



HIPAA Policy

2014

The Health Insurance Portability and Accountability Act is a federal law that protects the privacy and security of patients' health information and grants certain rights to patients.

Clarkson Eyecare, Inc. requires all employees to read and sign the HIPAA training policy as stated below and to practice HIPAA compliancy daily within your work environment.

PHI- Protected Health Information

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

- (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
- (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
 - (i) That identifies the individual; or
 - (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Examples-

- Name
- Address
- Telephone Number
- Fax Number
- E-Mail addresses
- Social Security Number
- Health Plan Beneficiary Number
- Photographic Images

Be aware of PHI around you to avoid unintentional use or disclosure; papers lying around, computer screens and conversations involving patients.

- When papers containing PHI are no longer needed place them in your shred bin.
- Verify mailing, faxing or e-mail address information when are correct before sending information.
- Do not remove patient records from any Clarkson Eyecare office.
- Lock your computer when not in use.
- Discuss patient information in private areas.
- If you do not need patient information to do your job do not seek it out. This includes
- Accessing patient information outside the performance of your job is against Clarkson Eyecare policy and will result in disciplinary action up to and including termination. This includes:
 - Your own record
 - The records of your family members
 - The records of your co-workers or friends



- The records of someone in the news

The unlawful or unauthorized access, use or disclosure of confidential information is prohibited. As well as sharing or posting your password or using someone else's password.

Clarkson Eyecare, Inc. must give our patients access to a copy of our "Notice of Privacy Practices" which will include a description of their rights and how their health information may be used. This notice is posted on our website at www.clarksoneyecare.com.

Use and Disclosure

Use is the sharing of PHI within the Clarkson Eyecare, Inc. practice which includes the Lab, Frame Department, Call Center, Corporate office and Central office.

Disclosure means the release, transfer, provision of access to, or divulging of information in any manner (verbally or in writing) by Clarkson Eyecare, Inc. to persons who are outside the HIPAA covered components of Clarkson Eyecare, Inc.

You may not use and disclose PHI for treatment, payment and healthcare operations (TPO) of our organization without patient authorization.

If the requestor is not known to you, verify their identity and authority before providing PHI.

The need to know rule

- When using or disclosing PHI or requesting it from another practice we must make reasonable efforts to limit it to the smallest amount needed to accomplish the task.
- If the entire chart is not required, only ask for the information you need.

Accidental Disclosure-If you disclose private data in error to an unauthorized person or if you breach the security of private data, acknowledge the mistake and notify your supervisor or the HIPAA Privacy Office immediately.

Intentional Disclosures- If you ignore the rules and carelessly or deliberately use or disclose PHI inappropriately, you can expect Clarkson Eyecare, Inc. disciplinary action, civil liability, and/or criminal charges. Examples of intentional violations include:

- Sharing, posting or distributing personal passwords or account access information.
- Knowledge of unauthorized use by a co-worker of an account or password belonging to someone else.
- Attempting to learn or use another person's access information.
- Installing or downloading unauthorized computer programs that include or allow the entrance of viruses, worms or other malicious software.
- Failing to secure a workstation with access to or display of confidential information.
- Posting patient information on the internet without authorization.
- Placing unencrypted PHI or personal information on removable media or devices such as thumb drives, DVD's or CD's.
- Accessing personal information outside of your job.
- Illegally altering, destroying, or removing original paper or electronic PHI.



- Accessing electronic PHI at home and leaving information visible and/or accessible to family members, roommates and friends.
- Selling health or personal information or inappropriately giving such information to the news media.

Fax/E-Mail

Fax machines must be in a secure location. Fax/E-Mails containing PHI must have the Clarkson Eyecare, Inc. name, sender name and phone number attached. Verify fax number and e-mail address before transmittal.

All Clarkson Eyecare, Inc. email addresses will have the following notice posted in every email.

NOTICE This message is intended only for the individual to whom it is addressed and may contain information that is confidential or privileged. If you are not the intended recipient, or the employee or person responsible for delivering it to the intended recipient, you are hereby notified that any dissemination, distribution, copying or use is strictly prohibited. If you have received this communication in error, please notify the sender and destroy or delete this communication immediately.

Patient Rights

HIPAA gives patients the right to

- Access, inspect and copy PHI.
- Request amendment of PHI.
- Receive accounting disclosures.
- Request restrictions on disclosures.
- Request communications of PHI at alternative locations or means.
- Register complaints concerning their privacy right.

Requests must be granted within 30 days if PHI is on-site and within 60 days if PHI is off-site. Clarkson Eyecare, Inc. has a form within its software program to be filled out by patients and forwarded to the HIPAA Privacy Office, Kris Caldwell, to release information. Once this form is received the PHI is pulled, copied and sent to the requestor as indicated on the form.

A patient has the right to receive an accounting of PHI disclosures. All requests for accounting should be directed to the Clarkson Eyecare, Inc. Privacy Officer. Disclosures must be tracked.

Breach Reporting

All breaches must be reported to the Clarkson Eyecare, Inc. Privacy Office immediately. A breach is a disclosure of PHI that is not permitted by the privacy rule. For example an unencrypted laptop containing PHI is lost or stolen. PHI sent to the wrong fax, mailing address or e-mail.

Notify the Privacy Officer as soon as you suspect a possible breach. At this time it will be determined if an actual breach has occurred and take care of the notification process.



EPHI- Electronic Protected Health Information

EPHI means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, received by electronic media and/or stored by electronic media.

- Computer networks
- Desktop computers
- Laptop computers
- Disks of any type
- Thumb drives

Password Management

- Keep passwords confidential.
- Avoid maintaining a paper record of passwords.
- Change passwords when there is an indication of possible compromise.
 - Your CMS id can be changed by contacting the Privacy Officer
- Do not use all the same passwords for business and personal accounts.
- Change temporary passwords at first log in.
- Do not configure any log-on to remember your password.
- Always maintain and use passwords in a secure and confidential manner.
- Never use someone else's sign on information.
- If you are asked to sign on using someone else's information, refuse to do so and report them immediately.

Internet Access

Do not use workstations to engage in any activity that is in violation of Clarkson Eyecare, Inc. policy. For example, do not access inappropriate or offensive websites, engage in gambling, send malicious e-mails or download copyrighted materials.

Social Networks are not private. Never discuss patient care via social networks sites including Facebook, MySpace, Twitter, LinkedIn etc.

Clarkson Eyecare, Inc. prohibits the posting of any information about patients on websites. Violations of this policy will result in disciplinary action up to and including termination.

Drop Box and Google Docs are to never be used to store PHI. These are not secure sites and the Terms & Conditions of these websites specifically state they do not intend to comply with HIPAA.

Physical Security

All computers, remote and on-site, that contain e-PHI must be protected with a secure log-on. Anti-virus software approved by the Clarkson Eyecare, Inc. Network Manager must be installed on all computers that connect to the Clarkson Eyecare, Inc. network.



E-PHI must be destroyed before hardware or media is disposed of or made available for re-use.

If your job allows you to work from home you are responsible for maintaining the privacy and security of all confidential materials. This includes but is not limited to patient charts, computers and any other papers containing PHI.

Transporting PHI

Confidential information is not to be removed from Clarkson Eyecare, Inc. properties without prior approval. You are responsible for maintaining the privacy and security of all confidential information that you may be transporting, storing or accessing off-site. Never leave PHI in an unattended vehicle.

If you have any questions, concerns or comments please contact Kris Caldwell, HIPAA Privacy Office for Clarkson Eyecare, Inc.