

Goldsmith Eye Care, PC

Privacy

Policy Manual

112 Main St. E.
PO Box 261
New Prague MN 56071
952-758-2080

214 4th St. NE
PO Box
Gaylord MN 55334
507-237-2014

5116 Gateway St. S.E.
Suite 201
Prior Lake MN 55372
952-226-1400

7-1-2014

This manual and all associated forms and letters is copyrighted by Optometric Business Solutions. Any reproduction, unauthorized alteration, or other unauthorized use is prohibited and may result in legal action.

CONTENTS

POLICY

Entity Declarations.....	1A
Privacy Officer	2A
Public Information Officer	2B
Notice of Privacy Policy (NPP)	3A
Acknowledgement of NPP	3B
No Authorization Required.....	4A
Designated Record Set.....	5A
Limited Data Sets	5B
De-identification of PHI.....	5C
Disclosures for Research.....	6A
Marketing and Advertising	6B
Personal Representation	7A
Information to Family, Friends	8A
Minimum Necessary Use.....	9A
Patient Access, Inspecting, Copying	10A
Patient Amendment	11A
Disclosure Accounting	12A
Restrictions on Use of PHI.....	13A
Confidential Communication.....	14A
Handling Patient Complaints	15A
Safeguards to Privacy.....	16A
Business Associates.....	17A
Disaster Recovery Plan	18A
Privacy Contingency Plan.....	18B

FORMS AND LETTERS

Notice of Privacy Policy
Acknowledgement of Notice of Privacy Policy
Employee Confidentiality Agreement
Business Associate Contract
Patient Access, Copy letter-approval
Patient Access, Copy letter-delay
Patient Access, Copy letter-denial
Amend Request letter-approval
Amend Request letter-delay
Amend Request letter-denial
Accounting Request letter-approval
Accounting Request letter-delay
Accounting Request letter-denial
Special Accommodations letter-approval
Special Accommodations letter-denial

ENTITY DECLARATION

Policy Number: 1A

7-1-2014

1. Pursuant to HIPAA's Privacy Rule, the following organization elects to be considered as an Organized Health Care Arrangement for the purposes of compliance with the Privacy Rules:

Goldsmith Eye Care PC
PO Box 261 New Prague MN 56071

2. This organization and its affiliated entities will use and distribute a joint Notice of Privacy Practices and will otherwise comply with HIPAA's Privacy Rule as a single unit.
3. This organization disclaims any intention to affiliate for any purpose other than the HIPAA Privacy Rule compliance. For all other purposes, each affiliated entity is a legal entity as it exists outside of any relation to HIPAA Privacy Rules.

PRIVACY OFFICER

Policy Number: 2A

7-1-2014

In order to comply with HIPAA's Privacy Rule, Goldsmith Eye Care PC will have a Privacy Officer.

1. Duties of the PO will include:
 - a. create and implement policies and procedures to comply with HIPAA's Privacy Rule;
 - b. monitor compliance efforts;
 - c. respond to specific HIPAA Privacy Rule compliance questions;
 - d. conduct educational sessions for Goldsmith Eye Care PC's workforce about HIPAA requirements and Goldsmith Eye Care PC Privacy Rules;
 - e. Receive and investigate allegations of non-compliance, and resolve any problems that might arise.

2. Until otherwise changed, the PO for Goldsmith Eye Care PC is Dr. Wendy Goldsmith, OD

PUBLIC INFORMATION OFFICER

Policy Number: 2B

7-1-2014

In order to comply with HIPAA's Privacy Rule, Goldsmith Eye Care PC will have a Public Information Officer (designated "PIO").

1. Duties of the PIO will include:
 - a. receive, investigate, substantiate or not substantiate patient privacy complaints;
 - b. correct problems identified through investigation of privacy complaints;
 - c. provide information to patients and the public about Goldsmith Eye Care PC;
 - d. report any concerns about privacy compliance at Goldsmith Eye Care PC and cooperate in the investigation and resolution of any problem;
 - e. accept and act upon patient requests for confidential methods of communication;
 - f. accept and act upon patient request to restrict the way Goldsmith Eye Care PC handles protected health information for treatment, payment, or health care operations;
 - g. accept and act upon patient request for access to their own protected health information;
 - h. accept and act upon patient request to amend their own protected health information;
 - i. accept and act upon patient request for accounting of Goldsmith Eye Care PC disclosures of their protected health information.

2. Until otherwise changes, the PIO for Goldsmith Eye Care PC is Barb Skluzacek, COO.

Goldsmith Eye Care PC NOTICE OF PRIVACY POLICY

Policy Number: 3A

7-1-2014

In order to comply with HIPAA's Privacy Rule, it is the policy of Goldsmith Eye Care PC to develop a Notice of Privacy Policy (designated "NPP") and obtain acknowledgement from all patients of Goldsmith Eye Care PC's policies to protect unauthorized disclosure of patient's protected health information.

1. The PO will develop Goldsmith Eye Care PC's NPP and periodically review this document for any necessary changes.
2. Goldsmith Eye Care PC's NPP will be displayed at the check in area, on the practice website, or other easily accessible location.
3. Copies of Goldsmith Eye Care PC's NPP will be kept on hand to distribute to patients at their individual request. Goldsmith Eye Care PC is required to supply copies of the NPP only to new patients.
4. Goldsmith Eye Care PC personnel will explain to each patient the desire of Goldsmith Eye Care PC to protect the privacy of patient's health care information and attempt to obtain a signed Acknowledgement of Notice of Privacy Policies (designated "ANNP") from each patient in accordance with Policy 3B.
5. Any disclosure not mentioned in the Goldsmith Eye Care PC's NPP is considered as non-routine disclosure and will require Authorization from the patient.
6. In all cases, any patient genetic information cannot be utilized by a health plan or Business Associate in their underwriting or marketing activities.
7. Routine disclosure allows patients and Goldsmith Eye Care PC to exchange PHI through electronic media (email, computer monitored and generated telephone messaging, social media, specific patient portal access). Patient understands and accepts the inherent risks in disclosure of PHI by such means.

ACKNOWLEDGEMENT OF NOTICE OF PRIVACY PRACTICES

Policy Number: 3B

7-1-2014

In order to comply with HIPAA's Privacy Rule, it is the policy of Goldsmith Eye Care PC to perform the following as it pertains to informing patients regarding Goldsmith Eye Care PC's privacy policies.

1. The PO will develop a Notice of Privacy Practice as described in Policy 3A (designated as "NPP") that summarizes the policies of Goldsmith Eye Care PC in relation to use and disclosure of protected health information.
2. Goldsmith Eye Care PC personnel will make a reasonable attempt to have every patient view and sign an Acknowledgement of Notice of Privacy Practices (designated "ANPP") at their first appointment, deliver of optical goods, or other encounter on or after April 14, 2003.
 - a. Only the PO has the authority to change the ANPP.
 - b. Any employee handling a patient encounter is responsible to distribute the ANPP and ask the patient to read and sign the ANPP.
 - c. The signed ANPP will be kept in the Goldsmith Eye Care PC Privacy File or patients digital document file and provided to the patient upon request.
 - d. If the patient declines to sign the ANPP, the employee handling the encounter must make a note of the patient's decline to sign on the ANPP and file the ANPP in the Goldsmith Eye Care PC Privacy File or patient digital document file. Care cannot begin unless the patient signs the ANPP or in other fashion assures understanding of the policies in the ANPP. If a patient refuses to acknowledge the ANPP, they by default have elected to change their care to another practitioner.
 - e. It is not necessary to give an ANPP after April 14, 2003 unless:
 1. the PO substantially changes the ANPP or NPP;
 2. {Practice name} personnel cannot confirm that a signed ANPP is on file for the patient in question;
 3. it is the first encounter with the patient.
3. A copy of the NPP will be posted in a likely visible location in the office.
4. Patients can have a copy of the NPP if requested.
5. Goldsmith Eye Care PC will use and disclose protected health information in manner that is consistent with HIPAA and with Goldsmith Eye Care PC's NPP and Privacy Manual. If we substantially change our NPP or Privacy Manual, the new NPP or Privacy Manual will apply to all protected health care information, not just the information generated or obtained after the changes were made.

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

Policy Number: 4A

7-1-2014

In order to comply with HIPAA's Privacy Rule, it is the policy of Goldsmith Eye Care PC 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 or in cases where the patient specifically acknowledges by signing the Acknowledgement of Notice of Privacy Practice that they agree to such disclosures that are standard operation at Goldsmith Eye Care PC. As provided by HIPAA, we will not obtain a signed patient authorization in the following circumstances.

1. Uses and disclosures for treatment, payment, or health care operations. This includes, among other activities:
 - a. providing health care to patients in our office;
 - b. seeking assistance from consultants or other health care professionals;
 - c. making referrals of patients for additional or follow-up care;
 - d. writing, sending, and filling prescriptions for medications, eyewear, and contact lenses or facilitating requests for refills of medications or contact lenses;
 - e. preparing and submitting claims and bills to patients, third party payors, employee benefit plans, and Worker's Compensation Insurance representatives;
 - f. receiving and posting payments and processing such payments with a financial institution;
 - g. collection efforts;
 - h. professional licensure and specialty certification;
 - i. quality assurance;
 - j. financial audits and management;
 - k. training of professional and non-professional staff, including students and other doctors;
 - l. office management;
 - m. fraud and abuse prevention activities;
 - n. personnel activities;
 - o. completion and release of information to schools regarding a student's performance on a vision screening;
 - p. completion and release of information for drivers license certification;
 - q. providing access to health information of a patient to communication companies that provide computer generated messages to patient's regarding appointments, status of ophthalmic products ordered, or other information pertinent to office operations.

Policy Number: 4A (con't.)

2. Disclosures to Business Associates that have signed a business associate contract with Goldsmith Eye Care PC
3. Disclosures that are required by state law, provided that we disclose only the precise protected health information required; and only to the recipient required.
4. Disclosures to state, local, or federal government public health authorities to prevent or control disease, injury, or disability, report of suspected child abuse or neglect and reports regarding offenders with mental illness.
5. Disclosures to individuals or organizations under the jurisdiction of the federal Food and Drug Administration (“FDA”), such as drug or medical device manufactures, regarding the quality or safety of drugs or medical devices.
6. Disclosures to local, state, or federal government agencies in order to report suspected abuse, neglect, or domestic violence regarding adults, provided that Goldsmith Eye Care PC:
 - a. obtains and informal agreement from the patient unless:
 1. Goldsmith Eye Care PC is required by law to report our suspicions;
 2. Goldsmith Eye Care PC is permitted, but not required by law; to disclose the protected health information, and we believe that a report is necessary to prevent harm to our patient or other potential victims, or;
 - b. informs the patient that we are making a disclosure, unless:
 1. telling the patient would put the patient at risk for serious harm, or;
 2. someone else is acting on behalf of the patient and we think this person is the abuser and that 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 that Goldsmith Eye Care PC only disclose to a federal, state, or local government agency (or a private person or organization acting under contract with or grant of authority from the government agency) that is authorized by law to conduct oversight activities.
8. Disclosures in response to a court order, provided that we disclose only the precise protected health information ordered, and only to the person ordered.
9. Disclosures in response to a proper subpoena, provided that:
 - a. Goldsmith Eye Care PC assures that either Goldsmith Eye Care PC or the person seeking the subpoenaed information makes a reasonable effort to notify the patient in advance, and the patient has a chance to object to the court about the disclosure;
 - b. Goldsmith Eye Care PC assures that either Goldsmith Eye Care PC 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 that Goldsmith Eye Care PC thinks happened at our office, provided that we reasonably believe that the protected health information is evidence in or of a crime.

Policy Number: 4A (con't.)

11. Disclosures to organizations involved in the procurement, banking, or transplantation of eye in order to facilitate eye donation and transplantation.
12. Uses of protected health information to market or advertise Goldsmith Eye Care PC's own health care products or services, or for any 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 or deceased patients, provided that the researcher gives Goldsmith Eye Care PC the assurances required by HIPAA.
14. Information to a certified Electronic Health Information network, although in some cases the patient has the right to individually opt-out of such disclosures.
15. If at any time a proposed use or disclosure does not fit exactly into one of the exceptions to the need for an authorization described in this Policy 4A, we will obtain a signed patient authorization before making the use or disclosure.
16. Goldsmith Eye Care PC understands that the patient has the right to request that any PHI related to services for which the patient has paid without any input or assistance from a third party payor not be disclosed to any individual or group without expressed Authorization.

DESIGNATED RECORD SET

Policy Number: 5A

7-1-2014

In order to comply with HIPAA's Privacy Rule, Goldsmith Eye Care PC designates the following records to be our "designated record set" for purposes of patient's right to access and amend their protected health information.

1. The patient's medical record, hard copy or electronic:
 - a. history and medication reports;
 - b. reports of screening and diagnostic testing;
 - c. notes on examination;
 - d. consultation reports;
 - e. optical and medication prescriptions;
 - f. all other clinical information.

2. The patient's billing records, hard copy or electronic:
 - a. insurance claims;
 - b. remittance advice from insurance companies;
 - c. electronic fund deposit receipts;
 - d. bills to patients;
 - e. evidence of payment by patients;
 - f. collection records;
 - g. referrals to collection agencies or attorneys;
 - h. reports to consumer credit agencies for unpaid balances;
 - i. all other billing, claim, payment and collection records.

3. Optical product orders and receipt forms specific to a particular patient, hard copy or electronic:
 - a. orders for glasses;
 - b. orders for contact lenses;
 - c. acceptance of delivery for products ordered;
 - d. patient pick up records;
 - e. repair requests and documentation of completion;
 - f. fitting information;
 - g. distribution of optical accessories;
 - h. any other records related to optical goods.

LIMITED DATA SETS

Policy Number: 5B

7-1-2014

It is the policy of Goldsmith Eye Care PC to use a limited data set for certain disclosures of protected health information, whenever this is appropriate and feasible.

1. A limited data set is protected health information from which all of the following identifiers have been removed:
 - a. names;
 - b. postal address information other than city, state, and zip code;
 - c. telephone numbers;
 - d. fax numbers;
 - e. electronic mail addresses;
 - f. social security numbers;
 - g. medical record numbers;
 - h. health plan beneficiary numbers;
 - i. account numbers;
 - j. certificate or license numbers;
 - k. vehicle identifiers
 - l. device identifiers and serial numbers;
 - m. universal resource locators (URLs)
 - n. internet protocol addresses (IPs)
 - o. biometric identifies;
 - p. full face photographs;
 - q. information about the patient's relatives, members of the patient's household, and the patient's employer
2. The PIO is responsible for determining whether it is feasible and practical for Goldsmith Eye Care PC to disclose a limited data set, and if so, to create it.
3. Whenever Goldsmith Eye Care PC discloses a limited data set, the recipient will be required to enter into a Data Use Agreement with Goldsmith Eye Care PC.

DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION

Policy Number: 5C

7-1-2014

It is the policy of Goldsmith Eye Care PC to use de-identified information instead of protected health information whenever feasible and possible. None of HIPAA's Privacy Rule restrictions on the use and disclosure of protected health information apply to de-identified information.

1. De-identified protected health information is information where all possible personal identifiers have been removed. This includes information relative to the patient, the patient's relatives, the patient's household members, and the patient's employer. The identifiers removed are as follows:
 - a. names;
 - b. all geographic subdivisions smaller than a state including street address, city, county, precinct, zip code (except for the initial three digits);
 - c. all elements of date except year including birth date, admission date, discharge date, date of death;
 - d. telephone numbers;
 - e. fax numbers;
 - f. electronic email addresses;
 - g. social security numbers;
 - h. medical record numbers;
 - i. health plan beneficiary numbers;
 - j. account numbers;
 - k. certificate or license numbers;
 - l. vehicle identifiers;
 - m. device identifiers and serial numbers;
 - n. universal resource locators (URLs);
 - o. internet protocol addresses (IPs);
 - p. biometric indicators;
 - q. full face photographs;
 - r. any other unique identifying number, characteristic, or code.
2. Even after removal of all elements in #1 of this Policy, the information will not be considered de-identified unless we have no actual knowledge that the remaining information can be used, either alone or in combination with other reasonably available information, to identify a patient.
3. The PIO will determine the feasibility of using de-identified information and for performing such de-identification if it is feasible.

DISCLOSURES FOR RESEARCH

Policy Number: 6A

7-1-2014

In order to comply with HIPAA's Privacy Rule, it is the policy of Goldsmith Eye Care PC to obtain a signed patient authorization before using or disclosing protected health information for research purposes, unless the research satisfies one of HIPAA's exceptions to the need for authorization. In accordance with these exceptions:

1. We will not obtain a signed patient authorization if the researcher has obtained and presents to Goldsmith Eye Care PC a proper waiver of authorization from an Institutional Review Board ("IRB") or Privacy Board.
2. In order to be a proper waiver, the following criteria must be satisfied:
 - a. Goldsmith Eye Care PC must have documentation that the IRB or Privacy Board determined that a waiver is appropriate because:
 1. the use or disclosure of protected health information during the research poses no more than minimal risk to the privacy of the research participants;
 2. the protected health information is necessary for the research;
 3. as a practical matter, the research could not be conducted without a waiver.
 - b. we must have documentation of the IRB or the Privacy Board specification of what protected health information can be used or disclosed as part of the waiver;
 - c. we must have documentation of the IRB or Privacy Board made all its determinations according to proper procedures;
 - d. the documentation must include the name of the IRB or Privacy Board and the date of its approval of a waiver;
 - e. documentation must be signed by the chair of the IRB or Privacy Board.
3. The PO is responsible for obtaining proper IRB or Privacy Board waivers of authorization for research or any ongoing communication that Goldsmith Eye Care PC wants to conduct without a signed patient authorization.
4. Goldsmith Eye Care PC will rely on the IRB or Privacy Board's statement of the protected health information that is subject to the waiver as being the minimum amount of protected health information that is necessary of the research.
5. Goldsmith Eye Care PC will not obtain a signed patient authorization if the researcher gives us specific assurances that:
 - a. the researcher wants to review or disclose the protected health information solely to prepare a research protocol or take other steps in preparation for research, including preliminary analysis of the patient's candidacy for inclusion in the research;
 - b. the researcher will not take any protected health information off-site from where it is held;

Policy Number: 6A (con't.)

- c. researcher needs the protected health information for research purposes.
- 6. The PO is responsible for reviewing all assurances that an outside researcher may give Goldsmith Eye Care PC in support of a disclosure of protected health information.
- 7. Goldsmith Eye Care PC will not obtain a signed patient authorization if a researcher wants the protected health information in order to conduct research only solely on deceased patients and provides specific assurances that:
 - a. the researcher is asking for protected health information strictly to conduct research;
 - b. the person identified in the protected health information is dead as verified by a death certificate;
 - c. researcher needs the protected health information in order to perform research.

MARKETING AND ADVERTISING

Policy Number: 6B

7-1-2014

In order to comply with HIPAA's Privacy Rule it is the policy of Goldsmith Eye Care PC to 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.

1. Marketing means to make a communication that encourages a person receiving the communication to purchase a product or service. Marketing also includes any communication from Goldsmith Eye Care PC where Goldsmith Eye Care PC receives any financial or in-kind remuneration for the information.
2. Goldsmith Eye Care PC uses protected health information in connection with a marketing communication if we review patient databases or records to target the communication to specific recipients.
3. If a marketing communication uses or discloses protected health information of an individual patient, we will always obtain a signed patient authorization except for:
 - a. marketing communications about our own health care products or services;
 - b. communications that support or advertise a third party product as long as we are receiving no compensation of any kind for the communication;
 - c. communications made in the course of treatment, case management, or care coordination for an individual patient;
 - d. communications made during a face-to-face encounter with a patient;
 - e. communications consisting of distribution of promotional gifts of nominal value (less than \$10.00 per item per occurrence or less than \$50.00 to any one patient per year).
4. Any marketing communication that does not require a signed patient authorization must be included in Goldsmith Eye Care PC's accounting of disclosures available to a patient upon request.
5. Any marketing consent will inform the patient of their option to have their name removed from any mailing list. Goldsmith Eye Care PC will remove the patient from any such mailing list within five (5) days of receiving a written request from the patient.
6. When an authorization is required, it will include information about any money or other valuable thing that Goldsmith Eye Care PC obtains from someone else in connection with the communication.
7. Marketing communications that do not use or disclose protected health information such as general TV ads or brochures mailed to "occupant" on a zip code bases.
8. Regarding sale of PHI, Goldsmith Eye Care PC will not release patient's PHI in any condition where Goldsmith Eye Car PC receives direct or in-kind remuneration for the information without patient Authorization unless the release is related to treatment, payment or business operations of patient's relationship with Goldsmith Eye Care PC.

PERSONAL REPRESENTATION FOR PATIENTS

Policy Number: 7A

7-1-2014

In order to comply with HIPAA's Privacy Rule, it is the policy of Goldsmith Eye Care PC to allow a properly authorized personal representative of a patient to exercise all the rights that the patient could exercise regarding the use and disclosure of protected health information and to give any required permission for a use or disclosure of protected health information. Properly authorized individuals would include the following.

1. Adult patients (a patient over the age of 18).
2. Emancipated minor (a patient under the age of 18 who, by demonstrated court action, has been granted the legal right to be treated as an adult).
3. If the adult or emancipated minor is unable to handle matters regarding their protected health information due to mental incapacity, an individual with a demonstrated Power of Attorney can substitute for the adult or emancipated minor to sign all permissions and exercise all rights regarding protected health information.
4. Parents or guardians for unemancipated minors (patients under the age of 18). These would include:
 - a. either parent;
 - b. a court appointed guardian
5. Family or legal authorities representing deceased patients.
6. In certain instances, Goldsmith Eye Care PC will not comply with the personal representatives listed above. This can happen for the following reasons:
 - a. Goldsmith Eye Care PC feels that a person claiming to be a personal representative has or may have committed domestic violence, abuse, or neglect against the patient, and it is not in the patient's best interest to treat that person as the personal representative.
 - b. Goldsmith Eye Care PC feels that treating such person as a personal representative could endanger a patient, and it is not in the patient's best interest to treat that person as the personal representative.
7. Before Goldsmith Eye Care PC agrees to work with a persona claiming to be a personal representative of a patient, we will check their authority to do so. This might include:
 - a. checking identification;
 - b. looking at court or other documents;
 - c. consultation with Goldsmith Eye Care PC legal consultants.

Policy Number: 7A (con't.)

8. Nothing in this policy precludes Goldsmith Eye Care PC staff from taking phone calls from individuals stating to represent a patient for the purpose of making or changing appointments.
9. Nothing in this policy precludes Goldsmith Eye Care PC staff from taking phone calls or answering questions in person from individuals stating they represent a patient for the purpose of determining if optical products ordered are ready to be picked up or in actually delivering optical products to that person.
10. If a patient presents with other individuals that the patient invites into an examination or treatment area, Goldsmith Eye Care PC physicians would interpret this action as consent on the patient's part for the individual accompanying the patient to be witness to disclosure of any and all matters related to the patient's PHI.
11. In some cases, minors have the right to consent for evaluation and management of limited conditions and we will honor those rights.

PROVIDING INFORMATION TO FAMILY AND FRIENDS OF PATIENTS INVOLVED IN CARE OF PATIENT

Policy Number: 8A

7-1-2014

In order to comply with HIPAA's Privacy Rule, it is Goldsmith Eye Care PC's policy 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. It we feel that it is 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:

- a. obtain an oral agreement from the patient that the disclosure is acceptable;
- b. give the patient a chance to object to the disclosure;
- c. infer from the circumstances that the patient does not object. For example Goldsmith Eye Care PC will infer the patient does not object if the family member or friend is in the examination or treatment room with the patient and the patient makes no attempt to excuse the individual(s).

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 comes to the office to pick up eyewear or contact lenses that the patient previously ordered, as a convenience to the patient. In this example, we would provide the eyewear or contact lenses previously ordered but not disclose any diagnoses or special features of the optical goods.

2. If someone claiming to be a family member or friend of the patient initiates contact with Goldsmith Eye Care PC seeking information regarding the patients personal health information not specifically excluded from routine disclosure as noted in Policy 8A(3), we will:
 - a. verify the identity of the caller and their relationship to the patient;
 - b. determine if they are involved in the patient's care;
 - c. determine if the patient is available (by phone, email, FAX or other communication method) to either agree or object to the disclosure. If so, Goldsmith Eye Care PC will give the patient the chance to agree or object. 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.

3. Nothing in this Policy precludes Policy 7A(8) and 7A(9) dealing with patient representation in the facilitating of the ordering, delivery, dispensing or otherwise handling of optical goods (glasses, contact lenses).
4. Goldsmith Eye Care PC will make disclosures of a deceased patient's health information to individuals as long as they were involved in the providing of care or delivery of care to the patient while they were alive. This does not preclude the right to disclose deceased patient's medical information to an individual legally empowered to obtain the information.

MINIMUM NECESSARY USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

Policy Number: 9A

7-1-2014

In order to comply with HIPAA's Privacy Rule, it is the policy of Goldsmith Eye Care PC to only use or disclose the minimum amount of protected health information necessary to accomplish the purpose for the use or disclosure, under the terms and conditions of this policy.

1. Individuals in the following categories will have access to the kind or amount of protected health information indicated.
 - a. All doctors and technicians – any and all protected health information, including the entire medical record, for treatment purposes.
 - b. All other employees – only that information required to process payment issues, fill prescriptions, assist in patient referrals, or in other ways assist in completing necessary functions for the care of the patient. This may in some cases include any or all of the patient's protected health information.
2. Goldsmith Eye Care PC will keep all medical records and billing records secure when they are not in use. All information will be confined to the patient's paper or electronic medical record unless separate storage arrangements are office protocol (ex. photographs or other diagnostic data, optical invoices and statements, insurance information, etc.). Only authorized staff members will have access to this information, whether contained in hard copy or electronic storage. We require that no health care information be visible on a workstation computer screen when a Goldsmith Eye Care PC doctor or employee is away from their workstation. All staff are prohibited from using any security passwords not specifically assigned to them.
3. All Goldsmith Eye Care PC staff are restricted from any discussion regarding a patient's protected health information when not in the confines of the office of Goldsmith Eye Care PC.
4. All staff members 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 policies contained in the Goldsmith Eye Care PC Privacy Manual.
 - a. Unintentional violations of Goldsmith Eye Care PC privacy policy by an employee will result in the employee being issued a written warning and be required to stand before an oral investigation of the PO to demonstrate knowledge of Goldsmith Eye Care PC's privacy policies.
 - b. Intentional violations of Goldsmith Eye Care PC privacy policy may result in immediate termination with no payments of accrued benefits. The employee may also be subject to civil or criminal penalties. Goldsmith Eye Care PC will assist applicable authorities in the prosecution of any employee who willfully and intentionally violates a patient's privacy.

Policy Number: 9A (con't.)

5. The policy of minimum necessary information disclosure does not apply to cases where the patient has authorized the disclosure or the disclosure is restricted to information related to treatment, payment, or business operations.
6. We will rely on the representations of the following third parties that 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 of law or court;
 - c. professionals providing services to us (attorneys, accountings, etc.)
 - d. researchers supplying documentation of IRB waivers.
7. The PIO is responsible for determining what the minimum amount of information necessary for us to disclose in situations that are not routine.
8. Whenever we ask for protected health information about one of our patients from someone else, we will ask for only the minimum necessary amount of information necessary for us to accomplish the purpose that prompted us to ask for the information.

PATIENTS' ACCESS TO THEIR PROTECTED HEALTH INFORMATION

Policy Number: 10A

7-1-2014

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

1. Goldsmith Eye Care PC requires that patients send a written request to the PIO to inspect or copy their protected health information. If a patient calls on the telephone asking to inspect or copy their personal health information, the staff member will inform the patient of the requirement to send the request in writing.
2. Goldsmith Eye Care PC's PIO is responsible for handling patient requests to inspect or copy their protected health information.
3. Goldsmith Eye Care PC will respond to a patient's request to inspect or copy their protected health information within 30 days of receiving the written request. If more time is needed to comply with the request, Goldsmith Eye Care PC may be granted one 30 day extension as long as the patient is notified in writing of the need to time extension before the original 30 day time period expires.
4. Goldsmith Eye Care PC may substitute a summary or written explanations for certain tests in lieu of providing hard copies of the data (ex. visual fields, scanning laser, imaging, photographs, corneal topography, etc.)
5. Goldsmith Eye Care PC may deny the patients request only for one or more of the following reasons:
 - a. a patient cannot inspect or copy information 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. Goldsmith Eye Care PC must have informed the patient about this restriction when the patient signed up for the clinical trial and the patient must be allowed to inspect or copy the protected health information once the clinical trial is concluded;
 - c. a patient cannot inspect or copy information that Goldsmith Eye Care PC obtained from someone else who is not a health care provider and we promised that person that his/her identity would remain confidential;
 - d. a patient cannot inspect or copy information if we or another health care provider determine that this action would likely endanger the life or physical safety or 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 person referenced;

Policy Number: 10A (con't.)

- f. a patient's personal representative cannot inspect or copy information about the patient if we or another health care provider determines that this would likely cause substantial harm to the patient or another person;
 - g. a patient cannot inspect or copy information that is not in a designated record set;
- 6. The PIO will review any request for inspection or copy of protected health information to determine if such request can be honored. If Goldsmith Eye Care PC denies a patient access to their protected health information, the PIO will notify the patient in writing of this decision.
- 7. When Goldsmith Eye Care PC allows a patient to inspect or copy the requested information, Goldsmith Eye Care PC will adhere to the following.
 - a. Goldsmith Eye Care PC will provide the information in a form or format that the patient requests, if we can reasonably do so. In most cases, the patient may inspect the information in the form in which it is normally kept. In most cases, requests to copy protected health information will be carried out by Goldsmith Eye Care PC for the patient. The patient retains the right to copy the records themselves as long as the records or information does not leave the practice premises.
 - b. Goldsmith Eye Care PC will allow the patient to inspect or copy the requested information during normal business hours. Within the limit of normal business hours, the patient may select the time and date for inspection or copy of information.
 - c. Goldsmith Eye Care PC reserves the right to charge the patient \$1 per page for copying the information requested by the patient. If the patient requests said information be mailed or delivered to them, additional mailing or delivery charges may be levied. All charges must be paid before any copies are made.
 - d. 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. We may charge the patient the cost of preparing the summary. All charges must be paid before the summary is prepared.
 - e. Goldsmith Eye Care PC acknowledges that the patient has the right to ask for a transfer of their PHI onto a portable storage device or computer supplied by the patient but Goldsmith Eye Care PC feels this is not a secure and safe practice and therefore refuses to acknowledge said requests.

AMENDMENT OF PROTECTED HEALTH INFORMATION

Policy Number: 11A

7-1-2014

In order to comply with HIPAA's Privacy Rule, it is Goldsmith Eye Care PC's policy to permit patients to request an amendment to their protected health information under the conditions stated in this policy. If the patient has an approved personal representative, the approved personal representative may exercise this right on behalf of the patient.

1. Goldsmith Eye Care PC requires that all requests to amend protected health information be made in writing. If a patient calls on the telephone to request an amendment, the patient will be informed of the requirement to submit this request in writing.
2. Goldsmith Eye Care PC's PIO is responsible for handling patient requests to amend their protected health information.
3. Goldsmith Eye Care PC will respond to requests for amendment within 30 days after we receive the written request. We are allowed a 30 day extension if we notify the patient in writing that we need this additional time before the original time period expires.
4. The PIO may deny a request to amend only for one or more of the following reasons:
 - a. the information as stated is accurate and complete;
 - b. Goldsmith Eye Care PC did not create the information;
 - c. information is not in a designated record set.
5. If we deny a request to amend, the PIO will notify the patient in writing. The response will inform the patient of their right to either submit a statement of disagreement or have the original amendment request accompany the health care information.
6. If request to amend is granted, Goldsmith Eye Care PC will:
 - a. notify the patient in writing of the approval to amend;
 - b. append or link the corrected information to the original information;
 - c. send the corrected information to anyone who we know has previously received the original information or anyone else the patient requests.

ACCOUNTING FOR DISCLOSURES OF PROTECTED HEALTH INFORMATION

Policy Number: 12A

7-1-2014

In order to comply with HIPAA's Privacy Rule, it is Goldsmith Eye Care PC's policy to provide our patients, upon request, with an accounting of the disclosures that we have made of their protected health information subject to the terms and conditions stated in this policy.

1. The request for disclosure history may be made for any time period up to six years preceding the request.
2. Goldsmith Eye Care PC will provide an accounting of all disclosures of a patient's protected health information, except for the following:
 - a. disclosures for treatment, payment, or health care operations;
 - b. disclosures made with signed patient authorization
 - c. disclosures that are incident to other permitted disclosures;
 - d. disclosures to family or friends involved in the patient's care;
 - e. disclosures made prior to April 14, 2003.
3. In order to be able to provide an accounting when a patient requests one, Goldsmith Eye Care PC will keep track of all disclosures except for those listed in #2 above.
4. The following information regarding disclosures will provided to the patient upon request:
 - a. the date of the disclosure;
 - b. the name and address (if known) of the person or organization who received the information;
 - c. a description of the protected health information that was disclosed;
 - d. a statement of the purpose for the disclosure or copy of nay request that prompted the disclosure
5. All requests for disclosure must be made in writing. If a request is made by telephone, Goldsmith Eye Care PC staff members will advise the patient of the requirement to request accountings in writing.
6. Goldsmith Eye Care PC will respond to a request for an accounting within 30 days from our receipt of the written request. An additional 30 day extension may be granted as long as we notify the patient in writing of the need for such extension before the end of the original time period.
7. The accounting will contain all information stated in #4 of this policy. If repeated disclosures were made to the same person or organization for the same purpose, our accounting will provide all this information for the first disclosure, and then indicate the frequency of the other disclosures and the date of the last disclosure.
8. Patients will be provided with one free accounting, upon request, within any 12 month period. For additional accounting requests within any 12 month period, a charge of \$10.00 will be made and must be paid before the report is prepared or furnished to the patient.

RESTRICTIONS ON THE USE OF PROTECTED HEALTH INFORMATION

Policy Number: 13A

7-1-2014

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

1. Goldsmith Eye Care PC's PIO will handle requests from patients for special restrictions on use or disclosure of protected health information.
2. Generally, Goldsmith Eye Care PC will not agree to such restrictions requested by patients. In unusual circumstances that the PIO considers meritorious, we may agree to these requests.
3. If we agree to the requested restriction, the PIO will document the terms of the request and put this documentation in the Goldsmith Eye Care PC Privacy File. The PIO will also communicate the terms of such an agreement to any other business associate or staff member on a need to know basis.
4. Goldsmith Eye Care PC 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 Goldsmith Eye Care PC has agreed to a special restriction but can no longer honor that request, the PIO will do either of the following.
 - a. The PIO will contact the patient to work out a mutually agreeable termination of the restriction. Any new agreement will be documented by the PIO and kept in the Goldsmith Eye Care PC Privacy File or the patient's electronic health record.
 - b. The PIO will contact the patient and advise him/her that we are no longer able to honor the restriction. This notice to no longer adhere to the terms of the original restriction will only apply to information obtained or generated after notice to terminate is given.
6. Goldsmith Eye Care PC acknowledges that the patient has the right to ask that any information in the patient's record, whether PHI or not, be restricted from release to any entity, including the patient's health insurance provider, if the patient has paid in full for the services related to that information. The patient must specify in writing to the PIO their said request. If the patient requests such restrictions, Goldsmith Eye Care PC understands that this information cannot be released to any entity, even when requested for audit purposes.
7. Goldsmith Eye Care PC upon patient request will agree to not release any medical information to a patient's insurance provider if the patient pays for those services out of pocket.

CONFIDENTIAL COMMUNICATION METHODS WITH PATIENTS

Policy Number: 14A

7-1-2014

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

1. If possible, Goldsmith Eye Care PC will accommodate reasonable requests from a patient to use a particular manner or method of communication with them in order to preserve the confidentiality of their information. In general, we accommodate requests to communicate or not communicate with patients by telephone, standard mail, secure email, FAX, or in person. Privacy laws allow providing information directly to patients by transferring electronic data onto the patient's personal storage device but Goldsmith Eye Care PC does consider this a safe practice.
2. We require that such requests be made in writing. If a request is made by telephone, the patient will be informed of the need to make such request in writing.
3. Goldsmith Eye Care PC will not ask or require a patient to explain why they want a particular communication method.
4. Goldsmith Eye Care PC may charge the patient a reasonable cost of complying with their request, if any.
5. Goldsmith Eye Care PC's PIO is responsible for receiving and acting upon these patient requests.

HANDLING PATIENT COMPLAINTS ABOUT PRIVACY VIOLATIONS

Policy Number: 15A

7-1-2014

In order to comply with HIPAA's Privacy Rule, it is Goldsmith Eye Care PC's policy to accept complaints from patients who believe that we have not properly respected their privacy and to thoroughly investigate and resolve said complaints.

1. All complaints regarding presumed privacy violations must be made in writing to the PIO. If a complaint is made by telephone, the staff member will inform the patient of the need to make the complaint in writing to the PIO. The patient may remain anonymous if they so desire, although this may hinder our ability to respond to and resolve their complaint.
2. The PIO will keep all patient complaints for at least six years. These complaints, as well as information about the investigation and resolution of the complaint, will be kept in the Goldsmith Eye Care PC Privacy File.
3. Upon receiving a complaint, the PIO will investigate it thoroughly. The PIO has the discretion to conduct the investigation in the manner considered reasonable and logical in light of the nature of the complaint. At a minimum, this will include the following.
 - a. Talking to the employee whom the patient thinks violated the patient's privacy.
 - b. Review the patient's medical record.
 - c. Talking to other staff members about the patient's allegations.
 - d. Talking to the patient.
 - e. Reviewing any information or evidence that the patient presents in support of their claim.
4. Based on the results of the investigation, the PIO will determine if the patient's complaint is substantiated or not. If the complaint is not substantiated, the PIO will notify the patient in writing of that decision. If the complaint is substantiated, the PIO will take the following minimum steps in order to resolve the issue:
 - a. If the violation was caused by an employee's failure to comply with established policy, the PIO will report the issue to the Office Manager for action as a human resource disciplinary matter.
 - b. If the problem was caused by a lack of an appropriate policy, or an inadequate policy, the PIO will consult with the PO to determine how the policy should be changed, or if a new policy needs to be developed.
 - c. If a business associate was involved in a valid violation, action must be taken to prevent the violation from recurring. If the business associate cannot cure the breach, the business associate contract must be terminated. The PIO will communicate evidence of such a violation to the PO.
 - d. If the privacy violation causes harm, the PIO and PO will determine what steps are necessary to mitigate the harm.

Policy Number: 15A (con't.)

5. If new policies or procedures are put into place as part of any resolution, the PO will conduct mandatory training for the staff regarding the new policies.
6. All patient complaints will be addressed within 30 business days of receiving the written complaint from the patient.
7. If a violation occurs and resolution put into place, the PIO will develop a way to monitor whether or not the resolution is working to improve Goldsmith Eye Care PC's privacy protections. The PIO will report to the PO on the results of such monitoring.

SAFEGUARDS TO INFORMATION PRIVACY

Policy Number: 16A

7-1-2014

In order to comply with HIPAA's Privacy Rule, it is the policy of Goldsmith Eye Care PC to put certain safeguards in place to protect the privacy of protected health information.

1. Security Levels

- a. All employees are on a "need to know" basis regarding access to a patient's protected health information. Access is granted to any part of the designated record set as long as it is for the purpose of treatment, payment, or business operations at Goldsmith Eye Care PC.
- b. All employees are assigned security levels consistent with their job functions that allow them to access certain parts of the medical record or business management software.
- c. Only Administrative staff have a security level allowing them to delete or destroy medical records.

2. Physical Barriers

- a. All records, schedules, payment information or any other information that could identify a patient must be kept within the confines of the examination or treatment rooms, business office, optical, or laboratory. Information should never be left in plain sight of anyone but Goldsmith Eye Care PC staff and the patient or their approved representative.
- b. The office will remain locked during all non-business hours. Any intrusions will immediately be reported to Drs. Tim and/or Wendy Goldsmith or Barb Skluzacek, COO.
- c. Doors to business offices and administrative offices will remain closed during normal business hours unless the office is occupied.
- d. Doors to examination rooms will remain closed at all times.

3. Workstation Barriers

- a. Only Goldsmith Eye Care PC staff have access to workstations.
- b. Medical records are never left on a screen in any area of the office unless a Goldsmith Eye Care PC personnel is present in the room.

4. Technical Security

- a. All Goldsmith Eye Care PC have assigned passcodes into the medical record system. Passcodes have limited security level access as assigned by the Goldsmith Eye Care PC's Security Officer.

Policy Number: 16A (con't.)

- b. Goldsmith Eye Care PC personnel should never use another employee's passcode and never give their passcode to another employee for their use.

- 5. Network Security
 - a. Network security levels are assigned and monitored by the Goldsmith Eye Care PC's Security Officer.
 - b. Goldsmith Eye Care PC's Security Officer functions as network administrator.

- 6. To ensure that the policies of Goldsmith Eye Care PC are carried out by every employee, Goldsmith Eye Care PC trains every staff member on the privacy and security standards of Goldsmith Eye Care PC. Every new employee is trained within 90 days of their hire date and all employees are re-trained if there is a material change in the State, Federal or Goldsmith Eye Care PC standards.

BUSINESS ASSOCIATES

Policy Number: 17A

Effective January 1, 2003

In order to comply with HIPAA's Privacy Rule, Goldsmith Eye Care PC will enter into contracts with individuals designated as Business Associates. Business associates will be deemed those individuals or groups with whom Goldsmith Eye Care PC contracts services outside of the normal treatment, payment, and business operations of Goldsmith Eye Care PC. Sub-Business Associates will be considered any individuals or groups that the Business Associate contracts with where the Sub-Business Associate would be involved in services related to management of a patient's PHI outside normal TPO operations. The contract will legally obligate any Business Associate or Sub-Business Associate to conform to the privacy policies of Goldsmith Eye Care PC.

1. The Goldsmith Eye Care PC Privacy Officer will determine if a contracted individual or group falls under the definition of a Business Associate and assure that a Business Associate Contract exists with that individual or group.
2. It is the responsibility of the individual or group designated as a Business Associate to understand and remain compliant with all Goldsmith Eye Care PC Privacy Policies and any other HIPAA privacy policies.
3. Business Associate Agreements will be reviewed on an annual basis or if any changes are made in the Goldsmith Eye Care PC Privacy Manual.

DISASTER RECOVERY PLAN

Policy Number: 18A

7-1-2014

In order to comply with HIPAA's Privacy Rule, Goldsmith Eye Care PC has a disaster recovery plan in place should a significant break in network security occur that could compromise the privacy of protected health information.

1. A backup system is in place to copy all medical and business information by Revolution HER System. Backup information is handled in the manner as outlined in Goldsmith Care PC's Security Manual.
2. Any loss of information will be recovered from the Revolution HER System.
3. For purposes of this Notice of Practice Privacy, a "significant" breach is defined as any release of PHI, intentional or unintentional, where the breach results in a significant risk of financial, reputation, or other harm to the patient.
4. In the case of a significant breach, Goldsmith Eye Care PC must demonstrate to patients that there is low probability the compromise in PHI poses a risk of harm to the patient. This demonstration must include the following:
 - a. The nature of the PHI breach and exactly what identifiers were released;
 - b. Who accessed the information, if known;
 - c. Was the information simply acquired or was it viewed, if known;
 - d. The extent of the PHI breach and the likelihood that the information could be used to for identity theft or insurance fraud.
5. Goldsmith Eye Care PC is not required to notify a breach if the information released is encrypted according to NIST Standards.

PRIVACY CONTINGENCY PLAN

Policy Number: 18B

Effective 7-1-2014

In order to comply with HIPAA's Privacy Rule, Goldsmith Eye Care PC has a privacy contingency plan in place should an unforeseen breach or possible breach in privacy of all or a substantial portion of the protected health information occur.

1. A breach or potential substantial breach must be reported to the Privacy Officer immediately. The Privacy Officer and Security Officer will assess the situation and develop a plan, whenever possible, to recapture the information and place policies into action, if needed, to eliminate the probability of future recurrences of the breach all in accordance with Goldsmith Eye Care PC's Security Manual.
2. Whenever possible, Goldsmith Eye Care PC will notify those patients whose privacy may have been disclosed and update them periodically on the course of action designed to, whenever possible, recapture the data and, if needed, eliminate the probability of future recurrences of the breach.
3. Any employee or business associate of Goldsmith Eye Care PC who knowingly or unknowingly causes an unforeseen or possible breach in a patient's privacy will be dealt with in the manner specified in Goldsmith Eye Care PC's Security Manual. Goldsmith Eye Care PC does not consider money reparations to be appropriate mitigation for any unforeseen or other possible breach in privacy.