AMENDMENTS
TO HIPAA POLICIES AND PROCEDURES
OF THE
ROMAN CATHOLIC ARCHDIOCESE OF BOSTON HEALTH BENEFIT PLAN

Whereas, the Roman Catholic Archdiocese of Boston Health Benefit Plan (the "Plan") has adopted certain Policies and Procedures in accordance with the requirements of HIPAA (the "Policies and Procedures"); and

Whereas, in light of the Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH") and the final HIPAA regulations issued by the Department of Health and Human Services on January 25, 2013 (the "Omnibus Regulations"), the Plan has determined that it is necessary or appropriate to amend the Policies and Procedures.

Now, therefore, the Policies and Procedures are hereby amended as follows:

1. The Policies and Procedures shall be subject to the Plan's most recent Notice of Privacy Practices (the "Notice"). To the extent any of the Policies and Procedures are inconsistent with the Notice, the Policies and Procedures are hereby amended to the extent necessary to conform with the Notice and the Plan shall be administered in accordance with the Notice.

2. With respect to the Policies and Procedures relating to the "Minimum Necessary" requirement of HIPAA, the Policies and Procedures are amended as follows:

"Limitation of Use and Disclosures to Minimum Necessary Standard

Until the Secretary of the U.S. Department of Health and Human Services releases further guidance regarding the minimum necessary standard, the Plan will limit disclosures and uses of PHI to the information contained in a HIPAA limited data set. However, if it is not practicable for the Plan to limit its use or disclosure of PHI to a limited data set, then the Plan will make reasonable efforts not to use, disclose or request more than the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure or request, taking into consideration practical and technological limitations.

However, the minimum necessary standard will <u>not</u> apply in the following situations:

- Disclosures to or requests by a health care provider for treatment purposes;
- Uses or disclosures made to a covered person;
- Uses or disclosures authorized by a covered person;
- Disclosures made to the Secretary of the U.S. Department of Health and Human Services;

- Uses or disclosures that are required by law; and
- Uses or disclosures that are required by the Plans' compliance with legal requirements.

3. With respect to the Policies and Procedures relating to Business Associate Agreements, the Policies and Procedures are amended as follows:

BUSINESS ASSOCIATES

A "business associate" is a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information. A "business associate" also is a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of another business associate. The HIPAA Rules generally require that covered entities and business associates enter into contracts with their business associates to ensure that the business associates will appropriately safeguard protected health information. The business associate contract also serves to clarify and limit, as appropriate, the permissible uses and disclosures of protected health information by the business associate, based on the relationship between the parties and the activities or services being performed by the business associate. A business associate may use or disclose protected health information only as permitted or required by its business associate contract or as required by law. A business associate is directly liable under the HIPAA Rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of protected health information that are not authorized by its contract or required by law. A business associate also is directly liable and subject to civil penalties for failing to safeguard electronic protected health information in accordance with the HIPAA Security Rule.

A written contract between a covered entity and a business associate must: (1) establish the permitted and required uses and disclosures of protected health information by the business associate; (2) provide that the business associate will not use or further disclose the information other than as permitted or required by the contract or as required by law; (3) require the business associate to implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the HIPAA Security Rule with regard to electronic protected health information; (4) require the business associate to report to the covered entity any use or disclosure of the information not provided for by its contract, including incidents that constitute breaches of unsecured protected health information; (5) require the business associate to disclose protected health information as specified in its contract to satisfy a covered entity's obligation with respect to individuals' requests for copies of their protected health information, as well as make available protected health information for amendments (and incorporate any amendments, if required) and accountings; (6) to the extent the business associate is to carry out a covered entity's obligation under the Privacy Rule, require the business associate to comply with the requirements applicable to the obligation; (7) require the business associate to make available to HHS its internal practices, books, and records relating to the use

and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity for purposes of HHS determining the covered entity's compliance with the HIPAA Privacy Rule; (8) at termination of the contract, if feasible, require the business associate to return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity; (9) require the business associate to ensure that any subcontractors it may engage on its behalf that will have access to protected health information agree to the same restrictions and conditions that apply to the business associate with respect to such information; and (10) authorize termination of the contract by the covered entity if the business associate violates a material term of the contract. Contracts between business associates and business associates that are subcontractors are subject to these same requirements.

4. With respect to the Policies and Procedures relating to a breach of PHI, the following Policy and Procedure shall apply:

RESPONSE TO BREACH OF UNSECURED PHI SCOPE OF POLICY

This policy applies to Roman Catholic Archdiocese of Boston employees who provide plan administration functions on behalf of the Roman Catholic Archdiocese of Boston Group Health Plan (the "Plan") subject to the privacy and security requirements of the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA"), including but not limited to the Plan Privacy and Security Official or an individual designated by the Privacy and Security Official to perform HIPAA-related functions on behalf of the Privacy and Security Official (referred to collectively as the "Privacy and Security Official"). These Roman Catholic Archdiocese of Boston employees are collectively referred to in this policy as Administrative Service Providers ("ASPs"). This policy also applies to outside vendors, as determined by the Plan, who provide services on behalf of the Plan ("Business Associates").

STATEMENT OF POLICY

The Plan is required by law to protect the privacy of health information that may reveal the identity of a Plan Member. If a breach of certain types of individually identifiable health information occurs, the Plan is required to provide notification to certain individuals and entities pursuant to Subtitle D of the Health Information Technology for Economic and Clinical Health Act, which is Title XIII of the American Recovery and Reinvestment Act of 2009 and any regulations promulgated thereunder ("HITECH") and in accordance with the Omnibus Regulations. The Plan may have additional reporting obligations under other federal laws and state breach notification laws. Those obligations are not addressed in this policy.

IMPLEMENTATION OF POLICY

1. Definition of Breach

For purposes of this policy, the term "breach" means the acquisition, access, use or disclosure of protected health information in a manner not otherwise permitted under the HIPAA Privacy Rule which compromises the security or privacy of the protected health information. The term "protected health information" means any Plan Member information, including basic information such as the Plan Member's name or address, that (1) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and (2) either identifies the individual or could reasonably be used to identify the individual.

2. Report of Breaches to Privacy and Security Official

It is the responsibility of the Plan to protect and preserve the confidentiality of all protected health information. To avoid possible breaches of protected health information and inform ASPs of the importance of promptly reporting privacy and security incidents and the consequences for the failure to do so, the Privacy and Security Official will coordinate with other officials and departments to train all ASPs on their respective responsibilities and obligations under HIPAA and HITECH. In addition to training ASPs, the Privacy and Security Official may re-evaluate persons authorized to access protected health information to determine if authorization is necessary and, if necessary, whether such access complies with the minimum necessary standard under HIPAA.

Any ASP or Business Associate who knows, believes, or suspects that a breach of protected health information has occurred, must report the breach to the Privacy and Security Official immediately. Within one business day of his or her receipt of a report, the Privacy and Security Official will notify the Office of the General Counsel.

After a potential breach is reported, the Privacy and Security Official will work with other officials and departments, including the Office of the General Counsel and RCAB's information technology department to conduct a thorough investigation, which will include an analysis to determine whether a breach of unsecured protected health information under HITECH has occurred and if so, what notifications are required. The Privacy and Security Official should complete his or her investigation no later than 20 calendar days (or earlier if required by law) to ensure sufficient time for the preparation and coordination of notifications, if required, provided that the investigation may take more or less time depending on the circumstances. As part of the investigation, the Privacy and Security Official will take all necessary steps to mitigate any

known harm. The details of the investigation will be documented in a memo that is kept on file with the Privacy and Security Official with a copy sent to the Office of the General Counsel.

As part of the Privacy and Security Official's investigation to determine whether a breach of unsecured protected health information under HITECH has occurred, the Privacy and Security Official must take certain steps to ensure a complete investigation.

The Privacy and Security Official must first decide whether the information is protected health information and if so, whether the protected health information is unsecured.

- *If the information is not protected health information* because, of example, the information is de-identified in compliance with HIPAA, no further investigation is required under HITECH. The Privacy and Security Official will have other responsibilities, including evaluating whether notifications are required pursuant to the Red Flag Rules and/or applicable state breach notification laws.

- *If the information is protected health information*, the Privacy and Security Official will then need to determine if the information has been properly "secured" by the methods set forth in HITECH (e.g., encryption and destruction). If the Privacy and Security Official determines that the protected health information is "secured," although no further steps are required pursuant to this policy, the Privacy and Security Official is responsible for determining whether the Plan has accounting and mitigation obligations under HIPAA. If it is determined that the protected health information is unsecured, the Privacy and Security Official must determine whether a breach under HITECH has occurred (see part 3 below of this policy).

The Privacy and Security Official must document the analysis performed to determine if the information is protected health information and, if necessary, whether the protected health information is secured, in a memo to be kept on file with the Privacy and Security Official with a copy to be sent to the Office of the General Counsel.

As discussed in more detail in part 4 below of this policy, if a breach under HITECH has occurred and notifications are required, the time period by which notifications must be sent to the affected individuals, the Secretary of the U.S. Department of Health and Human Services (and, if necessary, the media), begins when the breach is first discovered, not when the Privacy and Security Official completes his or her investigation of whether a breach has occurred. A breach is treated as discovered when the Plan:

a. Has knowledge of or, by exercising reasonable diligence, should have had knowledge of the breach; or

b. Is deemed to have knowledge of the breach because an ASP or Business Associate has knowledge of or, by exercising reasonable diligence, should have had knowledge of the breach.

The Privacy and Security Official will document when the Privacy and Security Official reasonably believes the breach occurred.

3. Determination of Breach

If the Privacy and Security Official has determined that there is an acquisition, access, use or disclosure of unsecured protected health information, the Privacy and Security Official must then conduct the following analysis:

i. Determine whether there has been an impermissible acquisition, access, use, or disclosure of protected health information under the HIPAA Privacy Rule.

ii. If no, no further analysis required pursuant to this policy. If yes, determine whether the impermissible acquisition, access, use or disclosure compromises the security or privacy of the protected health information.

iii. If no, no further analysis required pursuant to this policy. If yes, determine whether an exception applies.

a. Impermissible Acquisition. Access, Use or Disclosure

Protected health information may only be used or disclosed pursuant to a valid authorization or one of the specifically enumerated exceptions under HIPAA. To determine if protected health information was impermissibly acquired, accessed, used or disclosed under the HIPAA Privacy Rule, the Privacy and Security Official will conduct an analysis (the results of which will be detailed in a memo that is kept on file with the Privacy and Security Official with a copy sent to the Office of the General Counsel). If the acquisition, access, use, or disclosure is permitted, no further investigation pursuant to this policy is required. If the Privacy and Security Official determines that an impermissible acquisition, access, use, or disclosure has occurred, he/she is responsible for complying with the applicable policies and procedures (including making an accounting of such disclosure and, if necessary, mitigating any known harm) and conducting the analysis set forth in b. below.

b. Compromises the Security or Privacy of Protected Health Information (PHI) -Presumption of Breach

- If there has been an impermissible acquisition, access, use, or disclosure of unsecured protected health information under the HIPAA Privacy Rule, it will be presumed that a breach has occurred, unless the Plan or Business Associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of the following factors:
- The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the protected health insurance information or to whom the disclosure was made;

- Whether the protected health information was actually acquired or viewed; and
- The extent to which the risk to the protected health information has been mitigated.

In addition, given the circumstances of the impermissible use or disclosure, additional factors, to the extent permitted under HIPAA, may need to be considered by the Plan or Business Associate as applicable, to appropriately assess the risk that the protected health information has been compromised.

The Privacy and Security Official will document the above risk assessment in a memo that is kept on file with the Privacy and Security Official with a copy sent to the Office of the General Counsel. If the Privacy and Security Official determines that there is no breach has occurred based on that risk assessment, no further steps need to be taken pursuant to this policy. The Privacy and Security Official, however, is responsible for conducting a separate analysis regarding the Plan accounting and mitigation obligations, if any.

c. <u>Exceptions to the Definition of Breach</u>

If, based on the above analysis, the Privacy and Security Official determines that there has been an impermissible acquisition, access, use, or disclosure which compromises the security or privacy of the protected health information, the Privacy and Security Official must determine if any of the following exceptions apply:

- Any unintentional acquisition, access or use of protected health information by a workforce member or person acting under the authority of a covered entity or a Business Associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Rule;

- Any inadvertent disclosure by a person authorized to access protected health information at a covered entity or Business Associate to another person authorized to access protected health information at the same covered entity or Business Associate, or organized health care arrangement in which the covered entity participates, and the information received from such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule; or

- Disclosure of protected health information where a covered entity or Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

The Privacy and Security Official will perform a fact specific analysis to determine if an exception applies and document its analysis and findings in a memo that is kept on file with the Privacy and Security Official with a copy sent to the Office of the General Counsel. If so, the Privacy and Security Official can conclude that a breach did not occur and that no notification is required.

If none of these exceptions apply, the Privacy and Security Official must conclude that a breach of unsecured protected health information has occurred and notification to affected individuals, the Secretary of the U.S. Department of Health and Human Services (the "Secretary") and, if applicable, the media is required.

4. Breach Notification

Once the Privacy and Security Official has determined that a breach has occurred, he or she is responsible for coordination of a response to certain persons and entities.

a. Notification to Affected Individuals

Notification must be provided to each individual whose unsecured protected health information has been or is reasonably believed to have been, acquired, accessed, used or disclosed as a result of the breach without unreasonable delay and in no case later than 60 calendar days. If the breach requires the involvement of law enforcement, the notification may be delayed for a period of time as determined by a law enforcement official.

The Privacy and Security Official must prepare a notification that includes (to the extent possible):

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
- A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
- Any steps individuals should take to protect themselves from potential harm resulting from the breach;
- A brief description of what the Plan is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
- Contact procedures for individuals to ask questions or learn additional information, which must include a toll-free telephone number, an email address, web site or postal address.

The Privacy and Security Official will be sensitive to only include general information (i.e., listing the types of information involved as opposed to listing the actual protected health information that was involved in the breach) in the notification. Depending upon the nature of the breach and the information obtained during the investigation, the Privacy and Security Official may also include:

- Recommendations that the individual contact applicable credit card companies and information about how to obtain credit monitoring services;
- Information about what steps the Plan is taking to retrieve the breached information and improve security to prevent future breaches; and
- Information about sanctions the Plan imposed on its workforce members involved in the breach.

To comply with other applicable laws, the Privacy and Security Official may also need to translate the notice into other languages and make the notice available in alternate formats, such as Braille, large print or audio.

The Privacy and Security Official will send a draft of the notice to the Office of the General Counsel for review. The preparation and review of the notice should be completed within 15 calendar days (more or less time may be necessary depending on the circumstances).

The notice will be sent by first-class mail or, if the Plan does not have sufficient contact information for some or all of the affected individuals, by substitute notice (depending on the number of individuals for whom the Plan does not have sufficient contact information, through an alternate form of written notice, by telephone or other means, or by a posting on RCAB's website for 90 days or in major print or broadcast media in geographic areas where the affected individuals likely reside).

b. <u>Notification to the Secretary</u>

The Privacy and Security Official must provide notice to the Secretary concurrently with the notification sent to the affected individuals (for any breach involving 500 or more individuals) or within 60 days after the end of each calendar year (for breaches involving less than 500 individuals). In the latter case, the Privacy and Security Official will maintain a log and other documentation of each breach to ensure that the scope and extent of the information provided to the Secretary is in compliance with HITECH. The content of the notice will be the same as described above.

No later than November 30th of each year, the Privacy and Security Official and the Information Security Officer (if they are not the same person) will meet to discuss the process and content of the report to be sent to the Secretary. The Privacy and Security Official and Information Security Officer will prepare a draft of the report and by January 31st , will send the draft to the Office of the General Counsel. By February 15th, the Office of the General Counsel, the Privacy and Security Official and the Information Security Officer (if the Privacy and Security Official and Information Security Officer are not the same person) will finalize the report for submission to the Secretary on or before March 1st.

c. Notification to the Media

The Privacy and Security Official may also be required to notify a prominent media outlet for any breach that involves more than 500 residents of anyone state or jurisdiction. The notification will contain the same information as described above and will be made concurrently with the notification sent to the affected individuals. The Privacy and Security Official, depending on the circumstances of the breach, will determine what constitutes a prominent media outlet.

The Privacy and Security Official will be responsible for documenting that all notifications required under HITECH were made in a memo to be kept on file with the Privacy and Security Official with a copy to be sent to the Office of the General Counsel.

d. Notification by Business Associates

The Privacy and Security Official will work with Business Associates of the Plan to ensure that Business Associates report any breaches of protected health information promptly to the appropriate individual at the Plan. To the extent the unsecured protected health information is the protected health information of a covered entity that participates in an organized health care arrangement with the Plan, the Privacy and Security Official will coordinate with the respective Privacy Official(s) of such covered entities.

VIOLATIONS

The Privacy and Security Official has a general responsibility for implementation of this policy. Any member of the Plan who violates this policy will be subject to disciplinary action up to and including termination of employment with Roman Catholic Archdiocese of Boston. Anyone who knows or has reason to believe that another person has violated this policy should report the matter promptly to his or her supervisor or the Privacy and Security Official. All reported matters will be investigated and, where appropriate, steps will be taken to remedy the situation. Where possible, RCAB will make every effort to handle the reported matter confidentially. Any attempt to retaliate against a person for reporting a violation of this policy will itself be considered a violation of this policy that may result in disciplinary action up to and including termination of employment with Roman Catholic Archdiocese of Boston. Any questions about this policy should be immediately directed to the Privacy and Security Official."

5. With respect to the Policies and Procedures relating to the security of electronic PHI, those Policies and Procedures are amended as follows:

"Security of PHI – Technical Safeguards

A. Access Controls

The Plan shall implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights.

a. Unique user identification. The Plan shall assign a unique name and/or number for identifying and tracking user identity.
b. Emergency access procedure. The Plan shall establish (and implement as needed) procedures for obtaining necessary electronic PHI during an emergency.
c. Automatic logoff. The Plan shall implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
d. Encryption and decryption. The Plan shall implement a mechanism to encrypt and decrypt electronic PHI.

B. Audit Controls

The Plan shall implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI.

C. Integrity

The Plan shall implement policies and procedures to protect electronic PHI from improper alteration or destruction.

a. Mechanism to authenticate electronic PHI. The Plan shall implement electronic mechanisms to corroborate that electronic PHI has not been altered or destroyed in an unauthorized manner.

D. Person or Entity Authentication

The Plan shall implement procedures to verify that a person or entity seeking access to electronic PHI is the one claimed.

E. Transmission Security

The Plan shall implement technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network.

a. Integrity controls. The Plan shall implement security measures to ensure that electronically transmitted electronic PHI is not improperly modified without detection until disposed of.
b. Encryption. The Plan shall implement a mechanism to encrypt electronic PHI whenever deemed appropriate."

***

6. To the extent any of the Policies and Procedures conflict with HIPAA (including, but not limited to, HITECH or the Omnibus Regulations), the Policies and Procedures shall be automatically amended to so comply and shall be administered in accordance with all such automatic amendments. The Privacy and Security Official shall from time to time notify RCAB employees involved in the administration of the Plan of such automatic amendments.

7. The Amendments set forth above shall be effective on the applicable date or dates required by HIPAA, including but not limited to, HITECH and the Omnibus Regulations.

In Witness Whereof, the Amendments set forth above are hereby adopted effective July 1, 2013.

The Trustees of the Roman
Catholic Archdiocese of Boston
Health Benefit Trust

By:

Carol Gustavson
Plan Administrator