



SOUTH GROVE EYE CARE PC

Abbey C Hoffman OD and Regina R Harvey OD

Notice of Privacy Practices

Effective Date: October 16, 2006

2020 S SR 135
Suite 200
Greenwood IN
46143

PHONE (317) 535-3935
FAX (317) 535-3905
WEB SITE www.southgroveeyecare.com

I. NOTICE OF PRIVACY PRACTICES

In order to comply with HIPAA's Privacy Rule, it is the policy of South Grove Eye Care PC (SGEC) to:

1. Make available a Notice of Privacy Practices ("NPP") to every patient at their first appointment, eyewear pickup, or similar encounter on or after October 16, 2006.
 - A copy of our NPP(extended version) is available to the patient upon request.
 - A copy of our NPP (overview version) is also available upon request. (Addendum A)
 - SGEC must ask the patient to sign an acknowledgement of receipt of the NPP ("AOR") (Addendum A). These will be kept in the Business Office.
 - If the patient opts not to sign the AOR, it will be noted the patient refused. This note will be kept in the Business Office.
 - It is not necessary to give an NPP to a patient every time they come in after October 16, 2006, unless SGEC changes the NPP (see below).
 - * At every patient encounter SGEC must look to see if a signed AOR is available.
 - * If available, it is not necessary to give that patient another NPP. Our most current NPP will always have an effective date on the front.
 - * If no, then it is necessary to distribute a NPP and ask for signature on an AOR.
 - If our first encounter with a patient after October 16, 2006, is electronic, our electronic system will automatically send an NPP and ask for a signed AOR.
2. Only SGEC has authority to change this NPP. If this happens, we will follow the same procedures above.
3. We will use and disclose protected health information in a manner consistent with HIPAA and with our NPP. If we change our NPP, the revised NPP will apply to all protected health information we have, not just protected health information we generate or obtain after we have changed the NPP.

II. NO AUTHORIZATION IS REQUIRED TO MAKE CERTAIN DISCLOSURES OF PROTECTED HEALTH INFORMATION

In order to comply with HIPAA's Privacy Rule, it is the policy of this office to obtain a signed patient authorization before making a use or disclosure of protected health information, except in those circumstances in which HIPAA does not require such an authorization. As stated in HIPAA, we will not obtain a signed patient authorization in the following circumstances of use and disclosure for treatment, payment, or health care operations:

- Providing care to patients in our office
- Seeking assistance from consultants
- Making referrals of patients for follow-up care
- Writing, sending, and filling prescriptions for drugs and eyewear or contact lenses
- Preparing and submitting claims and bills
- Receiving/posting payments, and collection efforts
- Managed care credentialing
- Professional licensure and specialty board credentialing
- Quality assurance
- Financial audits/management
- Training of professional and non-professional staff including students
- Office management
- Fraud and abuse prevention activities
- Personnel activities

Other uses and disclosures:

1. Disclosures to business associates with signed business associate contracts with us. (Addendum K)
2. Disclosures required by our state law, provided we disclose only the precise protected health information required and only to the recipient required.
3. Disclosures to state, local or federal governmental public health authorities to prevent or control disease, injury, or disability.
4. Disclosures to local, state, or federal governmental agencies to report suspected child abuse or neglect.
5. Disclosures to individuals or organizations under the jurisdiction of the federal Food and Drug Administration (“FDA”), such as drug or medical device manufacturers, regarding the quality or safety of drugs or medical devices.
6. Disclosures to local, state, or federal governmental agencies in order to report suspected abuse, neglect, or domestic violence regarding adults, provided we:
 - a. Get an informal agreement from the patient unless:
 - We are required by law to report our suspicions.
 - We are permitted, but not required by law, to disclose the protected health information, and we believe a report is necessary to prevent harm to our patient or other potential victims.
 - b. We tell the patient we are making this disclosure, unless:
 - Telling the patient would put the patient at risk for serious harm, or
 - Someone else is acting on behalf of the patient, and we think this person is the abuser and telling him or her would not be in the best interest of the patient.
7. Disclosures for health oversight audits, investigations, or disciplinary activities, provided we only disclose to a federal, state or local governmental agency (or a private person or organization acting under contract with or grant of authority from the governmental agency) which is authorized by law to conduct oversight activities.
8. Disclosures in response to a court order, provided we disclose only the precise protected health information ordered, and only to the person ordered.
9. Disclosures in response to a proper subpoena, provided:
 - a. We make sure either SGEC or the person seeking the subpoenaed information makes a reasonable effort to notify the patient in advance. The patient has a chance to object to the court about the disclosure
 - b. We make sure either SGEC or the person seeking the subpoenaed information makes a reasonable effort to have the court issue a protective order.
10. Disclosures to police or other law enforcement officers regarding a crime we think happened at our office, provided we reasonably believe the protected health information is evidence of a crime.
11. Disclosures to organizations involved in the procurement, banking, or transplantation of eyes in order to facilitate eye donation and transplantation.
12. Uses of protected health information to market or advertise our own health care products or services, or for any other marketing exception.
13. Disclosures to a researcher with a waiver of authorization from an IRB or privacy board; to a researcher using the protected health information only for purposes preparatory to research or to a researcher only using the protected health information of deceased patients, provided the researcher gives us the assurances required by HIPAA.
14. If at any time a proposed use or disclosure does not fit into one of these exceptions to the need for an authorization described in these exceptions, we will obtain a signed patient authorization before making the use or disclosure.

III. PROVIDING INFORMATION TO FAMILY AND FRIENDS OF PATIENTS INVOLVED IN CARE

In order to comply with HIPAA’s Privacy Rule, it is the policy of this office to give patients a chance to agree or object to providing protected health information to close family or friends who are helping with the patient’s care.

1. If we feel it necessary or appropriate to inform a close family member or friend who is involved in a patient’s care about certain protected health information relevant to their involvement, we will give the patient a chance to agree

or object to such disclosure before we make it. If the patient is present or available when this need arises, we will do any of the following:

- Get an oral agreement from the patient that the disclosure is acceptable.
- Give the patient a chance to object to the disclosure.
- Infer from the circumstances that the patient does not object. For example, we can reasonably infer the patient does not object if the family member or friend is in the examining room with the patient.

If the patient is not present or available when the need arises, we will use our best judgment about whether it is in the patient's best interest to disclose the information. An example might be when a family member or friend, as a convenience to the patient, comes to our office to pick up eyewear the patient previously ordered.

2. If we make a disclosure to a close family member or friend under the circumstances noted in paragraph 1, we will only disclose information which is relevant to the family member or friend's involvement with the patient's care. Examples:

- If the patient's spouse will pick up ordered eyewear, we will provide the eyewear but not disclose any diagnoses or special features of the eyewear.
- If a son or daughter will assist a patient with eye drops, we will provide information about when and how the drops should be administered, but will not disclose the patient's diagnosis.

3. If someone claiming to be a family member or friend of the patient initiates contact with us seeking information, we will:

- Verify the identity of the caller and their relationship to the patient.
- Determine if they are involved in the patient's care.
- Determine if the patient is available (by phone, email, or other communications method) to either agree or object to the disclosure. If so, we will give the patient the chance to agree or object. If the patient objects, we will not disclose any information to the caller. If the patient is not available by any reasonable means, we will use our best judgment to determine whether disclosure of information is in the patient's best interest.

IV. MARKETING AND ADVERTISING

In order to comply with HIPAA's Privacy Rule, it is the policy of this office to base require or not require a signed patient authorization to use or disclose protected health information for marketing or advertising purposes subject to the conditions and exceptions described in this policy. Marketing means to make a communication which encourages a person receiving the communication to purchase a product or service.

1. We may use protected health information in connection with a marketing communication if we review patient databases or records to target specific recipients. We may disclose protected health information in connection with a marketing communication if the content includes protected health information, ie photographs, testimonials, etc.
2. If a marketing communication discloses protected health information outside the policies of the NPP, we will get a signed patient authorization.
3. If we use protected health information in connection with a marketing communication, we will get a sign patient authorization with the exception of:
 - Marketing communications about our own health care products or services.
 - Communications made in the course of treatment, case management, or care coordination for an individual patient; for example, sending recall Correspondence Cards
 - Communications made during a face-to-face encounter with a patient.

4. Communications falling into these specified categories do not require a signed patient authorization:
- Any marketing communication which does not require a signed patient authorization must be included in our accounting of disclosures available to a patient upon request.
 - When we need an authorization, we will include information about any money or other valuable thing we get from someone else in connection with the communication.
 - Many marketing communications do not use or disclose protected health information. These communications are not affected by HIPAA's Privacy Rule. Examples of these communications are:
 - *general TV ads
 - *brochures mailed to "occupant" using a zip code data base
 - SGEC is responsible for obtaining signed patient authorizations for marketing, when they are required, and for making sure the authorization discloses any money or thing of value we get from someone else in connection with the marketing communication.

V. DESIGNATED RECORD SET

In order to comply with HIPAA's Privacy Rule, this office designates the following records to be our "designated record set" for purposes of patients' right to access and amend their protected health information:

1. The patient's clinical chart, hard copy or electronic:
 - reports of screening and diagnostic tests
 - notes on examinations
 - consultant reports
 - refraction results
 - eyewear prescriptions
 - history and medication reports
 - all other clinical information
2. The patient's billing records, hard copy or electronic:
 - insurance claims
 - remittance advice from insurance companies
 - electronic fund deposit receipts
 - bills to patients
 - evidence of payment by patients
 - collection records
 - referrals to collection agencies or attorneys
 - reports to consumer credit agencies for unpaid balances
 - all other billing, claim, payment and collection records
3. Eyewear order and receipt forms specific to a particular patient, hard copy or electronic:
 - orders for glasses
 - orders for contact lenses
 - acceptance of delivery of ordered eyewear
 - patient pick up records
 - repair requests and documentation of completion
 - fitting information
 - distribution of eyewear accessories
 - any other records relating to eyewear

4. Other information in any form used by SGEC to make decisions about a particular patient. This does not include any documents created in connection with litigation.

VI. PATIENTS' ACCESS TO THEIR PROTECTED HEALTH INFORMATION

In order to comply with HIPAA's Privacy Rule, it is the policy of this office to allow patients to inspect and/or copy their own protected health information under the conditions stated in this policy. If the patient has a personal representative, the personal representative can inspect or copy the patients protected health information on behalf of the patient.

1. We require patients to send a written request to inspect or copy their protected health information. If a patient calls on the telephone asking to inspect or copy their protected health information, we will inform the patient of the requirement to send the request in writing.
2. We will respond to a patient's request to inspect or copy their protected health information within 30 days of receiving the written request, or 60 days if the protected health information is stored off-site. If we need more time, we can have one 30 day extension, but we must notify the patient in writing of the extension before the original time period expires. (Addendum B)
3. We can deny the patient's request only for one or more of the following reasons:
 - a. A patient cannot inspect or copy information if it was prepared in connection with a lawsuit.
 - b. A patient cannot inspect or copy information if it is generated as part of the patient's participation in a clinical trial and the request is made during the clinical trial. We must have informed the patient about this restriction when the patient signed up for the clinical trial. The patient must be allowed to inspect or copy this information when the clinical trial is over.
 - c. A patient cannot inspect or copy information if we received it someone else who is not a health care provider and we promised that person his/her identity would remain confidential.
 - d. A patient cannot inspect or copy information if we, or another health care professional, determine this would likely endanger the life or physical safety of the patient or someone else.
 - e. A patient cannot inspect or copy information if it references someone else, and we, or another health care professional, determine that access would likely cause substantial harm to such other person.
 - f. A patient's personal representative (for example, legal guardian, or parent of a minor) cannot inspect or copy information about the patient if we, or another health care professional, determines this would likely cause substantial harm to the patient or another person.
 - g. A patient cannot inspect or copy information which is not in a designated record set (ref. section V)
4. If we deny a patient access to their protected health information, we will notify the patient of our decision in writing. (Addendum C)
6. If the denial is based upon reasons 4 d, e, or f, the patient has a right to a review of our decision.
 - a. The owners of SGEC will handle the review.
 - b. We will look at the information the patient wants to inspect or copy, and decide if we were correct in thinking the patient's circumstances meet the specifications of paragraph 4d, e, or f.
 - If not, the patient may inspect or copy the information.
 - If so, the patient may not inspect or copy the information.

The patient may not further question our decision. Our notice to the patient will include instructions about how the patient may take advantage of this review right. We will use the denial notice letter accompanying this policy.

7. When a patient is granted access to view or copy the requested information, we will:

- a. Notify the patient in writing. (Addendum D)
- b. Provide the information in the form or format the patient requests, if we can reasonably produce it that way. If we cannot, we will either agree with the patient about another format or give it to the patient in hard copy.
- c. Allow the patient to inspect or copy the information at our office during normal business hours as pre-arranged. Within certain limits, the patient may select the date and time to inspect or copy the records.
- d. There may be a charge for copying the requested information for the patient. If the patient wants the information mailed to him or her, there may also be a charge for the cost of mailing or any special delivery method the patient wants us to use.
- e. If the patient agrees in advance, we may summarize the requested information and give this to the patient instead of having the patient inspect all the information or copy all of it. If we do this, we may charge the patient the cost of preparing the summary.
- f. Any charges need to be paid in advance.

VII. AMENDMENT OF PROTECTED HEALTH INFORMATION

In order to comply with HIPAA's Privacy Rule, it is the policy of this office to permit patients to request us to amend their protected health information under the conditions stated in this policy. If the patient has a personal representative, the personal representative may exercise this right on behalf of the patient.

1. We require all requests to amend protected health information be in writing. If a patient calls on the telephone to request an amendment, we will inform the patient of the requirement to submit this request in writing.
2. We will respond to requests for amendment within 60 days after we receive the written request. We can have one 30-day extension if we notify the patient we need this additional time before the original time period expires. (Addendum E)
3. We can deny a requested amendment only for one or more of the following reasons:
 - The information is accurate and complete as it is.
 - We did not create the information.
 - The information is not in a designated record set (ref. section V)

The patient would not be able to inspect or copy the information.

4. If we deny a request, we will notify the patient in writing (Addendum F). We will inform the patient of the right to either submit a statement of disagreement or to have the original amendment request accompany the information.
5. If we grant the requested amendment, we will notify the patient (Addendum G). We will:
 - Append or link the corrected information to the information we are holding.
 - Send the corrected information to anyone who we know has previously received the incorrect information.
 - Send the correct information to anyone the patient requests.

VIII. ACCOUNTING FOR DISCLOSURES OF PROTECTED HEALTH INFORMATION

In order to comply with HIPAA's Privacy Rule, it is the policy of this office to provide our patients, upon request, with an accounting of disclosures we have made of their protected health information during the six years preceding their request, subject to the terms and conditions stated in this policy.

1. We will provide an accounting of our disclosures of a patient's protected health information, except for:
 - a. Disclosures for treatment, payment, or health care operations
 - b. Disclosures made with a signed patient authorization
 - c. Disclosures incident to other permitted disclosures.
 - d. Disclosures to the patient personally
 - e. Disclosures to family or friends involved in a patient's care
 - f. Disclosures of a limited data set
 - g. Disclosures made before October 16, 2006
2. In order to be able to provide an accounting when a patient requests one, we will keep track of disclosures except for those disclosures listed in paragraph 1. Only SGEC is authorized to make a disclosure of protected health information not listed in paragraph 1. All disclosures will be documented electronically (Addendum H) for up to six years and will include:
 - a. The date of the disclosure
 - b. The name and address (if known) of the person or organization who got the information
 - c. A description of the disclosed protected health information
 - d. A statement of the purpose or basis for the disclosure, or a copy of any request for the protected health information which prompted the disclosure.
3. We require all requests for an accounting be made in writing. If a request is made by telephone, we will advise the caller to submit a written request.
4. We will respond to a request for an accounting within 60 days from our receipt of the written request. If we are unable to provide the accounting within this 60 day period, we may have an additional 30 days, provided we notify the patient of this delay before the original 60 day period expires. This notice will include the reason for the delay and the date we will have the accounting ready. (Addendum I)
5. Our accounting will list all the information described in paragraph 2 of this policy. We will use the same electronic method as stated in paragraph 2 to make our accounting. If we make repeated disclosures of protected health information about a patient to the same person or organization for the same purpose, our accounting will provide all of this information for the first such disclosure, and then indicate the frequency or periodicity of the other disclosures, and the date of the last such disclosure.
6. We will provide patients with one free accounting, upon request, within any 12 month period. For additional accountings there may be a charge payable in advance.

IX. RESTRICTIONS ON USE OF PROTECTED HEALTH INFORMATION

In order to comply with HIPAA's Privacy Rule, it is the policy of this office to permit patients to request we restrict the way we use some protected health information for purposes of treatment, payment, or health care operations.

1. SGEC will accept requests from patients for restrictions on the way we use protected health information for treatment, payment, or health care operations.

2. We may not agree to restrictions requested by patients; however, in unusual circumstances we may agree to the requested restriction.
3. If we agree to a requested restriction, we will document its terms; this will be kept in the Business Office. The staff of SGEC will be informed of the terms of restriction. It might be possible one or more of our business associates will also need to know.
4. We will honor any restriction we have agreed to. However, no restriction can prevent us from using any protected health information in an emergency treatment situation.
5. If we have agreed to a restriction but can no longer practically honor it, we will do either of the following:
 - a. Contact the patient to work out a mutually agreeable termination of the restriction. This agreement will be kept in the Business Office.
 - b. Contact the patient and advise we are no longer able to honor the restriction we previously agreed to. This notice will only apply to protected health information we obtain or generate after the notice is given.

X. CONFIDENTIAL COMMUNICATION METHODS WITH PATIENTS

In order to comply with HIPAA's Privacy Rule, it is the policy of this office to accommodate requests from patients to send protected health information to them in a confidential way, subject to the conditions in this policy.

1. If a patient requests we use a particular method to communicate with them in order to preserve the confidentiality of their information, we will accommodate if reasonably possible.
2. We require such requests be in writing. If a request comes in by telephone, we will advise the patient to send the request in writing.
3. We will not ask or require a patient to explain why they want the particular communication method.
4. We may charge the patient the reasonable cost of complying with their request, if any.

XI. MINIMUM NECESSARY USES AND DISCLOSURES OF PHI

In order to comply with HIPAA's Privacy Rule, it is the policy of this office to only use or disclose the minimum amount of protected health information necessary to accomplish the purpose for the use or disclosure, under the conditions and exceptions described in this policy.

1. People in the following job categories will only have access to the kind or amount of protected health information needed to perform their specific job duties including but not limited to the entire clinical chart, presenting symptoms, diagnosis, treatment, glasses or contact lens prescriptions, ocular:
 - a. All doctors and technicians
 - b. Insurance billers or other accounts receivable staff
 - c. Receptionist
 - d. Opticians
 - e. Other - at the discretion of SGEC

2. We will keep all clinical charts and billing records secure within our computer network when not in use. Only authorized staff has access to this secure storage. Computers are disabled when the user is away from the desk.
3. All staff will sign a “confidentiality agreement” indicating their commitment to access only the minimum amount of protected health information necessary for them to do their job, and to abide by the restrictions listed in paragraph 2. Violation of this agreement is grounds for employment discipline according to our personnel policies. (Addendum J)
4. When we get a request from a third party for protected health information about one of our patients, or whenever we intend to make a unilateral disclosure of protected health information about one of our patients, we will disclose only the minimum necessary amount of protected health information necessary to satisfy the purpose of that disclosure. This does not apply in the following cases:
 - a. The patient has authorized the disclosure.
 - b. The disclosure is for treatment purposes (for example, disclosures to a consultant or follow-up health care provider).
5. We will rely upon the representations of the following third parties which they have requested only the minimum amount of protected health information necessary for their purposes:
 - a. Another health care provider or health plan.
 - b. A public official, like a law enforcement officer.
 - c. Professionals providing services to us (such as attorneys or accountants).
 - d. Researchers supplying documentation of IRB waivers
6. SGEC is responsible for determining the minimum amount of protected health information necessary for us to disclose in situations which are not routine. We will consider the reason for the disclosure, whether it falls into either of the circumstances described in paragraph 4 of this policy, and the protected health information which we have, in making this determination.
8. Whenever we request protected health information about one of our patients from someone else, we will ask for only the minimum necessary amount of protected health information necessary for us to accomplish the purpose which prompted us to ask for the information.

XII. VERIFICATION BEFORE DISCLOSING PROTECTED HEALTH INFORMATION

In order to comply with HIPAA’s Privacy Rule, it is the policy of this office to verify the authority and identity of people or organizations who request us to disclose protected health information about our patients, subject to the conditions of this policy statement.

1. If a patient has a personal representative who seeks to sign an authorization to disclose the patient’s protected health information to a third party, or to exercise any of the rights patients have regarding their protected health information, we will take the following steps before we accept their signature or allow them to exercise those rights:
 - a. Ask for copies of any documents relevant to their status as personal representative. For example, we will ask for a copy of the court papers appointing a legal guardian, or a power of attorney designating someone to make health related decisions for an incapacitated adult.
 - b. We will ask for a picture identification of the person serving as personal representative.

2. We will review all documents we receive and make sure they in fact authorize the personal representative to control the patient's protected health information, and there are no limits or expiration dates affecting this authority.
3. If we receive a request from a third party to see or have a copy of protected health information we have about our patients without a signed patient authorization, we will take the following steps before we allow such access:
 - a. Ask the requestor for evidence they are affiliated with an organization or government agency authorized to have access to protected health information without an authorization. Evidence can include an official badge or identification card, an assignment on official letterhead, or similar items.
 - b. Ask the requestor for picture identification.
 - c. Ask the requestor to specify the legal authority the requestor believes allows access to protected health information.

For example, if we are asked by a representative of a drug or medical device manufacturer to supply protected health information relating to our use of a particular drug or device, we will make sure the representative is truly affiliated with the drug or device manufacturer; that the drug or medical device manufacturer is under the jurisdiction of the U.S. Food and Drug Administration; and that the drug or device manufacturer is seeking the information because of a quality or safety concern about a product they manufacture as provided in 45 CFR 164.512.

4. We will review all evidence supplied by the requestor to make sure they have proper authority to access protected health information and there are no limits or expiration dates affecting this authority.
5. If there are questions about these documents, we will work to resolve them. We will not disclose any protected health information until all questions are answered and we have proper evidence of the authority of the person acting as personal representative.

XIII. LITIGATION OF KNOWN HARM FROM AN IMPROPER DISCLOSURE OF PROTECTED HEALTH INFORMATION

In order to comply with HIPAA's Privacy Rule, it is the policy of this office to mitigate known harm from an improper disclosure of protected health information, when it is practicable to do so.

1. When we learn of harm caused by an improper disclosure of our protected health information, we will take reasonable steps to mitigate the harm. We will take these steps whether the improper disclosure was made by us or by one of our business associates.
2. We will determine what specific steps are appropriate to mitigate particular harm. It is our policy to tailor mitigation efforts to individual harm. Examples of some mitigation steps include:
 - a. Getting back protected health information which was improperly disclosed.
 - b. Preventing further disclosure through agreements with the recipient.
3. We do not consider money reparations to be appropriate mitigation.
4. If a business associate has made the improper disclosure, we will require the business associate to cure the problem to our satisfaction, or terminate our relationship with them.

XIV. HANDLING PATIENT COMPLAINTS ABOUT PRIVACY VIOLATIONS

In order to comply with HIPAA's Privacy Rule, it is the policy of this office to accept complaints from patients who believe we have not properly respected their privacy, and to thoroughly investigate and resolve them.

1. SGEC will accept all patient complaints about alleged privacy violations. We require all complaints to be in writing. If a complaint comes over the telephone, we will inform the patient to send it in writing. This can be hard copy or electronic, as the patient wishes. If a patient wishes to remain anonymous, we will accommodate that to the extent practical.
2. We will keep all patient complaints for at least six years. These will be stored, along with information about the investigation and resolution of the complaint, in the Business Office.
3. Upon receiving a patient complaint about privacy, it will be investigated. We have the discretion to conduct the investigation in the manner considered reasonable and logical in light of the nature of the complaint. Generally, we will do at least the following in order to investigate a complaint:
 - a. Talk to the person in the office the patient thinks violated the patient's privacy.
 - b. Review the patient's clinical chart.
 - c. Talk to other office staff about the patient's concern.
 - d. Talk to the patient.
 - e. Review any information or evidence the patient presents in support of the claim of a violation of privacy.
4. Based upon the results of the investigation, SGEC will determine whether or not the patient's complaint is substantiated. If not, the patient will be notified in writing. If it is substantiated, we will determine what steps are necessary to resolve the issue so it does not recur.
5. In determining what steps are necessary to resolve a substantiated complaint of a violation of privacy, we will consider at least the following points:
 - a. What caused the privacy violation?
 - b. If the violation was caused by a failure to comply with existing policy, the issue will be reported for action as a human resources disciplinary matter.
 - c. If the problem was caused by a lack of an appropriate policy, or an inadequate policy, SGEC will seek to determine how the policy should be changed, or if a policy needs to be developed. If policy revisions or new policies are needed, we will work to accomplish that.
 - d. If a business associate was involved in the violation, what must the business associate do to prevent the violation from reoccurring? If the business associate cannot cure the breach, the business associate contract may be terminated.
 - e. If the privacy violation caused harm, what steps are necessary to mitigate that harm? We will take necessary steps to mitigate that harm.
6. Once a resolution is determined, we will work to take the steps identified as necessary for resolution.
7. If new policies or procedures are put into place as part of the resolution, mandatory training will be conducted for our workforce regarding the new policies or procedures.
8. SGEC will develop a way to monitor whether the resolution is working to improve our privacy protections. If we discover problems through monitoring, we will work cooperatively to fix the problems.