A Plan will notify affected Participants (and others as described below) of any Breach of Unsecured PHI as discussed in more detail below.

A. Exceptions/Incidents Not Requiring a Report

Incidents that fall into one of the categories below are not required to be reported pursuant to this Section 11 (unless state law requires a report). However, Workforce Members must always report to the Privacy Officer any incident believed to be a violation of these Policies and Procedures so that the Privacy Officer can determine whether the incident is a Breach and whether corrective actions or other measures should be taken in response to the incident.

1. *Breach Exceptions*. If any of the following exceptions apply, the incident is not a Breach.

    - Certain unintentional uses. Any unintentional acquisition, access, or use of PHI by a Plan, Workforce Members or any individual acting under the authority of the Plan or its Business Associate if:
        - the acquisition, access, or use was made in good faith and within the course and scope of authority; and
        - the information is not further used or disclosed in a manner not permitted by the HIPAA Rules.
    - Certain inadvertent disclosures. Any inadvertent disclosure by a person who is authorized to access PHI at a Plan or its Business Associate to another person authorized to access PHI at the Plan or the same Business Associate, if the information received as a result of the disclosure is not further used or disclosed in a manner not permitted by the HIPAA Rules.
    - Incidents involving no ability to retain the PHI. A disclosure of PHI where a Plan or its Business Associate has a good faith belief that the recipient would not reasonably have been able to retain the information (such as an envelope that is incorrectly addressed and is returned unopened as undeliverable by the U.S. Post Office).

2. *Low probability that the information has been compromised.* Except for the categories listed above, an acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA Rules is presumed to be a Breach unless the applicable Plan can demonstrate that there is a low probability that the PHI has been compromised. In order to make this determination, the Plan will perform, and document the outcome of, a risk assessment taking into account at least the following factors:

    i. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

    ii. The unauthorized person who used the PHI or to whom the disclosure was made;

    iii. Whether the PHI was actually acquired or viewed; and

    iv. The extent to which the risk to the PHI has been mitigated.

B. Determination of Breach/Reports

All employees, officers and agents of a Plan must report any incidents believed to be Breaches or non-permissible uses or disclosures of PHI to the Privacy Officer as soon as possible. The Privacy Officer will review all incident reports received from employees, agents, Business Associates or others promptly to determine: (i) whether the reported use or disclosure was permissible under the HIPAA Rules; (ii) if not, whether the incident constitutes a Breach; and (iii) if the incident is a Breach, how to properly report the Breach under this Section 11; and if the incident is not a Breach, whether the incident requires a report under state or other law (for example, state laws may apply to personal information that is not considered to be PHI).

If the Privacy Officer concludes that a Breach has occurred, each affected Participant will be notified without unreasonable delay, but no longer than 60 days from the discovery of a Breach. A Breach is considered to be discovered on the first day that the Plan (or any of its agents or Workforce Members who did not themselves commit the Breach) knows of the Breach or would have known of it by using reasonable diligence.

The Plans will also comply with any applicable state law requirements that impose additional breach notification duties or more restrictive breach obligations (for example, state law may require a report to be made within a shorter period, that the notice letter contain specific wording not required by the HIPAA Rules, or that additional government agencies or other entities be notified).

If the Breach involves more than 500 residents of a State or jurisdiction, the applicable Plan will notify prominent media outlets serving the State or jurisdiction without unreasonable delay, but no longer than 60 days from the discovery of a Breach. In addition, (1) if the Breach involves 500 or more Participants, the Plan will notify HHS without unreasonable delay, but no longer than 60 days from the discovery of a Breach; or (2) if the Breach involves fewer than 500 Participants, the Plan will maintain a log or other documentation of the Breaches and, not later than 60 days after the end of each calendar year, notify HHS of the Breaches discovered during the previous calendar year.

A Plan must delay notification to affected Participants of a Breach if a law enforcement official states that notification would impede a criminal investigation or cause damage to national security as follows: (i) if the law enforcement statement is in writing, the Plan will delay the notification or posting for the time period specified in the statement; or (ii) if the law enforcement statement is made orally, the Plan will delay the notification or posting for the time period requested or for 30 days, whichever time period is shorter. If the law enforcement official confirms an oral statement with a written request to delay notification or posting, the Plan will delay the notification or posting for the time period specified in the written statement.

C. Content of Notice Required

Notification to affected Participant(s) and the media (when required) will include: (i) a brief description of what happened including the date of the Breach and the date of the discovery of the Breach; (ii) a description of the types of Unsecured PHI that were involved in the Breach; (iii) any steps Participants should take to protect themselves from potential harm resulting from the Breach;

(iv) a brief description of what the Plan is doing to investigate the Breach and to mitigate harm to Participants; and (v) contact procedures for Participants to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address. Notification to HHS will include the items requested on HHS's website.

D. Method of Notice

A Plan will notify affected Participants by first-class mail at the last known address of the Participant or, if the Participant agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available. If the Plan knows the Participant is deceased and has the address of the next of kin or Personal Representative of the Participant, the Plan may provide such written notice to the next of kin or Personal Representative.

If there is insufficient or out-of-date contact information for a Participant, the Plan will use a substitute form of notice reasonably calculated to reach the Participant. If there is insufficient or out-of-date contact information for fewer than 10 Participants, the substitute notice may be provided by an alternative form of written notice, telephone, or other means. If there is insufficient or out-of-date contact information for 10 or more Participants, the substitute notice will: (1) be in the form of either a conspicuous posting for a period of 90 days on the Plan's website or conspicuous notice in major print or broadcast media in geographic areas where the Participants affected by the breach likely reside; and (2) include a toll-free phone number that remains active for at least 90 days where an Participant can learn whether the Participant's Unsecured PHI may be included in the Breach.

E. Documentation of Breaches

Incident reports, their resolution, assessments of harm and whether an incident was a Breach, copies of notices provided to Participants, the media and HHS and all other information required to be kept by this Section 11 will be documented and retained as described in Section 12. Attached as Exhibit A is a Breach Investigation Record that should be used to record the investigation of incidents believed to be Breaches or non-permissible uses or disclosures of PHI.

Section 12: Documentation

The Plans will maintain documentation, in written or electronic form, of these Policies and Procedures and all other communications and other documents required by the HIPAA Rules (such as signed Business Associate Agreements, authorization forms, documentation of complaints and their resolution and the Notice) for a period of at least 6 years from the date of creation or the effective date of the document, whichever is later.

Section 13: Safeguards and Adequate Separation

A Plan shall use reasonable safeguards to protect PHI from any intentional or unintentional use or disclosure that is in violation of these Policies and Procedures and the HIPAA Rules. Such safeguards shall be consistent with and in addition to the safeguards outlined in Sections 14 through 24 for EPHI. A Plan will safeguard the confidentiality of PHI in paper form by, among

other things, shredding documents that contain PHI prior to discarding and locking file cabinets that contain PHI when not in use. Workforce Members will not hold phone conversations or other discussions involving PHI in areas where unauthorized persons may overhear. Phone conversations involving PHI should not be held on speakerphone, unless everyone within listening distance is an authorized recipient of the PHI. A Plan will limit the amount of PHI disclosed when leaving a voice mail, message on an answering machine or other message to as little PHI as possible. Workforce Members will take reasonable steps to send and receive facsimile transmissions securely, including double checking fax numbers, locating fax machines in secure areas, using a cover sheet with a confidentiality statement and not leaving faxes on the fax machine.

Workforce Members of a Plan may access PHI to the extent necessary to perform Plan administration functions that Ryman as Plan Sponsor performs for the Plan. Other employees of Ryman may not access PHI from or on behalf of the Plan unless an authorization that complies with Section 4(E) is received or such access is otherwise expressly permitted by these Policies and Procedures. A Plan will maintain adequate controls to protect PHI from access by employees of the Plan Sponsor who are not Workforce Members of the Plan or are not otherwise authorized to access such information.

Section 14: Security of EPHI Generally

In addition to complying with the safeguard requirements specified in Section 13, a Plan will (1) maintain appropriate and reasonable safeguards to protect the confidentiality, integrity and availability of all EPHI it creates, receives, maintains or transmits; (2) take reasonable measures to protect against any reasonably anticipated threats or hazards to the confidentiality, availability or integrity of EPHI; (3) take reasonable measures to protect against any reasonably anticipated uses or disclosures that are not permitted by these Policies and Procedures; and (4) require compliance with these Policies and Procedures by all Workforce Members.

Determinations of reasonable security measures will be based on the size, complexity and capabilities of the Plan, the infrastructure, hardware and software security capabilities of the Plan, the costs of security measures and the probability and criticality of potential risks to EPHI.

A Plan will periodically review technical and non-technical security measures implemented pursuant to these Policies and Procedures and documentation created pursuant to these Policies and Procedures. The Plan will revise such measures, documentation and these Policies and Procedures as necessary to continue to provide reasonable and appropriate protection of EPHI in light of environmental, legal and operational changes. Environmental and operational changes include the following: (1) significant security incidents; (2) significant new threats or risks to the Plan's information systems; (3) significant reorganization of the Plan; and (4) significant changes to the Plan information systems or information security responsibilities. Evaluation(s) of the Plan's security measures will include consideration of the steps outlined in the risk analysis process performed pursuant to Section 15, and the Security Officer will update the Plan's risk analysis as necessary upon completion of a security evaluation.

Section 15: Security Management and Risk Analysis

A. In General

The Plans will maintain a process, including the processes described below, to identify security risks and to prevent, detect, contain and correct security violations. This process will include training of Workforce Members as described in Section 10, properly handling and responding to Security Incidents as described in Section 10 and regular evaluation of the Plans' security policies, procedures and controls as described in Section 14.

B. Risk Analysis

The goal of risk analysis is to identify, define and prioritize risks to the confidentiality, integrity and availability of the Plans' systems that contain EPHI. The Plans have conducted a survey of all computer and information systems in order to determine (1) where EPHI is stored; (2) how EPHI is transmitted; (3) which Workforce Members have access to EPHI; (4) what types of information are stored on each system and the criticality of such information; (5) threats and vulnerabilities to information systems containing EPHI; (6) existing security measures; (7) the likelihood that a given threat could exploit a vulnerability on a Plan system containing EPHI; (8) the potential impact of a threat occurrence; (9) the level of risk to EPHI; and (10) security measures that can be used to reduce risk to a reasonable and appropriate level. This process is referred to in these Policies and Procedures as a risk analysis or risk analysis process. The risk analysis process will be repeated for new equipment, information systems and computer systems that are installed and will be updated as necessary in light of environmental and operational changes, as specified in Section 14. Documentation of the risk analysis will be maintained by the Security Officer.

C. Risk Management

The Plans will implement security measures that reduce the risks to its information systems that contain EPHI to reasonable and appropriate levels in light of the size, complexity and capabilities of the Plan; its technical infrastructure, hardware and software security capabilities; the costs of security measures; and the probability and criticality of potential risks to EPHI. The Plans' risk management process will include assessing and prioritizing risks to its information systems (see Risk Analysis discussion above); selecting and implementing reasonable and appropriate security measures; providing training to the Plans' employees and evaluating and revising its security measures consistent with Section 14, which may include revising these Policies and Procedures.

D. Audit Controls/Information System Activity Review

The Plans will regularly review records of information system activity, such as audit logs, access reports and Security Incident reports (see Sections 10 and 24) in order to determine whether any EPHI has been used or disclosed inappropriately.

Information system activity reviews will be structured in light of the Plans' risk analysis and risk management program, considering the capabilities of all information systems with EPHI and the audit controls implemented as described below. To the extent consistent with the capabilities of the Plans' information systems, activity reviews will include information regarding the date and time of activity on the system; the origin of the activity; an identification of the user performing the activity and a description of the attempted or completed activity. The Plans will review

periodically information system activity logs and review daily e-mail traffic, web traffic and firewall traffic. The Security Officer is responsible for overseeing information system activity reviews. Whenever possible, Workforce Members (including the Security Officer) should not monitor or review activity related to their own accounts.

The Plans shall maintain appropriate technical audit controls that record activity in Plan information systems that contain EPHI and allow for the examination of such activity. The Security Officer shall identify existing hardware, software and/or procedural audit controls that record activity in the Plans' information systems that contain EPHI.

The Security Officer shall examine any proposed hardware or software purchases to confirm that the new items contain appropriate technical audit controls to allow the recording and examination of information system activity consistent with the risk analysis process (see Risk Analysis discussion above).

Section 16: Information Access Management, Workforce Security and Authorization of Access

A. In General

The confidentiality and integrity of data stored on company computer systems must be protected by administrative and technical access controls to ensure that only authorized Workforce Members have access. This access shall be restricted to only those capabilities that are appropriate to each Workforce Member's job duties, while permitting Workforce Members to access the EPHI that is minimally necessary to perform their job functions. Such measures shall include reasonable technical measures to verify that a person or entity seeking access to EPHI is the one claimed and take into account that most EPHI held by the Plans is stored at the TPAs and not readily accessible to Workforce Members.

B. Authorization/Clearance

For each Workforce Member or job position, the employee's supervisor will determine what EPHI is needed and when access to EPHI is needed. Authorized access to EPHI will be limited to the minimum amount of EPHI needed for each Workforce Member (or job position) to perform his or her job functions. This determination of access shall be consistent with the minimum necessary requirements of Section 8.

Workforce Members are only permitted to access EPHI for which they have received authorization from their supervisors. If a Workforce Member needs temporary access to EPHI that the Workforce Member has not been authorized to access to perform a job function, the Workforce Member must receive prior approval from the Privacy Officer or Security Officer to access the EPHI. The Privacy Officer or Security Officer must define the type and length of the temporary access. Before approving temporary access, the Privacy Officer or Security Officer must confirm that the Workforce Member has a legitimate need to temporarily access the EPHI or assign the job function to another Workforce Member with appropriate access.

For newly-hired Workforce Members, the Security Officer will identify and define the security responsibilities and level of access required and permitted for the position.

C. Authentication/Control of Access

Potential authentication methods include the following: (1) requiring something known only to the individual, such as a password or PIN; (2) requiring something that individuals possess, such as a smart card, a token or a key; or (3) requiring something unique to the individual such as biometrics (i.e., fingerprints, voice patterns, facial patterns). The Security Officer shall determine the mechanisms used for authenticating access to EPHI based on the risk analysis process performed pursuant to the Section 15. Currently, the Plans use the following authentication method: assigning unique passwords to each authorized user and assigning a unique user identification as specified below.

Each Workforce Member or other individual authorized to access the Plans' systems containing EPHI shall be assigned a unique name and/or number so that users of the Plans' systems may be tracked and identified. The Security Officer shall determine the format of the unique user identification used for each system. In addition to the unique user identification, each Workforce Member shall be assigned or shall select a secret identifier (password) consistent with Section 17.

The Security Officer shall oversee the use of physical access controls as specified in Section 20 to assure that Workforce Members have only authorized access to EPHI.

D. Modification/Termination of Access

Access rights must be regularly reviewed and revised by the Security Officer as necessary to allow appropriate access and prevent inappropriate access. If a Workforce Member's job functions change, the Security Officer must review the Workforce Member's authorized access to EPHI and take appropriate measures to revise such access if necessary in light of the Workforce Member's revised job function.

Upon termination of a Workforce Member, the Workforce Member's supervisor must notify the Security Officer of the termination immediately (and with advance notice, if possible). The Security Officer must take appropriate steps to terminate the Workforce Member's access to EPHI, including access through or to workstations, servers, e-mail accounts, inclusion in bulk e-mail lists, by disabling or deleting the Workforce Member's passwords and taking any other additional reasonable steps.

Upon termination or other departures of a Workforce Member, the Security Officer is responsible for notifying appropriate Workforce Members of the termination so that the terminated individual is not mistakenly granted access to the Plans' facilities or systems. The terminated individual must return all identification badges and all keys, keycards, or other means of gaining access to the Plans' facilities. The Security Officer is responsible for verifying that these items have been returned and taking appropriate actions if unable to verify their return, such as notifying other

Workforce Members that the terminated individual may still have a badge or other means of access and should be denied access. If the Plans use security access codes and the terminated individual is aware of these codes, the Security Officer must confirm that the codes are deactivated or changed.

Upon termination or other departure of a Workforce Member, the terminated individual must return any portable/laptop computers, personal digital assistants or other equipment belonging to the Plan. The Security Officer is responsible for verifying that these items have been returned and taking appropriate actions if unable to verify their return.

E. Log-in Monitoring

The Plans will maintain reasonable processes to monitor log-in attempts and respond appropriately to log-in discrepancies. The Plans' log-in process includes measures to assure a secure log-in process, such as not providing help messages during the log-in process that would assist an unauthorized user.

The Plans' log-in process will be configured to identify multiple unsuccessful log-in attempts and automatically lock out any account that has had the wrong password input 6 times. Lockout will be automatically lifted after 30 minutes or, if required, when an administrator re-enables the user ID. The Security Officer will investigate detected improper log-in attempts consistent with Section 10(C).

Section 17: Password Management

It is the policy of the Plans for unique passwords to be set up for all workstation and server access and, as determined to be appropriate, for applications. Passwords will be initially assigned for new users and will be changed upon first use. Workforce Members must safeguard their passwords to protect the security of EPHI and the information systems of the Plans.

Passwords must be a minimum of 8 letters, at least one uppercase letter and one lowercase letter, at least one digit (0-9) or special character ($, @, # and so on). Passwords should not be names or words from the dictionary or consist of previously used passwords. Passwords should be easy to remember and should never be written down on notes in accessible places. Some passwords may be written down and secured by information technology Workforce Members due to the requirement of alternate access.

Passwords will be changed periodically at least every 90 days. This is enforced at the server level. The system will remember old passwords to enforce adequate password changes. If the Plan is required to change a password, a message will be left on voice mail for the Workforce Member and then the password reset to a temporary password.

Each Workforce Member shall be responsible for all computer transactions made with his/her User ID and password. Workforce Members shall not disclose passwords to others. Workforce Members must change their password and notify the Security Officer immediately if they have reason to believe that another individual knows his or her password. Passwords should not be recorded where they may be easily obtained. Workforce Members will change passwords when the system requests the change and should use passwords that will not be easily guessed by others. Workforce Members should log out or lock the screen when leaving a workstation.

Section 18: Protection from Malicious Software and Unauthorized Access

The Plans will maintain reasonable processes to guard against, detect and report malicious software and unauthorized access. Workforce Members must protect the Plans' systems from malicious software by complying with software use and installation policies and reporting known or suspected instances of malicious software to the Security Officer.

Workforce Members may not install software on the Plans' systems without the prior approval of the Security Officer or Desktop Services. Similarly, any materials residing on USB flash drives, magnetic or optical media, and all material downloaded from the Internet or from computers or networks that do not belong to a Plan must be pre-scanned for viruses and other destructive programs. Workforce Members may not modify web browser security settings without the prior approval of the Security Officer.

All computers and servers are protected with antivirus software. The Information Technology Department, working with the Security Officer, will ensure that all such software is provisioned to allow for updates as soon as practical to ensure adequate protection. Workforce Members may not bypass or disable anti-virus software without the prior approval of the Security Officer.

Workforce Members must use extreme caution when opening attachments associated with personal e-mail, since such attachments often spread viruses, and must not open e-mail attachments or click on any hyperlink contained in an email from senders they do not know.

As determined appropriate by the Security Officer in light of the risk analysis process performed pursuant to Section 15, the Plans shall maintain appropriate technical safeguards, which may include encryption, to prevent access by persons or software programs that have not been granted access rights.

Section 19: Contingency Plans and Data Back-Up

The Plans will develop, document and implement, as necessary, strategies for recovering access and protecting EPHI in the event of an emergency or other disruption of critical business operations. The Security Officer currently assumes responsibility for Information Systems and the network. The Security Officer will ensure that processes are in place to allow for restoration of business in the event of a disaster affecting the Plans' networks. In most cases, EPHI will be restored by contacting the TPA.

A. Applications and Data Criticality Analysis

In conjunction with its risk analysis process performed pursuant to Section 15, the Security Officer will regularly analyze the criticality of the Plans' information systems. The Security Officer will oversee the identification of all software applications that store, maintain or transmit EPHI and the determination of how important each is to the Plans' needs. The applications and data criticality analysis will assist the Plans in prioritizing data backup, disaster recovery and emergency operations plans. It will take into account the amount of duplicate EPHI held by the TPA.

For instance, some systems must be available at all times, while others are less critical and could be down for a certain period without significant disruption to the Plans' operations. Among the items to be considered when performing the applications and data criticality analysis are:

a. identification of dependencies between the applicable Plan's information systems;

b. identification of the impact of identified risks on the applicable Plan's operations;

c. identification of estimated maximum time periods for which information systems can be unavailable.

B. Data Backup Plan/Disaster Recovery

Data backups of EPHI are performed consistently with Ryman's general data back-up policies. The Security Officer is responsible for confirming that data backup is occurring consistent with the needs of the Plans and considering the amount of duplicate EPHI held by the TPA. The Security Officer will ensure that backups are properly stored.

The Plans maintain a disaster recovery plan to allow recovery of its operations in the event of a disaster the impacts the Plans' systems containing EPHI. The Security Officer will oversee the recovery of EPHI in such event. The disaster recovery plan may utilize where appropriate the Plan Sponsor's general disaster recovery plan. It will include the following items: (1) the conditions for activating the plan; (2) a description of the actions to be taken to return the Plans' systems to normal operations; (3) the order in which information systems will be recovered, in light of the application and data criticality analysis; and (4) a list of key individuals, their contact information and their responsibilities.

Copies of the disaster recovery plan must be kept at more than one location and distributed to appropriate Workforce Members as determined by the Security Officer.

C. Emergency Access/Emergency Mode Operation Plan

The Plans do not anticipate the need for access for the purpose of emergency mode operations. Emergency mode operations typically relates to the need of clinicians needing access to PHI in an emergency. If such need arises, the request should be forwarded to the Security Officer who will balance the need to protect EPHI with the need to access EPHI during an emergency or other crisis and the information held by the TPA.

D. Testing and Revision of Contingency Plan

The Security Officer will oversee the regular testing of each aspect of the contingency plan. The Security Officer has authority to select the most appropriate method of testing, which may range from "paper" walk-throughs of each plan to live tests. Among the items to be considered by the Security Officer are the following items: (1) are the processes for restoring data from backups, disaster recovery and emergency mode operations adequately documented? (2) do the individuals responsible for performing contingency plan tasks understand their responsibilities? and (3) have the results of the testing been analyzed?

The Security Officer will also periodically review the contingency plan and update the contingency plan as needed in the event of significant changes, such as significant changes in Workforce Members, the TPA or the Plans' technical or physical infrastructure, and threats to its information systems as identified through the risk analysis process performed pursuant Section 15.

Section 20: <u>Facility Access Controls</u>

The Plans maintain physical measures, policies and procedures to protect EPHI from natural and environmental hazards and unauthorized intrusion, while permitting properly authorized access to its information systems and facilities consistent with Section 16.

The Plans maintain a physical security plan that documents the physical safeguards used by each Plan to protect its facilities and reflects the Plans' risk analysis performed pursuant to Section 15. The Plans will review their physical security measures periodically as part of updates to the risk analysis and in the event of significant changes to the environment or Plan information systems.

It is the Plans' policy to protect computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards. All servers will be secured and accessed only by approved staff or vendors. Workforce Members must store diskettes and other storage media (tapes, CDs, etc.) out of sight when not in use. If the media contain highly sensitive or confidential data, they must be locked up. Diskettes should be kept away from environmental hazards such as heat, direct sunlight, and magnetic fields. Environmental hazards to hardware such as food, smoke, liquids, high or low humidity, and extreme heat or cold should be avoided.

Workforce Members must exercise care to safeguard the valuable electronic equipment assigned to them. Workforce Members who neglect this duty may be accountable for any loss or damage that may result.

Controls used in the facility security plan include securing access to the Plans' areas by lock after hours or monitored entry during business hours. The Plans will take appropriate steps to control and validate the access of Workforce Members, patients, visitors and business associates based on each individual's role or function. All visitors are required to check in before access to the offices is allowed.

The Security Officer shall determine the job functions requiring access to areas with EPHI, document the job functions and notify Workforce Members of their physical access rights, consistent with Section 16. Workforce Members must report any loss or theft of any device (key or card, etc.) that enables them to gain physical access to areas with EPHI.

In the event of termination or departure of a Workforce Member, the Security Officer must verify that identification badges, keys, keycards or other means of access to the Plans' premises are returned and other appropriate actions are taken consistent with Section 16.

The Plans shall document repairs and modifications to physical components of the Plans' facilities that are related to security (such as hardware, walls, doors and locks). Documentation should include the date, reason for repair or modification, who authorized the repair or modification, and other information deemed material and relevant. The Security Officer shall determine the manner for maintaining such documentation. Examples of situations requiring modifications include termination of the Plan employees with access to large amounts of EPHI.

As part of the Plans' contingency plans developed pursuant to Section 19, the Plans will allow proper facility access to necessary personnel to restore lost data in the event of an emergency.

Section 21: Workstation Use and Security

All workstations will be secured when not in use. Workstations should be either logged out or screen locked when Workforce Members are not present with the machine. All workstation screens will auto lock after 15 minutes of inactivity.

Workstations must be located in areas that minimize the risk of unauthorized individuals gaining access to them. Workstations are kept inside Ryman's facilities which are locked and require badges for access. To the extent reasonable, workstation terminal screens must be turned away from visitors and other unauthorized persons.

When accessing the Plan system remotely (at home or any other location), Workforce Members must keep their workstations in a secure manner so that household members or other individuals do not have access to the workstation or EPHI. Workforce Members shall only use Plan workstations to perform their job functions or to otherwise support the functions of the Plan. Workforce Members may not use Plan workstations to engage in any illegal activity or activities that violate the Plan policies, including but not limited to procuring or transmitting material in violation of Plan Sponsor harassment policies.

Section 22: Device and Media Controls

The Security Officer shall periodically inventory the Plan information systems and electronic media that contain EPHI, in connection with the risk analysis process performed pursuant to Section 15. The Plan will implement reasonable safeguards to protect EPHI from improper destruction or disposal.

When disposal is authorized, all media, including CDs, diskettes, and computers will be disposed of in an appropriate manner so that all EPHI is no longer accessible and cannot be reasonably recovered. Prior to destruction of any EPHI or electronic media containing EPHI, the procedures set forth below for data backup and accountability must be followed. Additional care should be taken with the disposal of transportable media. At a minimum, Workforce Members will follow the following requirements for disposing of both fixed and transportable electronic media:

- All computers and all individual hard drives that are being disposed of will have the hard drives wiped. Data erasure should be performed before either removal from a Plan or by the vendor that is disposing of the equipment.
- All individual hard drives that are being disposed of should be wiped before disposal.
- All transportable media, diskettes, CDs, and zip drives should be destroyed or wiped clean before being disposed of, transferred to an area that should not use or have access to EPHI, or transferred to another entity.
- If a zip disk or diskette is being sent to another entity it should be reformatted/fully erased so that no remnants of EPHI could remain on the disk and be recoverable at an inappropriate location.
- USB Keys, if they are used to transfer EPHI, should be securely deleted with specialized secure deletion software.

Prior to re-using electronic media, EPHI must be removed from the media or made inaccessible. The Security Officer shall determine situations that only require reformatting so that files with EPHI are not accessible versus situations that that require permanent deletion of EPHI. An example of a situation requiring permanent deletion would be the donation of a computer to a school or charity. Prior to deletion of any EPHI or electronic media containing EPHI, the procedures set forth below for data backup and accountability must be followed.

Workforce Members intending to dispose of, re-use or remove hardware or electronic media containing PHI must first notify and receive the approval of the Security Officer. Workforce Members aware of any new hardware or electronic media containing EPHI entering the Plan premises must notify the Security Officer. The Security Officer shall maintain appropriate records of the disposal and the movement of hardware and electronic media containing EPHI into and out of the Plan premises.

The Security Officer shall maintain a record of the removal of electronic media containing EPHI out of Plan facilities (as appropriate and not including the removal of a laptop by a Workforce Member for the purpose of using the laptop outside of Plan facilities), which shall include the date of removal, a brief description of the hardware or electronic media, the name of the person removing and receiving it, and other information determined to be pertinent by the Security Officer. In the case of disposal or re-use of electronic media containing EPHI, the Security Officer shall maintain appropriate records, including the date of the disposal or deletion of PHI and what hardware and electronic media were disposed of or re-used.

Before equipment containing EPHI is moved from Plan facilities, re-used or disposed of, a retrievable, back-up copy of the EPHI shall be created and securely maintained, unless (1) a back-up or duplicate copy already exists at the Plan or the TPA; or (2) the EPHI no longer needs to be retained and its destruction is permissible consistent with the Plan document retention practices. In consultation with the Security Officer, Workforce Members responsible for moving, re-using or disposing of the equipment is responsible for confirming that an appropriate back-up copy of the EPHI (when required) has been created.

Section 23: <u>Encryption/Integrity and Transmission Security</u>

The Plans use reasonable technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network, including the internet. Encryption is to be used when emailing EPHI outside of the applicable Plan. E-mail messages between Workforce Members with EPHI that is related to the work function of the individuals do not have to be encrypted. Data at rest on a Plan server does not have to be encrypted but is instead protected through other security measures.

All laptops used by a Plan are equipped with whole-disk encryption to protect data on mobile work stations.

Section 24: Incident Response

A. In General

In accordance with Section 10(C), Workforce Members must report all known or suspected Security Incidents immediately to the Security Officer regardless of the time of day. A Security Incident includes any event with a negative consequence as well as any suspicious activity relating to EPHI in the possession of a Plan. Examples of potential Security Incidents include the following:

a. system crashes and computers rebooting on their own;

b. passwords that have been stolen, lost, or shared and used to access or attempt to access EPHI or passwords used by persons other than the individual to whom the password was assigned;

c. corrupted backup tapes that do not allow restoration of EPHI;

d. virus attacks or other malicious software being introduced into the Plan computer system;

e. unauthorized access to networks, computer systems or equipment rooms housing the computer system;

f. physical break-ins to EPHI facilities leading to the theft of or possible access to media with EPHI;

g. failure to terminate the account of a former the Plan workforce members that is then used by an unauthorized user to access information systems with EPHI;

h. loss of a laptop computer that may contain EPHI.

The Workforce Member noting the incident should document the time, date, details regarding the incident, steps taken for mitigation, and all conversations regarding the incident.

B. Incident Response

The Privacy Officer will oversee the prompt and appropriate investigation and resolution of all Security Incidents reported under this Section, in coordination with the Security Officer as needed. The Privacy Officer will determine whether the potential incident also implicates the privacy of

PHI and respond to any related privacy consistent with these Policies and Procedures, Section 10 and Section 11.

The investigation shall include identifying any vulnerability that led to the Security Incident. The Privacy Officer, in coordination with the Security Officer, will take reasonable and appropriate actions to mitigate any harm, contain the incident when possible and protect the confidentiality, integrity and availability of the applicable Plan information systems. These actions may include, as appropriate depending on the type of incident, the following:

a. immediately disconnecting the affected system from all networks;

b. handling communications between team members off line unless the communications are encrypted. Depending up on the type of incident, all internal communications should be considered suspect and hostile until proven otherwise. Phones, cell phones, standalone fax machines, etc. should be used for communications;

c. creating a backup of the system as soon as possible. A bit-by-bit back-up is preferred if any prosecution or further reconstruction is desired. A bit image will contain all files and all free space on the system. All drives in the system should be cloned;

d. cleaning the problem and determining what went wrong, if possible. After a restart, segment the machine and engage additional network and system monitoring tools to verify that the incident has been removed. In the event of a compromised system, it is better to reformat and start over from a fresh install of the operating system and reload ONLY DATA from the backup tapes;

e. having formal follow-up meeting required to assess additional steps needed and future prevention.

C. Other

The Plans will handle Security Incidents in compliance with the no waiver or retaliation and documentation requirements of Section 10. The Security Officer will document each reported incident and its resolution and maintain such documentation for 6 years from the date of its creation.

When appropriate, the Privacy Officer will recommend sanctions for the Workforce Members involved in a Security Incident, consistent with Section 10.

****

IN WITNESS WHEREOF, Ryman Hospitality Properties, Inc. adopts these revisions to its HIPAA Privacy and Security Policies and Procedures (which were updated on September 23, 2013) as of the ____ day of _____, 2016, with such revisions to be effective August 1, 2016.

RYMAN HOSPITALITY PROPERTIES, INC.

_____

Privacy Officer

_____

Security Officer

Exhibit A

Forms

1. **Business Associate Addendum**

2. **Authorization** (Note: this does not contain elements required for uses or disclosures for marketing purpose or the sale of PHI)

3. **Breach Investigation Record**

HIPAA BUSINESS ASSOCIATE ADDENDUM

This HIPAA Business Associate Addendum ("Addendum") amends and is made part of that certain _____ Agreement dated as of _____, 20___ ("Agreement"), by and between Ryman Hospitality Properties, Inc. on behalf of its group health plan or plans, as applicable, (collectively, "Entity") and ___ _____ ("Associate").

Entity and Associate agree that the parties incorporate this Addendum into the Agreement in order to comply with the requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act ("HITECH") and their implementing regulations set forth at 45 C.F.R. Parts 160 and Part 164 (the "HIPAA Rules"). To the extent Associate is acting as a Business Associate of Entity pursuant to the Agreement, the provisions of this Addendum shall apply and Associate shall be subject to the penalty provisions of HIPAA as specified in 45 C.F.R. Part 160.

1. Definitions. Capitalized terms not otherwise defined in this Addendum shall have the meaning set forth in the HIPAA Rules. References to "PHI" mean Protected Health Information maintained, created, received or transmitted by Associate from Entity or on Entity's behalf.

2. Uses or Disclosures. Associate will neither use nor disclose PHI except as permitted or required by this Addendum or as required by law. To the extent Associate is to carry out an obligation of Entity under the HIPAA Rules, Associate shall comply with the requirements of the HIPAA Rules that apply to Entity in the performance of such obligation. Without limiting the foregoing, Associate will not sell PHI or use or disclose PHI for purposes marketing or fundraising, as defined and proscribed in the HIPAA Rules and HITECH. Associate is permitted to use and disclose PHI:

(a) to perform any and all obligations of Associate as described in the Agreement, provided that such use or disclosure is consistent with the terms of Entity's notice of privacy practices and would not violate the HIPAA Rules, if done by Entity directly;

(b) as otherwise permitted by law, provided that such use or disclosure would not violate the HIPAA Rules, if done by Entity directly and provided that Entity gives its prior written consent;

(c) to perform Data Aggregation services relating to the health care operations of Entity;

(d) to report violations of the law to federal or state authorities consistent with 45 C.F.R. § 164.502(j)(1);

(e) as necessary for Associate's proper management and administration and to carry out Associate's legal responsibilities (collectively "Associate's Operations") provided that any disclosure made for purposes of Associate's Operations is required by law or is made after Associate obtains reasonable assurances, evidenced by a written contract, from the recipient that the recipient will: (1) hold such PHI in confidence and use or further disclose it only for the purpose

for which Associate disclosed it to the recipient or as required by law; and (2) notify Associate of any instance of which the recipient becomes aware in which the confidentiality of such PHI was breached;

(f) to de-identify PHI in accordance with 45 C.F.R. § 164.514(b), provided that such de-identified information may be used and disclosed only consistent with applicable law.

In the event Entity notifies Associate of a restriction request that would restrict a use or disclosure otherwise permitted by this Addendum, Associate shall comply with the terms of the restriction request.

3. Safeguards. Associate will use appropriate administrative, technical and physical safeguards to prevent the use or disclosure of PHI other than as permitted by this Addendum and shall maintain policies and procedures to detect, prevent, and mitigate identity theft based on PHI or information derived from PHI. Associate will also comply with the provisions of 45 C.F.R. Part 164, Subpart C of the HIPAA Rules with respect to electronic PHI to prevent any use or disclosure of such information other than as provided by this Addendum, which obligation shall include maintaining safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of electronic PHI.

4. Subcontractors and Agents. In accordance with 45 C.F.R. §§ 164.308(b)(2) and 164.502(e)(1)(ii), Associate will ensure that all of its subcontractors and agents that create, receive, maintain or transmit PHI on behalf of Associate agree by written contract to comply with the same restrictions and conditions that apply to Associate with respect to such PHI.

5. Minimum Necessary. Associate represents that the PHI requested, used or disclosed by Associate shall be the minimum amount necessary to carry out the purposes of the Agreement. Associate will limit its uses and disclosures of, and requests for, PHI (i) when practical, to the information making up a Limited Data Set; and (ii) in all other cases subject to the requirements of 45 CFR § 164.502(b), to the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure or request.

6. Obligations of Entity. Entity shall notify Associate of (i) any limitations in its notice of privacy practices, (ii) any changes in, or revocation of, permission by an individual to use or disclose PHI, and (iii) any confidential communication request or restriction on the use or disclosure of PHI affecting Associate that Entity has agreed to or with which Entity is required to comply, to the extent any of the foregoing affect Associate's use or disclosure of PHI.

7. Access and Amendment. In accordance with 45 C.F.R. § 164.524, Associate will permit Entity or, at Entity's request, an individual (or the individual's designee) to inspect and obtain copies of any PHI about the individual that is in Associate's custody or control and that is maintained in a Designated Record Set. If the requested PHI is maintained electronically, Associate must provide a copy of the PHI in the electronic form and format requested by the individual, if it is readily producible, or, if not, in a readable electronic form and format as agreed to by Entity and the individual. Associate will notify Entity of any request (including but not limited to subpoenas) that Associate receives for access to PHI that is in Associate's custody or control within five (5) business days of receipt of such request. Entity shall be responsible for

making determinations about access. Associate will, upon receipt of notice from Entity, promptly amend or permit Entity access to amend any portion of the PHI that is in Associate's custody or control so that Entity may meet its amendment obligations under 45 C.F.R. § 164.526.

8. Disclosure Accounting. Except for disclosures excluded from the accounting obligation by the HIPAA Rules and regulations issued pursuant to HITECH, Associate will record for each disclosure that Associate makes of PHI the information necessary for Entity to make an accounting of disclosures pursuant to the HIPAA Rules. In the event the U.S. Department of Health and Human Services ("HHS") finalizes regulations requiring Covered Entities to provide access reports, Associate shall also record such information with respect to electronic PHI held by Associate as would be required under the regulations for Covered Entities beginning on the effective date applicable to Entity. Associate will make information required by this Section 8 available to Entity promptly upon Entity's request for the period requested, but for no longer than the six (6) years preceding Entity's request for the information or such other period required by the HIPAA Rules (except Associate need not have any information for disclosures occurring before the effective date of any previous HIPAA business associate agreements between the parties or, if none, the effective date of this Addendum).

9. Inspection of Books and Records. Associate will make its internal practices, books, and records, relating to its use and disclosure of PHI available upon request to Entity or HHS to determine compliance with the HIPAA Rules.

10. Reporting. To the extent Associate becomes aware or discovers any use or disclosure of PHI not permitted by this Addendum, any Security Incident involving electronic PHI, any Breach of Unsecured Protected Health Information or any Red Flag (as defined at 16 CFR § 681.2(b)) related to any individual who is the subject of PHI, Associate shall promptly report such use, disclosure, Security Incident, Breach or Red Flag to Entity. Associate shall mitigate, to the extent practicable, any harmful effect known to it of a Security Incident, Breach or use or disclosure of PHI by Associate not permitted by this Addendum. Notwithstanding the foregoing, the parties acknowledge and agree that this Section constitutes notice by Associate to Entity of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents (as defined below) for which no additional notice to Entity shall be required. "Unsuccessful Security Incidents" shall include, but not be limited to, pings and other broadcast attacks on Associate's firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of electronic PHI. All reports of Breaches shall be made within ten (10) business days of Associate discovering the Breach and shall include the information specified at 45 CFR § 164.410. Associate shall promptly reimburse Entity all reasonable costs incurred by Entity with respect to providing notification of and mitigating a Breach involving Associate, including but not limited to printing, postage costs and toll-free hotline costs.

11. Term and Termination. This Addendum shall be effective as of the effective date of the Agreement and shall remain in effect until termination of the Agreement. Either party may terminate this Addendum and the Agreement effective immediately if it determines that the other party has breached a material provision of this Addendum and failed to cure such breach within thirty (30) days of being notified by the other party of the breach. If the non-breaching party determines that cure is not possible, such party may terminate this Addendum and the Agreement

effective immediately upon written notice to other party. If termination is not feasible, the non-breaching party may report the breach to HHS.

Upon termination of this Addendum for any reason, Associate will, if feasible, return to Entity or securely destroy all PHI maintained by Associate in any form or medium, including all copies of such PHI, at no cost to Entity. Further, Associate shall recover any PHI in the possession of its agents and subcontractors and return to Entity or securely destroy all such PHI. Notwithstanding the foregoing, Associate shall notify Entity and receive Entity's written consent prior to destroying any PHI of which Entity does not maintain a duplicate copy. In the event that Associate determines that returning or destroying any PHI is infeasible, Associate shall promptly notify Entity of the conditions that make return or destruction infeasible. With regard to any PHI that Entity agrees cannot feasibly be returned to Entity or destroyed, Associate may maintain such PHI but shall continue to abide by the terms and conditions of this Addendum with respect to such PHI and shall limit its further use or disclosure of such PHI to those purposes that make return or destruction of the PHI infeasible. Associate shall comply with this Section within thirty (30) days of termination of this Addendum. Associate shall provide Entity with written certification of its compliance with this Section within forty-five (45) days of termination of this Addendum. Upon termination of this Addendum for any reason, all of Associate's obligations under this Addendum shall survive termination and remain in effect (a) until Associate has completed the return or destruction of PHI as required by Section and (b) to the extent Associate retains any PHI pursuant to this Section.

12. <u>General Provisions</u>. In the event that any final regulation or amendment to final regulations is promulgated by HHS or other government regulatory authority with respect to PHI, this Addendum will automatically be amended to remain in compliance with such regulations, and Associate shall promptly amend its contracts, if any, with subcontractors and agents to conform to the terms of this Addendum. Any ambiguity in this Addendum shall be resolved to permit Entity to comply with the HIPAA Rules. Nothing in this Addendum shall be construed to create any rights or remedies in any third parties or any agency relationship between the parties. A reference in this Addendum to a section in the HIPAA Rules means the section as in effect or as amended. This Addendum replaces and supersedes and previous business associate agreements between the parties. The terms and conditions of this Addendum override and control any conflicting term or condition of the Agreement. To the extent Associate has limited its liability under the terms of the Agreement by a maximum recovery for direct damages, disclaimer against any consequential, indirect or punitive damages or any other limitation, all limitations shall exclude any damages to Entity arising from Associate's breach of its obligations under this Addendum. All non-conflicting terms and conditions of the Agreement remain in full force and effect.

IN WITNESS WHEREOF, the parties have executed this Addendum on the dates indicated below.

ENTITY	**ASSOCIATE**
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

Authorization for Use or Disclosure of Information

I hereby authorize the group health plans sponsored by Ryman Hospitality Properties, Inc. to use or disclosure my individually identifiable health information as described below. I understand that this authorization is voluntary. I understand that if the organization authorized to receive the information is not covered by federal privacy regulations, the released information may no longer be protected by federal privacy regulations and may be subject to redisclosure.

Individual Name: _____

- Persons/organizations authorized to receive my information:

  _____

- Specific description of information covered by this authorization:

  _____

  _____

- The purpose of the disclosure is:

  _____

- I understand that the persons hereby authorized to use or disclose information will not condition treatment, payment, enrollment in a health plan, or eligibility for benefits on my providing this authorization, except that a health plan may condition enrollment in the health plan or eligibility for benefits on this authorization if (1) I am not yet enrolled in the health plan, (2) the purpose of this authorization is to allow the health plan to obtain non-genetic information it needs to make an eligibility, enrollment, underwriting or risk determination, and (3) psychotherapy notes are not requested. If these three circumstances apply, refusal to sign this authorization may result in my being denied enrollment in the health plan or eligibility for health care benefits.

- I understand that this authorization will expire on either the date listed below or the occurrence of the following event related to the purpose of this authorization:

  _____

- I understand that I may revoke this authorization at any time by notifying _____ in writing at _____. I understand that this revocation shall not be effective (1) to the extent this authorization has already been relied upon, or (2) if the authorization was obtained as a condition for health plan coverage and Ryman Hospitality Properties, Inc.'s group health plan has a right to contest the coverage under applicable law.

- I understand that I have the right to receive a copy of this authorization after I have signed it.

Signature of individual or
individual's representative: _____ Date: _____

Printed name of individual's representative: _____

Basis of representative's authority to act for individual: _____

HIPAA Breach Investigation Record

1. Describe the incident:

   a. Number of participants whose PHI was involved: _____

   b. Date of the incident: _____

   c. Was Unsecured PHI used or disclosed? ☐ Yes ☐ No, the PHI was encrypted ☐ No, the PHI was shredded

   d. Format of the PHI that was involved: ☐ Paper ☐ Electronic ☐ Oral

   e. Type of PHI that was involved (e.g., claim that specified diagnosis, EOB): _____
   _____
   _____

   f. Identifiers that were involved: ☐ Name ☐ Address ☐ Zip Code ☐ SSN ☐ Date of Birth ☐ Telephone Number ☐ E-mail Address ☐ Other: _____

   g. Recipient of the PHI that was involved: _____

   h. Other details: _____
   _____
   _____
   _____
   _____
   _____

2. Date the incident was discovered (i.e., the first day on which the incident was known to the Plan or, by exercising reasonable diligence, would have been known to the Plan):
   _____

3. Does the incident fall within one of the following three exceptions to the definition of "Breach"?

   a. Was the incident (i) an unintentional acquisition, access, or use of PHI by the Plan, Workforce Members or any individual acting under the authority of the Plan or its Business Associate, (ii) made in good faith and within the course and scope of authority, and (iii) the information was not further used or disclosed in a manner not permitted by the HIPAA Rules? ☐ Yes ☐ No
   Explain: _____
   _____
   _____

   b. Was the incident (i) an inadvertent disclosure by a person who is authorized to access PHI at the Plan or its Business Associate to another person authorized to access PHI at the Plan or the same Business Associate and (ii) the information received as a result of the disclosure was not further used or disclosed in a manner not permitted by the HIPAA Rules? ☐ Yes ☐ No
   Explain: _____
   _____
   _____

   c. Was the incident a disclosure of PHI where the Plan or its Business Associate has a good faith belief that the recipient would not reasonably have been able to retain the information (such as an envelope that is incorrectly addressed and is returned unopened as undeliverable by the U.S. Post Office)? ☐ Yes ☐ No
   Explain: _____
   _____
   _____

If the answer to any of the three exceptions in Question 3 is "yes," then there was not a Breach and no further steps need to be taken with respect to providing Breach notification. Other steps may be required under state law or other policies (such as providing refresher training or taking other mitigation steps). If the answer to all three of the exceptions in Question 3 is "no," then proceed to Question 4.

4. Determine whether the Plan can demonstrate that there is a low probability that the PHI has been compromised:

   a. Consider the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification. Explain: _____
   _____
   _____

   b. Consider the unauthorized person who used the PHI or to whom the disclosure was made. Explain: _____
   _____
   _____

   c. Consider whether the PHI was actually acquired or viewed. Explain: _____
   _____
   _____

   d. Consider the extent to which the risk to the PHI has been mitigated. Explain: _____
   _____
   _____

   e. Based at least on the above four factors, can the Plan demonstrate that there is a low probability that the PHI has been compromised? ☐ Yes ☐ No

Signature of Privacy Officer: _____Date: _____