Health Programs Sponsored By
The Diocese of Rockville Centre

SUMMARY OF POLICIES AND PROCEDURES UNDER THE HIPAA ADMINISTRATIVE SIMPLIFICATION REGULATIONS

This document describes the policies and procedures that the Diocese of Rockville Centre (DRVC), as the Plan Administrator for its employee health plans, has adopted to provide for the integrity, security, privacy and availability of health information. The policies and procedures described in this document are intended to comply with all applicable requirements of the HIPAA Administrative Simplification Regulations and will be construed to be consistent with those requirements, where reasonable, and will be modified to match those requirements, as needed.

Nothing in this Summary of Policies and Procedures should be interpreted to be an acknowledgment by DRVC that the health plans that it sponsors are subject to any portion of the HIPAA Administrative Simplification Regulations to which they are not, in fact, subject.

This document uses the phrase, "the Plan", to refer to each of the separate employee health plans or benefit options sponsored by DRVC, and any plans or benefit options that provide coverage or reimbursement for medical, dental, vision, prescription drug or long term care expenses including any health care flexible spending arrangements. This document is intended to apply to each of those benefit plans or options separately and collectively.

The policies and procedures described in this document are general guidelines by which the Plan intends to operate. Also, to the extent that the Plan is required, under applicable law, to comply with any policies or procedures described in this document, this document is intended to provide for the Plan's compliance with applicable law. The Plan will make all reasonable efforts to ensure compliance with these policies and procedures. However, nothing in this document should be taken as a promise by the Plan (or by DRVC) to any individual or entity that the Plan will comply with any particular policy or procedure described within this document with respect to a specific transaction or a specific disclosure or use of health information.

EFFECTIVE DATE: This document is effective April 14, 2003, except as otherwise provided below.

DEFINITIONS

Administrative Simplification Regulations or "Regulations" refers to regulations issued by the Department of Health and Human Services ("DHHS") pursuant to the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 and includes the ***Privacy Rule*** (the regulations issued as "Standards for Privacy of Individually Identifiable Health

Information"); the ***Electronic Transactions Standards*** (the regulations issued as "Electronic Transactions and Code Sets Standards"); and the ***Security Rule*** (the regulations issued as "Security and Electronic Signature Standards"). In applying any references in this document to any of the regulations described in this paragraph, the Plan will refer to the regulations as modified and as in effect at the time the reference is to be applied. The Regulations will be interpreted in light of any guidance from DHHS or any other federal agency that the Plan determines is authoritative. To the extent that compliance with a regulatory provision or other guidance is not required, the Plan has discretion to follow or to decline to follow that provision.

Business Associate is defined at Section 160.103 of the Privacy Rule and refers to a person or organization, other than DRVC or its employees, that, pursuant to an agreement with DRVC or the Plan, performs services on behalf of the Plan that require the use or disclosure of PHI by the Business Associate.

Designated Record Set is defined at Section 164.501 of the Privacy Rule means a set of records (including paper and electronic records) maintained by or for the Plan that include PHI and that are either (1) enrollment, claims processing or medical management records or (2) any other records used by the Plan to make decisions about individuals.

Personal Representative means a person legally authorized, as determined under applicable State law, to act on behalf of another person, either generally or for a specified purpose, with respect to that other person. If, at any time, there is a substantial question as to whether a person who purports to be acting on behalf of any individual is authorized to do so, the Plan will require proof acceptable to the Plan that the purported personal representative, is acting within the scope of his or her authority as a Personal Representative. However, except to the extent that the Plan has specific information to the contrary or that it appears unreasonable under the circumstances, the Plan ordinarily will assume that a parent of a minor child is an authorized personal representative of that child. Any reference in these Policies and Procedures to a right or a responsibility of an individual who is the subject of any Protected Health Information possessed by the Plan should be understood as referring also to an authorized Personal Representative of that individual.

Protected Health Information ("PHI") is individually identifiable health information. Health information is any information maintained or received by the Plan that relates to an individual's health condition, health care or payment for health care. Health information is individually identifiable if there is a reasonable possibility that the identity of the individual can be determined from the information. Specifically, health information is individually identifiable if it includes names, addresses or Social Security Numbers, or any other details from which an individual's identity might be determined under the context in which it has been released.

Any word or phrase used in this document that is defined in the Administrative Simplification Regulations should be understood as having the same meaning as applies under the Regulations.

USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

The Plan acknowledges that PHI is to be used or disclosed by the Plan only to the minimum extent necessary to operate the Plan.

The Plan's agents and representatives ordinarily will use or disclose PHI only for purposes of payment, treatment or health care operations (as defined below). However, PHI may also be used or disclosed for certain other purposes, but only as described in this document.

If PHI is to be used or disclosed for any purpose that is not otherwise permitted under this document, an individual authorization for that use or disclosure will be obtained, in advance, from any individual whose information is to be used.

If the Plan receives PHI subject to an individual authorization provided by the individual, the Plan will use or disclose PHI only as permitted under the authorization.

In addition, the Plan will disclose PHI only as required or permitted under the Regulations or applicable Federal or State law. Specifically, the Plan may disclose PHI as follows:

- To an individual, or a Personal Representative of an individual, who requests PHI relating to that individual. The Plan, in its discretion, may limit the release of information to an individual, to the extent that the disclosure is not required by the Regulations. For example, psychotherapy notes, information compiled in anticipation of litigation and information provided for certain research purposes, may be withheld, if the Plan determines it is not required (or is not permitted) to disclose the information.

- To any person or organization, as required for purposes of payment, treatment or health care operations. The Minimum Necessary Standard applies, except if PHI is being released to a provider for treatment purposes. In that case, the entire medical record may be released. However, psychotherapy notes will not be disclosed without individual authorization. PHI will be disclosed to any person or organization (for payment, treatment or health care operations purposes) only if the person or organization receiving the information is subject to the Regulations and to the terms of any applicable authorization or other restriction, either directly or through a Business Associate contract.

- To DHHS, if required under the Regulations, to enable DHHS to verify that the Plan is complying with applicable Regulations.

- To appropriate State authorities, to the extent that the Secretary of Health and Human Services has determined that the disclosure is necessary:

1. to prevent fraud and abuse relating to health care or payment for health care;
2. for purposes of State regulation of insurance or health plans, as authorized under applicable law;
3. for State reporting on health care delivery or costs; or
4. to serve a compelling public health, safety or welfare need, if the Secretary has determined that the intrusion into privacy is warranted when balanced against the compelling need for the disclosure.

- For law enforcement purposes, to the extent required under the Regulations or applicable State law.

MINIMUM NECESSARY STANDARD

If the Minimum Necessary Standard applies, the Plan will make reasonable efforts to limit the use or disclosure of PHI to the minimum amount necessary to accomplish the intended use or disclosure. In addition, when requesting information from a covered entity or a business partner, the Plan will make reasonable efforts to limit the amount of PHI requested to the minimum amount necessary for the intended use or disclosure.

The Minimum Necessary Standard applies to most routine uses and disclosures of PHI (such as for payment and health care operations purposes). However, it does not apply to:

- disclosures to providers for treatment purposes;
- uses and disclosures that are **required** for purposes of complying with the Regulations or with applicable law;
- uses or disclosures that are required to be made to DHHS; or
- disclosures to the individual who is the subject of the PHI or to a third party pursuant to a request initiated by the individual.

If reasonable under the circumstances, the Plan will disclose PHI for a stated purpose, without making an independent determination about whether the information disclosed is the minimum necessary, under the following circumstances:

- the information is requested by a public official, who represents that the information is the minimum necessary for the stated purpose;
- the information is requested by another covered entity;
- the information is requested by a professional employed by or performing services for the Plan, if he or she indicates that the information requested is the minimum amount needed for the intended purpose; or
- the information is requested for research purposes and proper documentation has been provided (as determined under section 164.512(i) of the Regulations).

The Plan will develop and adhere to consistent policies regarding routine recurring uses and those policies are incorporated into this document by this reference.

For non-routine uses and disclosures that are subject to the Minimum Necessary Standard, the determination of the minimum necessary amount will be made on an individual basis.

SECURITY AND CONFIDENTIALITY OF PROTECTED HEALTH INFORMATION

The Plan periodically assesses potential risks and vulnerabilities regarding PHI in its possession to develop policies and procedures designed to safeguard protected information from loss or unauthorized use or disclosure. Procedures and policies are reviewed periodically for adequacy and compliance with applicable law. Those policies and procedures are revised as needed.

The Plan has adopted the following procedures to limit access to PHI to only those persons who must have access to that information to perform Plan functions:

Employee Benefit Staff Procedures:

- Access to paper and computer files containing PHI is limited to employees or service providers who need access to such information to help operate the Plan.

- Paper files are kept in secure locations, e.g., in offices that are locked when authorized personnel are not present or in locked filing cabinets.

- Care is taken to minimize incidental disclosure of PHI to unauthorized employees, clients or service providers. For example, although employees and Business Associates who are authorized to access PHI may use various means to communicate with each other about information that includes PHI (e.g., conversations in person or by telephone or messages sent by fax, mail or email), reasonable efforts are made to reduce the likelihood that those communications will be overheard or viewed by unauthorized people.

- Electronic files are kept on secure systems, with access available only to authorized personnel. Passwords are used to ensure that only authorized personnel can access PHI included in electronic files. Passwords are comprised of seven (7) or more characters and are changed frequently. Authorized users are limited to one log-on at one time. Passwords are deactivated as soon as the user's employment is terminated or if the user is no longer authorized to access files containing PHI.

- Workstations with access to electronic files are protected against unauthorized use. Authorized employees log off of computers or secured networks before leaving the office at the end of the day. Screen savers will automatic activate after 7 minutes of inactivity. These screen savers will require a password to re-activate.

- Routine audits are conducted to monitor access to protected information, including access, log-ins, updates and edits.

- Use of electronic files is tracked by user, to discourage unauthorized access.

- Remote access to electronic files is limited to the benefit software consultant. This would be used for updating, changing, or improving system design specifications to enrollment information shared with carriers.

- Copying, printing and downloading of electronic files are limited. To override the limit, approval from the designated Privacy Official is required.

- Inactive files are stored in locked file cabinets or archived in secure locations.

- Paper copies of records containing PHI that are no longer needed are returned to the entity that provided the records or are shredded or burned or disposed of in some other way that reduces the risk of accidental disclosure.

- Phone calls are screened so that the staff verified the authenticity of the individual who calls with questions on their account. Personal information will be shared with the covered employee only.

- Care is taken so that individuals who are not responsible for protecting health information do not overhear conversations. The Benefit Supervisor has an office, which will be used for all private conversations. In addition, the Employee Benefit Office staff must be mindful so that they do not discuss benefit matters outside of the office.

Controller's Office Staff Procedures:

- The collection and payroll staff of the Controller's Office will have access to PHI in their normal course of administrative work. This information will be properly maintained, secured and protected from unauthorized use or disclosure. PHI will be protected in their custody.

- The collection staff should only discuss payment on benefit invoices with either the Pastor, Entity Director, Business Manager or the individual if it is an extended coverage receivable.

Monthly Entity Invoice Procedures:

- Each entity will receive a monthly Benefit of Caring invoice that will list the name of the individuals and the benefits that they elect. This information is supplied for the purpose of communicating payment information. This document is considered PHI.

- The invoice has employee benefit details as well as a summary information page. The Pastor, Business Manager or Entity Director should separate the employee benefit details from the summary page of the invoice. The employee benefit detail page(s) should be secured and used only to verify coverage and payment. **This information must not be used in any unauthorized manner, according to the HIPAA regulations.** Once payment has been made to the DRVC for these amounts, the employee benefit detail page should be maintained in a locked and secure location.

- The Entity representatives must read and acknowledge the procedures related to

the securing of the monthly invoices. The Entity must designate no more than two individuals who are authorized to receive, review and discuss the details of those invoices with the Employee Benefit Office. That authorization will be kept on file with the Employee Benefit Office.

- The Entity representatives must exercise care in conversations concerning benefits. They should always refer the employees to the insurance carriers for benefit assistance and consultation. The Employee Benefit Office should be consulted whenever employees have questions regarding qualified changes, open enrollment, and other administrative matters.

DESIGNATION OF PRIVACY OFFICIAL

Until further notice, Ellen R. Huling is designated by the Plan as the Privacy Official who will coordinate the implementation and management of the Plan's privacy policies. The Privacy Official will regularly monitor the Plan's compliance with the relevant requirements of the Privacy Rule. Initial implementation will be completed on or before April 14, 2003.

COMPLAINT POLICY

The Plan will provide a process for individuals to file complaints concerning the Plan's privacy policies and procedures or about any perceived violation of the individual's privacy rights.

No individual will be intimidated or retaliated against for filing a complaint. Employees who violate this policy are subject to disciplinary action, up to and including termination.

Until further notice, the Privacy Officer will be responsible for receiving and investigating complaints submitted to the Plan. All mail will be received by the Privacy Officer unopened and this will include email.

Complaints must be filed in writing with the Plan's designated complaint contact person. However, a complaint is deemed to be submitted in writing to the Plan if a designated complaint contact person agrees to accept a complaint provided in person or over the telephone and documents the complaint on a Complaint Report Form. A complaint is received by the Plan on the date the written complaint (or Complaint Report Form completed by a designated contact person) is submitted to (or completed by) a designated complaint contact person.

A designated complaint contact person will investigate each properly filed complaint. The Plan and the DRVC will make all reasonable efforts to cooperate and to facilitate the investigation.

A written response will be provided to the individual within sixty (60) days from the date the complaint was filed.

A written summary of the complaint and action taken will be filed with the Privacy Officer.

Translators, interpreters, and readers who meet the communication needs of the individual may be provided during the complaint process.

An individual may designate a representative of their choice to represent their interests during the complaint process.

Complaints that raise potential liability issues will be referred to the appropriate DRVC employee or officer responsible for risk management.

At the option of any individual who has a complaint, a complaint may also be filed with the Department of Health and Human Services, Office of Civil Rights. The Plan will cooperate with any investigation of such a complaint.

All complaints received and all complaint dispositions will be documented and the documentation will be retained for at least six (6) years.

PLAN DOCUMENTS\INSURANCE CONTRACTS POLICY

The Plan will insure that the governing Plan documents, and, where applicable, the insurance contracts under which Plan benefits are provided include provisions required by the Regulations. The Plan will provide PHI to the Plan Sponsor only if and to the extent that the Regulations and the governing Plan documents permit such disclosure.

AMENDMENT OF PROTECTED HEALTH INFORMATION

If an individual feels that PHI maintained by the Plan in a Designated Record Set is inaccurate or incomplete, he or she may request an amendment or correction of that information.

A request for an amendment or correction of PHI must be made in writing to the Plan's Privacy Official, must specify the PHI to be amended and must state a reason for the request.

The Plan may deny a request for amendment, if the Plan determines that the PHI or record that is the subject of the request:

- was not created by the Plan (unless the individual provides information to the Plan explaining why the originator of the PHI is no longer available to act on the requested amendment);
- is not part of the individual's health record;
- would not be available for inspection under federal law; or
- is accurate and complete.

The Plan will respond to a request for an amendment within sixty (60) days after it

receives the individual's request. In certain cases, the Plan may take up to an additional thirty (30) days to respond to the request. In those cases, the Plan will provide a written statement of the reasons for the delay and the date by which the Plan expects to complete its action on the request.

If the Plan grants the individual's request for amendment, in whole or in part, the Plan will:

- amend the PHI or record that is the subject of the request for amendment;
- inform the individual that the amendment is accepted and ask the individual to identify the relevant persons with whom the amendment should be shared and agree to have the Plan notify those persons; and
- within a reasonable time after receiving the individual's permission to notify the relevant parties, the Plan will provide the amended information to persons identified by the individual, and persons, including Business Associates, that the Plan knows have the 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 individual.

If the Plan denies a requested amendment, in whole or in part, the Plan will provide a timely, written denial in plain language that includes:

- a description of the basis for the denial;
- a description of the individual's right to submit a written statement disagreeing with the denial and the procedure for filing such a statement;
- a statement that, if the individual does not submit a statement of disagreement, the individual may request that the Plan provide the individual's request for amendment and the denial with any future disclosure of the PHI that is the subject of the amendment; and
- a description of the Plan's complaint procedures. The description will include the name, or title, and telephone number of the contact person or office responsible for receiving complaints.

The Plan will permit the individual to submit a written statement disagreeing with the denial of all or part of the requested amendment and the basis of such disagreement. The Plan may reasonably limit the length of the statement.

The Plan may prepare a written rebuttal to the individual's statement of disagreement. If a rebuttal is prepared, the Plan will provide a copy to the individual who submitted the statement of disagreement.

The Plan will identify the record or PHI that is the subject of a disputed amendment and link the individual's request for an amendment, the Plan's denial of the request, the individual's statement of disagreement, if any, and the Plan's rebuttal, if any.

If the individual has not submitted a written statement of disagreement, the Plan must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of PHI only if the individual has requested such action.

When a subsequent disclosure is made using a standard transaction that does not permit the additional material to be included, the Plan must separately transmit the material required to the recipient of the standard transaction.

If the Plan is informed by another covered entity of an amendment to an individual's PHI the Plan will amend the PHI in written or electronic form.

SANCTIONS AND MITIGATION

The Plan will work with the Plan Sponsor to investigate potential violations of the Privacy Regulations or of these Policies and Procedures. The Plan will, to the extent practicable, work with the Plan Sponsor and, if appropriate, with any affected Business Associates to mitigate the harmful effects of any violation of which the Plan is aware.

After any investigation or discovery of a violation, if an employee or other agent of DRVC is determined to be responsible, in whole or in part, for a violation of the Regulations or these Policies and Procedures, the Privacy Officer (or another designated person acting on behalf of the Plan) will work with the Plan Sponsor to see that appropriate remedial or disciplinary action is taken, based on the severity of the violation and the culpability of the employee or other agent. The Privacy Officer (or his or her delegate) generally will follow the following general guidelines:

- If the Privacy Officer (or his or her designate) determines that the individual's involvement in the violation resulted from a misunderstanding of the relevant Policy or Regulations or was otherwise unintentional, the individual generally will receive additional training regarding the Plan's privacy procedures or will be reassigned to other duties, if appropriate.

- If the Privacy Officer (or his or her designate) determines that the individual's involvement in the violation was intentional and knowing, additional training or reassignment may be required. In addition, more severe sanctions will be recommended, if appropriate. In appropriate circumstances, these sanctions could include a suspension or termination of employment.

- If the Privacy Officer (or his or her designate) determines that a criminal violation has occurred or that a violation should be reported to any Federal or State agency, the Privacy Officer will report the violation as appropriate and the Plan will cooperate with any investigation.

Notwithstanding the above guidelines, the Plan Sponsor will bear final responsibility for determining the appropriate sanction, if any, and reserves the right to impose any sanction (or none) that it determines, in its absolute discretion, is appropriate. Any disciplinary action will be subject to the Plan Sponsor's general employment policies, including the requirements of any applicable collective bargaining agreement.

RECORDKEEPING

The Plan will maintain health information privacy records and documents required to be maintained by the Plan pursuant to Section 164.530(j) of the Privacy Rule. Records to be kept include:

- a copy of this "Summary of Policies and Procedures under the HIPAA Administrative Simplification Regulations" and any subsequent document which is intended to satisfy the "policies and procedures" standard of Section 164.530(i) of the Privacy Rule;
- a copy of any document used by the Plan as a "Notice of Health Information Privacy Practices" to be provided to participants;
- a copy of any communication that is required under the Privacy Rule to be in writing; and
- documentation of any action, activity or designation that is required under the Privacy Rule to be documented.

Such records will be kept for at least six (6) years after the date the record is created. For documents such as this "Policies and Procedures" document or any "Notice of Health Information Privacy Practices" provided to Plan participants, a copy of the document will be kept for at least six (6) years after the last date on which the document is in effect. Records may be maintained in electronic or written form.

SAFEGUARDS

The Plan will maintain appropriate administrative, technical and physical safeguards to protect the privacy of PHI. The Plan will comply with all applicable requirements of the Security Rule, on or before the required compliance date.

TRAINING

The Plan and the DRVC will see that each DRVC employee who requires access to PHI relating to the Plan receives appropriate training regarding the relevant requirements of the Regulations and of these Policies and Procedures. The Plan will provide additional training to all such employees, as needed, following any relevant change to the Plan's policies and procedures. Each employee's compliance with the requirements of the regulation will be periodically monitored and employees will receive additional training if appropriate.

The Plan will maintain appropriate records regarding each employee's completion of training requirements. Specifically, the Plan will require each employee who receives such training to review and sign a document that provides an overview of the health information privacy requirements.

REQUIRED HEALTH PLAN NOTICES

The Plan will maintain a "Notice of Health Information Privacy Practices" ("Privacy Notice") that describes the Plan's health information privacy practices for Plan participants. The Plan will comply with the requirements specified in the Plan's

Privacy Notice, which is incorporated into these Policies and Procedures by this reference. The Privacy Notice is intended to be and, where reasonable, is to be construed to be consistent with the Policies and Procedures described in the body of this document. To the extent that there is any conflict between the requirements specified in the Privacy Notice and in any other part of these Policies and Procedures, the Privacy Notice, as interpreted by the Plan Administrator and to the extent that the Privacy Notice is consistent with the requirements of the Regulations, will prevail.

To the extent required by the Privacy Rule, the Privacy Notice will be distributed as follows:

- Before April 14, 2003, to all employees who participate in the Plan, as of that date;
- Upon enrollment, to any employee who enrolls in the Plan after April 14, 2003; and
- Within sixty (60) days of any material revision to the Notice; to all employees who participate in the Plan.

In addition, at least once every three (3) years, the Plan will inform current employees who participate in the Plan that the Notice is available and that a participant may obtain a copy of the Notice by requesting one from the Employee Benefit Office. This information may be included in the Plan's summary plan description or other documents provided to participants as long as that approach satisfies the requirement mentioned in the previous sentence.

The Privacy Rule does not require the Plan to automatically distribute a privacy notice to non-employee participants. However, the Plan's Privacy Notice will be available upon request to anyone covered under the Plan.

The Plan may choose to distribute a Privacy Notice by email or other electronic means permitted under the Privacy Rule. In addition, any website (on the Internet or on an internal Intranet) that provides information about employee benefits to employees will include a link to a copy of the Privacy Notice, which will be available for download. However, a paper copy of the Notice will always be available upon request to any participant.

Notwithstanding the above, the Privacy Rule does not require the Plan to automatically distribute a Privacy Notice to participants in any fully-insured health plan or coverage option covered by these Policies and Procedures. Instead, the insurance issuer is required to provide a notice for such participants. However, the Plan's Privacy Notice will be available upon request to participants in any insured health plan covered by these Policies and Procedures.

ELECTRONIC TRANSACTIONS

Effective beginning October 16, 2003, the Plan, together with its Business Associates, where appropriate, will comply with all applicable requirements of the

Electronic Transactions Standards when engaging in a covered transaction. The Plan will begin testing its software and systems, as required by the Electronic Transactions Standards, on or before April 16, 2003. In addition, the Plan's contracts with any Business Associate will include provisions requiring the Business Associate to conduct any covered transaction engaged in on behalf of the Plan according to the applicable standards.

BUSINESS ASSOCIATE AGREEMENTS

Any Business Associate of the DRVC or the Plan will be required, as a condition for receiving PHI from or on behalf of the Plan on or after April 14, 2003 (or for using, disclosing or continuing to maintain PHI previously received from or on behalf of the Plan after that date), to comply with the requirements of the Administrative Simplification Regulations, as they apply to the Plan. On or before the date required under the Privacy Rule, the Plan or the DRVC will enter into a written agreement (or will modify an existing agreement) that meets the Business Associate agreement requirements of the Privacy Rule, as they apply to the Plan.

Employee Health Plans of the DRVC

MINIMUM NECESSARY PROCEDURES FOR RECURRING USES OR DISCLOSURES OF PROTECTED HEALTH INFORMATION

For common uses or disclosures of Protected Health Information ("PHI"), the health plans sponsored by the DRVC for its employees (the "Plan") have developed standard procedures for complying with the Minimum Necessary Standard of the Health Information Privacy Regulations. For other uses or disclosures, the Plan determines the minimum necessary amount on a case by case basis.

The following charts describe the Plan's procedures for dealing with certain types of routine uses and disclosures. The first chart describes the types of uses and disclosures to which the Minimum Necessary Standard does not apply. The second chart describes common uses and disclosures of PHI to which the Minimum Necessary Standard does apply and specifies the Plan's policies for complying with that standard. These charts are reviewed on a regular basis and revised as needed.

Table 1: Minimum Necessary Standard does not apply

TYPE OF USE OR DISCLOSURE	PROCEDURE
Disclosure of an individual's health information to that individual or an authorized personal representative upon request	The Plan will disclose as requested, subject to limits described in the Plan's Health Information Privacy Policies and Procedures and in applicable Regulations. (Disclosure to a personal representative will be limited to information relating to that representative's authority to represent the individual.)
Disclosure to provider for treatment purposes	The Plan will disclose as requested, subject to limits described in the Plan's Health Information Privacy Policies and Procedures and in applicable Regulations.
Disclosure pursuant to an individual authorization	The Plan will disclose as requested, subject to limits described in the Plan's Health Information Privacy Policies and Procedures and in applicable Regulations or in the authorization.
Disclosure to Plan Sponsor for Plan evaluation, amendment, termination purposes, insurance renewals or requests for premium quotes	Provide summary claim information only--no names, SSN, addresses, employee numbers, etc.
Disclosure to DHHS to monitor Plan compliance with regulations	The Plan will disclose as requested, subject to limits described in the Plan's Health Information Privacy Policies and Procedures and in applicable Regulations.

Employee Health Plans of the DRVC

MINIMUM NECESSARY PROCEDURES FOR RECURRING USES OR DISCLOSURES OF PROTECTED HEALTH INFORMATION - Continued

TYPICAL USES OR DISCLOSURES AND THE PROCEDURES FOR COMPLYING WITH THE MINIMUM NECESSARY STANDARD.

Table 2: Routine uses or disclosures that are subject to the Minimum Necessary Standard	
TYPE OF USE OR DISCLOSURE	**MINIMUM NECESSARY PROCEDURE**
Disclosure to another covered entity	The Plan will not make an independent determination of the minimum necessary amount, if it appears reasonable under the circumstances to provide the information requested for the intended use or purpose
Disclosure to a professional who performs services for the Plan	The Plan will not make an independent determination of the minimum necessary amount, if it appears reasonable under the circumstances to provide the information requested for the intended use or purpose. This will include auditors, accountants, attorneys and benefit consultants.