

REGISTRATION FORM

THE LASIK CENTER OF JACKSON

PATIENT INFORMATION

Patient Name (Last, First, Middle Initial)	Sex	Date of Birth	Marital Status	Age	Race	Social Security No.
Patient Address	City	State	Zip Code	Patient Phone No. ()		
Patient Employer	Occupation & Department					
Employer Address	City	State	Zip Code	Work Phone No. ()		

SPOUSE / GUARDIAN / NEXT OF KIN INFORMATION

Spouse or Guardian (Last, First, Middle Initial)	Date of Birth	Relationship to Patient <input type="checkbox"/> Spouse <input type="checkbox"/> Guardian <input type="checkbox"/> Parent	Alternate Phone Number
--	---------------	--	------------------------

REFERRING DOCTOR INFORMATION

Referring Doctor Name	City	State
Medical Doctor Name	City	State

How did you hear about the LASIK Center of Jackson and our doctors?

LASER VISION CORRECTION FINANCIAL AGREEMENT

I understand the fee for Laser Vision Correction Laser Treatment is **\$3990.00** for both eyes. The fee includes the pre-operative evaluation, laser treatment, facility fees and post operative fees. You will be expected to pay **\$150.00** on the day of your initial evaluation. This fee will be deducted from the total cost of your surgery.

Are you interested in financing Laser Vision Correction? YES or NO

ACKNOWLEDGMENT OF FINANCIAL RESPONSIBILITY: This information is accurate and true to the best of my knowledge. I understand that I am responsible to pay for services rendered, including reasonable attorneys fees and costs of collection in the event of default.

X _____ Date _____
Signature of Patient or Responsible Party

NOTICE OF PRIVACY PRACTICES / RED FLAGS RULE

Our Notice of Privacy Practices provides information about how we may use and disclose protected health information about you in the process of providing treatment, seeking payment or carrying out our own health care operations. This notice contains a Patient Rights section describing your rights under the law. A copy of the current notice in effect will be posted. Each time you receive treatment or healthcare services you may request a copy of the current notice.

Our Red Flags Rule Compliance Policies and Procedures provide information on safeguards in place to reasonably ensure protected health information and sensitive information related to identity theft.

I acknowledge that I have been offered a copy of the Notice of Privacy Practices.

X _____ Date _____
Signature of Patient or Responsible Party

BREACH NOTIFICATION ACT

Under the HITECH Act passed in 2009, The Hughes Eye Center will comply with the Breach Notification Rule. Patients will be notified of specified breaches of unsecured protected health information. This notification will occur in a timely manner and no less than 60 days from the date of the breach.

X _____ Date _____
Signature of Patient or Responsible Party



241-B Stonebridge Blvd. Jackson, TN 38305

To our new and established patients:

Effective Monday, April 14, 2003, the United States Federal Government implemented guidelines protecting personal information regarding your health care. The name of the program is "HIPPA" and The LASIK Center of Jackson and associates strictly abide by the rules and regulations of this federally mandated program. Our clinic staff has been comprehensively trained on HIPPA guidelines.

The privacy of your personal health information is extremely important and we will do whatever is necessary to maintain the confidentiality of your care and abide by your personal requests on how your personal information is shared with others.

Attached you will find our notice of privacy. The federal government requires our clinic to make this policy available and you have the right to request a copy of this notice. If you have questions or concerns regarding our privacy statement or the information contained in our privacy notice, please contact our director, Erica Ross, at 241-B Stonebridge Blvd, Jackson, TN 38305.

LASIK Center of Jackson

Owned and Operated by Hughes Eye Center

NOTICE OF PRIVACY PRACTICES

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

THE PRIVACY OF YOUR MEDICAL INFORMATION IS IMPORTANT TO US.

The following entities are covered by this notice:

- ◆ All employees, staff, and other associates to LASIK Center of Jackson and Hughes Eye Center
-

Uses and Disclosures of Medical Information

Primary Uses and Disclosures of Protected Health Information

We use and disclose protected health information about you for payment and health care operations. The federal health care Privacy Regulations generally do not “preempt” (or take precedence over) state privacy or other applicable laws that provide individuals greater privacy protections. As a result, to the extent state law applies, the privacy laws of a particular state, or other federal laws, rather than the HIPAA Privacy Regulations, might impose a privacy standard under which we will be required to operate. For example, where such laws have been enacted, we will follow more stringent state privacy laws that relate to uses and disclosures of the protected health information concerning HIV or AIDS, mental health, substance abuse/chemical dependency, genetic testing, reproductive rights. In addition to these state law requirements, we also may use or disclose protected health information in the following situations:

Payment: We might use and disclose your protected health information for all activities that are included within the definition of “payment” as written in the Federal Privacy Regulations. For example, we might use and disclose your protected health information to pay claims for services provided to you by doctors, hospitals, pharmacies and others for services delivered to you that are covered by your health plan. We might also use your information to determine your eligibility for benefits, to coordinate benefits, to examine medical necessity, to obtain premiums, and to issue explanations of benefits to the person who subscribes to the health plan in which you participate.

Health Care Operations: We might use and disclose your protected health information for all activities that are included within the definition of “health care operations” as defined in the Federal Privacy Regulations. For example, we might use and disclose your protected health information for stop-loss underwriting to determine our premiums for your health plan, to conduct quality assessment and improvement activities, to engage in care coordination or case management, and to manage our business.

Law Enforcement: Your health information may be disclosed to law enforcement agencies, without your permission, to support government audits and inspections, to facilitate law enforcement investigations, and to comply with government mandated reporting.

Other Covered Entities. In addition, we might use or disclose your protected health information to assist health care providers in connection with their treatment or payment activities, or to assist other covered entities in connection with certain of their health care operations. For example, we might disclose your protected health information to a health care provider when needed by the provider to render treatment to you, and we might disclose protected health information to another covered entity to conduct health care operations in the areas of quality assurance and improvement activities, or accreditation, certification, licensing or credentialing.

Other Possible Uses and Disclosures of Protected Health Information

The following is a description of other possible ways in which we might (and are permitted to) use and/or disclose your protected health information.

To You or with Your Authorization: We must disclose your protected health information to you, as described in the Individual Rights section of this notice. You may give us written authorization to use your protected health information or to disclose it to anyone for any purpose not listed on this notice. If you give us an authorization, you may revoke it in writing at any time. Your revocation will not affect any use or disclosures that we made as permitted by your authorization while it was in effect. Without your written authorization, we might not use or disclose your protected health information for any reason except those described in this notice.

Disclosures to the Secretary of the U.S. Department of Health and Human Services: We are required to disclose your protected health information to the Secretary of the U.S. Department of Health and Human Services when the Secretary is investigating or determining our compliance with the federal Privacy Regulations.

Special Circumstances

To Plan Sponsors: Where permitted by law, we may disclose your protected health information to the plan sponsor of your group health plan to permit the plan sponsor to perform plan administration functions. For example, a plan sponsor may contact us seeking information to evaluate future changes to your benefit plan. We may also disclose summary health information (this type of information is defined in the Federal Privacy Regulations) about the enrollees in your group health plan to the plan sponsor to obtain premium bids for the health insurance coverage offered through your group health plan or to decide whether to modify, amend or terminate your group health plan.

To Family and Friends: If you agree (or, if you are unavailable to agree), such as in a medical emergency situation we might disclose your protected health information to a family member, friend or other person to the extent necessary to help with your health care or with payment for your health care.

Underwriting: We might receive your protected health information for underwriting, premium rating or other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits. We will not use or further disclose this protected health information received under these circumstances for any other purpose, except as required by law, unless and until you enter into a contract of health insurance or health benefits with us.

Health Oversight Activities. We might disclose your protected health information to a health oversight agency for activities authorized by law, such as: audits; investigations; inspections; licensure or disciplinary actions; or civil, administrative, or criminal proceedings or actions. Oversight agencies seeking this information include government agencies that oversee: (i) the health care system; (ii) government benefit programs; (iii) other government regulatory programs; and (iv) compliance with civil rights laws.

Abuse or Neglect. We might disclose your protected health information to appropriate authorities if we reasonably believe that you might be a possible victim of abuse, neglect, domestic violence or other crimes.

To Prevent a Serious Threat to Health or Safety. Consistent with certain federal and state laws, we might disclose your protected health information if we believe that the disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public.

Coroners, Medical Examiners, Funeral Directors, and Organ Donation. We might disclose protected health information to a coroner or medical examiner for purposes of identifying you after you die, determining your cause of death, or for the coroner or medical examiner to perform other duties authorized by law. We also might disclose, as authorized by law, information to funeral directors so that they may carry out their duties on your behalf. Further, we might disclose protected health information to organizations that handle organ, eye, or tissue donation and transplantation.

Research. We might disclose your protected health information to researchers when an institutional review board or privacy board has: (1) reviewed the research proposal and established protocols to ensure the privacy of the information; and (2) approved the research.

Inmates. If you are an inmate of a correctional institution, we might disclose your protected health information to the correctional institution or to a law enforcement official for: (1) the institution to provide health care to you; (2) your health and safety and the health and safety of others; or (3) the safety and security of the correctional institution.

Workers' Compensation. We might disclose your protected health information to comply with workers' compensation laws and other similar programs that provide benefits for work-related injuries or illnesses.

Public Health and Safety: We might disclose your protected health information to the extent necessary to avert a serious and imminent threat to your health or safety or the health or safety of others.

Required by Law: We might use or disclose your protected health information when we are required to do so by law. For example, we must disclose your protected health information to the U.S. Department of Health and Human Services upon their request for purposes of determining whether we are in compliance with federal privacy laws.

Legal Process and Proceedings: We might disclose your protected health information in response to a court or administrative order, subpoena, discovery request, or other lawful process, under certain circumstances. Under limited circumstances, such as a court order, warrant, or grand jury subpoena, we might disclose your protected health information to law enforcement officials.

Law Enforcement: We might disclose to a law enforcement official limited protected health information of a suspect, fugitive, material witness, crime victim, or missing person. We might disclose protected health information where necessary to assist law enforcement officials to capture an individual who has admitted to participation in a crime or has escaped from lawful custody.

Military and National Security: We might disclose to military authorities the protected health information of Armed Forces personnel under certain circumstances. We might disclose to federal officials protected health information required for lawful intelligence, counterintelligence, and other national security activities.

Other Uses and Disclosures of Your Protected Health

Information: Other uses and disclosures of your protected health information that are not described above will be made only with your written authorization. If you provide us with such an authorization, you may revoke the authorization in writing, and this revocation will be effective for future uses and disclosures of protected health information. However, the revocation will not be effective for information that we already have used or disclosed in reliance on your authorization.

Individual Rights

Access: You have the right to look at or get copies of the protected health information contained in a designated record set, with limited exceptions. You may request that we provide copies in a format other than photocopies. We will use the format you request unless we cannot reasonably do so. You must make a request in writing to obtain access to your protected health information. You may obtain a form to request access by using the contact information listed at the end of this notice. You may also request access by sending a letter to the address at the end of this notice. If you request copies, we might charge you a reasonable fee for each page, and postage if you want the copies mailed to you. If you request an alternative format, we might charge a cost-based fee for providing your protected health information in that format. If you prefer, we will prepare a summary or an explanation of your protected health information, but we might charge a fee to do so.

We might deny your request to inspect and copy your protected health information in certain limited circumstances. Under certain conditions, our denial will not be reviewable. If this event occurs, we will inform you in our denial that the decision is not reviewable. If you are denied access to your information and the denial is subject to review, you may request that the denial be reviewed. A licensed health care professional chosen by us will review your request and the denial. The person performing this review will not be the same person who denied your initial request.

Disclosure Accounting: You have the right to receive a list of instances in which we or our business associates disclosed your protected health information for purposes other than treatment, payment, health care operations and certain other activities, after April 14, 2003. We will provide you with the date on which we made the disclosure, the name of the person or entity to which we disclosed your protected health information, a description of the protected health information we disclosed, the reason for the disclosure, and certain other information. If you request this list more than once in a 12-month period, we might charge you a reasonable, cost-based fee for responding to these additional requests.

You may request an accounting by submitting your request in writing using the information listed at the end of this notice. Your request may be for disclosures made up to 6 years before the date of your request, but in no event, for disclosures made before April 14, 2003.

Restriction Requests: You have the right to request that we place additional restrictions on our use or disclosure of your protected health information. We are not required to agree to these additional restrictions, but if we do, we will abide by our agreement (except in an emergency). Any agreement that we might make to a request for additional restrictions must be in writing and signed by a person authorized to make such an agreement on our behalf. We will not be liable for uses and disclosures made outside of the requested restriction unless our agreement to restrict is in writing. We are permitted to end our agreement to the requested restriction by notifying you in writing.

You may request a restriction by writing to us using the information listed at the end of this notice. In your request tell us: (1) the information of which you want to limit our use and disclosure; and (2) how you want to limit our use and/or disclosure of the information.

Confidential Communication: If you believe that a disclosure of all or part of your protected health information may endanger you, you have the right to request that we communicate with you in confidence about your protected health information. This means that you may request that we send you information by alternative means, or to an alternate location. We must accommodate your request if: it is reasonable, specifies the alternative means or alternate location, and specifies how payment issues (premiums and claims) will be handled. You may request a Confidential Communication by writing to us using the information listed at the end of this notice

Amendment: You have the right to request that we amend your protected health information. Your request must be in writing, and it must explain why the information should be amended. We may deny your request if we did not create the information you want amended or for certain other reasons. If we deny your request, we will provide you with a written explanation. You may respond with a statement of disagreement to be appended to the information you wanted amended. If we accept your request to amend the information, we will make reasonable efforts to inform others, including people you name, of the amendment and to include the changes in any future disclosures of that information.

Electronic Notice: Even if you agree to receive this notice on our web site, or by electronic mail (e-mail), you are entitled to receive a paper copy as well. Please contact us using the information listed at the end of this notice to obtain this notice in written form. If the e-mail transmission has failed, and LASIK Center of Jackson is aware of the failure, then we will provide a paper copy of the notice to you.

Questions and Complaints

Information on LASIK Center of Jackson Privacy Practices:

If you want more information about our privacy practices or have questions or concerns, please contact the member services number on the back of your card.

Filing a Complaint:

If you are concerned that we might have violated your privacy rights, or you disagree with a decision we made about your individual rights, you may use the contact information listed at the end of this notice to complain to us. You also may submit a written complaint to the U.S. Department of Health and Human Services (DHHS). We will provide you with the contact information for DHHS upon request.

We support your right to protect the privacy of your protected health and financial information. We will not retaliate in any way if you choose to file a complaint with us or with the U.S. Department of Health and Human Services.

LASIK Center of Jackson Contact Information

HIPAA Compliance and Privacy Office

Contact Office:	LASIK Center of Jackson
Telephone:	(731) 668-0064
Fax:	(731) 668-0065
E-mail:	lasikcenterofjackson@yahoo.com
Address:	241 – B Stonebridge Blvd. Jackson, TN 38305

Policies and Procedures

Identity Theft Prevention and Detection and Red Flags Rule Compliance

Policy

It is the policy of *LASIK Center of Jackson* to follow all federal and state laws and reporting requirements regarding identity theft. Specifically, this policy outlines how *LASIK Center of Jackson* will (1) identify, (2) detect, and (3) respond to “red flags.” A “red flag” as defined by this policy includes a pattern, practice, or specific account or record activity that indicates possible identity theft.

It is the policy of *LASIK Center of Jackson doctors / owners* that this identity theft prevention and detection and Red Flags Rule compliance program is approved as of May 1, 2009 and reviewed no less than annually.

It is the policy of *LASIK Center of Jackson* that the Compliance Official is assigned the responsibility of implementing and maintaining the Red Flags Rule requirements. Furthermore, it is the policy of *LASIK Center of Jackson* that this individual will be provided sufficient resources and authority to fulfill these responsibilities. At a minimum, it is the policy of *LASIK Center of Jackson* that there will be one individual or job description designated as the privacy official.

It is the policy of *LASIK Center of Jackson* that, pursuant to the existing HIPAA Security Rule, appropriate physical, administrative, and technical safeguards will be in place to reasonably ensure protected health information and sensitive information related to patient identity from any intentional or unintentional use or disclosure.

It is the policy of *LASIK Center of Jackson* that its business associates must be contractually bound to protect sensitive patient information to the same degree as set forth in this policy. It is also the policy of *LASIK Center of Jackson* that business associates who violate their agreement will be dealt with first by an attempt to correct the problem, and if that fails, by termination of the agreement and discontinuation of services by the business associate.

It is the policy of *LASIK Center of Jackson* that all members of its workforce have been trained by the May 1, 2009 compliance date on the policies and procedures governing compliance with the Red Flag Rule. It is also the policy of *LASIK Center of Jackson* that new members of its workforce receive training on these matters within a reasonable time after they have joined the workforce. It is the policy of *LASIK Center of Jackson* to provide training should any policy or procedure related to the Red Flags Rule materially change. This training will be provided within a reasonable time after the policy or procedure materially changes. Furthermore, it is the policy of *LASIK Center of Jackson* that training will be documented, indicating participants, date, and subject matter.

Procedures

I. Identify red flags. In the course of caring for patients, *LASIK Center of Jackson* may encounter inconsistent or suspicious documents, information, or activity that may signal identity theft. *LASIK Center of Jackson* identifies the following as potential red flags, and this policy includes procedures describing how to detect and respond to these red flags below:

1. A complaint or question from a patient based on the patient's receipt of:
 - A bill for another individual;
 - A bill for a product or service that the patient denies receiving;
 - A bill from a health care provider that the patient never patronized; or
 - A notice of insurance benefits (or explanation of benefits) for health care services never received.
2. Records showing medical treatment that is inconsistent with a physical examination or with a medical history as reported by the patient.
3. A complaint or question from a patient about the receipt of a collection notice from a bill collector.
4. A patient or health insurer report that coverage for legitimate hospital stays is denied because insurance benefits have been depleted or a lifetime cap has been reached.
5. A complaint or question from a patient about information added to a credit report by a health care provider or health insurer.
6. A dispute of a bill by a patient who claims to be the victim of any type of identity theft.
7. A patient who has an insurance number but never produces an insurance card or other physical documentation of insurance.
8. A notice or inquiry from an insurance fraud investigator for a private health insurer or a law enforcement agency, including but not limited to a Medicare or Medicaid fraud agency.

II. Detect red flags. *LASIK Center of Jackson* practice staff will be alert for discrepancies in documents and patient information that suggest risk of identity theft or fraud. *LASIK Center of Jackson* will verify patient identity, address, and insurance coverage at the time of patient registration/check-in.

Procedure:

1. When a patient calls to request an appointment, the patient will be asked to bring the following at the time of the appointment:
 - Driver's license or other photo identification;
 - Current health insurance card; and
 - Utility bills or other correspondence showing current residence if the photo identification does not show the patient's current address. If the patient is a minor, the patient's parent of guardian should bring the information listed above.

2. When the patient arrives for the appointment, the patient will be asked to produce the information listed above. **This requirement may be waived for patients who have visited the practice within the last six months.**

3. If the patient has not completed the registration form within the last six months, registration staff will verify current information on file and, if appropriate, update the information.

4. Staff should be alert for the possibility of identity theft in the following situations:
 - The photograph on a driver's license or other photo identification submitted by the patient does not resemble the patient.
 - The patient submits a driver's license, insurance card, or other identifying information that appears to be altered or forged.
 - Information on one form of identification the patient submitted is inconsistent with information on another form of identification or with information already in the practice's records.
 - An address or telephone number is discovered to be incorrect, non-existent, or fictitious.
 - The patient fails to provide identifying information or documents.
 - The patient's signature does not match a signature in the practice's records.
 - The Social Security number or other identifying information the patient provided is the same as identifying information in the practice's records provided by another individual, or the Social Security number is invalid.

III. Respond to Red Flags. If an employee of *LASIK Center of Jackson* detects fraudulent activity or if a patient claims to be a victim of identity theft, *LASIK Center of Jackson* will respond to and investigate the situation. If the fraudulent activity involves personal health information (PHI) covered under the HIPAA security standards, *LASIK Center of Jackson* will also apply its existing HIPAA security policies and procedures to the response.

Procedure

If potentially fraudulent activity (a red flag) is detected by an employee of *LASIK Center of Jackson*:

1. The employee should gather all documentation and report the incident to his or her immediate supervisor.
2. The supervisor will determine whether the activity is fraudulent or authentic.
3. If the activity is determined to be fraudulent, then *LASIK Center of Jackson* should take immediate action. Actions may include but are not limited to:
 - Cancel the transaction;
 - Notify appropriate law enforcement;
 - Notify the affected patient(s);
 - Notify the affected physicians(s); and
 - Assess impact to practice.

If a patient claims to be a victim of identity theft:

1. The patient should be encouraged to file a police report for identity theft if he/she has not done so already.
2. The patient should be encouraged to complete the ID Theft Affidavit developed by the FTC, along with the supporting documentation.
3. *LASIK Center of Jackson* will compare the patient's documentation with personal information in the patient's records.
4. If following investigation, it appears that the patient has been a victim of identity theft; *LASIK Center of Jackson* will promptly consider what further remedial act/notifications may be needed under the circumstances.
5. The physician will review the affected patient's medical records to confirm whether documentation was made in the patient's medical records that resulted in inaccurate information in the record. If inaccuracies due to identity theft exist, a notation should be made in the records to indicate identity theft.
6. The practice medical records staff will determine whether any other records and/or ancillary service providers are linked to inaccurate information. Any additional files containing information relevant to identity theft will be removed and appropriate action will be taken. The patient is responsible for contacting ancillary service providers.
7. If following investigation, it does not appear that the patient has been a victim of identity theft; *LASIK Center of Jackson* will take whatever action it deems appropriate.