National Academy of Opticianry

Continuing Education Course

Approved by the American Board of Opticianry and the National Contact Lens Examiners

HIPAA

National Academy of Opticianry
8401 Corporate Drive #605
Landover, MD 20785
800-229-4828 phone
301-577-3880 fax
www.nao.org

National Academy of Opticianry

PREFACE:

This continuing education course was prepared under the auspices of the National Academy of Opticianry and is designed to be convenient, cost effective and practical for the Optician.

The skills and knowledge required to practice the profession of Opticianry will continue to change in the future as advances in technology are applied to the eye care specialty. Higher rates of obsolescence will result in an increased tempo of change as well as knowledge to meet these changes. The National Academy of Opticianry recognizes the need to provide a Continuing Education Program for all Opticians. This course has been developed as a part of the overall program to enable Opticians to develop and improve their technical knowledge and skills in their chosen profession.

The National Academy of Opticianry

INSTRUCTIONS:

Read and study the material. After you feel that you understand the material thoroughly take the test following the instructions given at the beginning of the test. Upon completion of the test, mail the answer sheet to the National Academy of Opticianry, 8401 Corporate Drive, Suite 605, Landover, Maryland 20785 or fax it to 301-577-3880. Be sure you complete the evaluation form on the answer sheet. Please allow two weeks for the grading and a reply.

CREDITS:

The American Board of Opticianry and the National Contact Lens Examiners have approved this course for one (1) Continuing Education Credit toward certification renewal. To earn this credit, you must achieve a grade of 80% or higher on the test. The Academy will notify all test takers of their score and mail the credit certificate to those who pass. You must mail the appropriate section of the credit certificate to the ABO and/or your state licensing board to renew your certification/licensure. One portion is to be retained for your records.

AUTHORS:

Diane F. Drake, LDO, ABOM, FCLSA, FNAO
David F. Meldrum, LDO, ABOM, FNAO
Randall L. Smith, M.S., ABOM, NCLEC, FNAO

INTENDED AUDIENCE:

This course is intended for opticians of all levels.

COURSE DESCRIPTION:

This course will present information on patient privacy (HIPAA). Included will be, who is affected, business associates, ways to comply, and updates from 2013. Due to the subject matter, it is important that each person in the optical environment understand the importance of complying with the rule. The Security Rule, Privacy Rule, as well as breaches, will be discussed.

LEARNING OBJECTIVES:

At the completion of this course, the student should be able to:

- Understand key requirements of patient privacy
- Explain the use of the term "business associate" as it applies to these regulations
- Describe how to implement a privacy policy and training
- Discuss the Privacy Rule and the Security Rule

National Academy of Opticianry
8401 Corporate Drive #605
Landover, MD 20785
800-229-4828 phone
301-577-3880 fax
www.nao.org

HIPAA

Diane F. Drake, LDO, ABOM, FCLSA, FNAO
David F. Meldrum, LDO, ABOM, FNAO
Randall L. Smith, M.S., ABOM, NCLEC, FNAO

Introduction

HIPAA

Disclosure

The information in this section is not intended to be used exclusively for business or HR purposes. The information included in this section is current as of the writing of this document. However, due to the nature of this Act, some or all of the particulars may be subject to governmental change. Therefore, for any business or HR purposes, it would be prudent to check with the respective agencies for updates.

Sources for information

http://www.hhs.gov/ocr/hipaa/privacy.html

http://aspe.os.dhhs.gov/admnsimp

HIPAA is the acronym for the Health Insurance Portability and Accountability Act of 1996. The Centers for Medicare & Medicaid Services (CMS) is responsible for implementing various unrelated provisions of HIPAA, therefore HIPAA may mean different things to different people.

Purpose

The purpose of the act is to reform health insurance and protect health insurance coverage for workers and their families when they change or lose their jobs.

The administrative simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) require the Department of Health and Human Services to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers. It also addresses the security and privacy of health data. Adopting these standards aims to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in health care.

Basic Terms

OCR = Office for Civil Rights
DHHS = Department of Health and Human Services
PHI = Protected Health Information
TPO = **T**reatment or **P**ayment or Health care **O**perations

- Anything to make operations work, for example, Phone and files

Reasonable Safeguards

A covered entity must have in place appropriate administrative, technical, and physical safeguards that protect against uses and disclosures not permitted by the Privacy Rule, as well as that limit incidental uses or disclosures. See 45 CFR 164.530(c). It is not expected that a covered entity's safeguards guarantee the privacy of protected health information from any and all potential risks. Reasonable safeguards will vary from covered entity to covered entity depending on factors such as the size of the covered entity and the nature of its business. In implementing reasonable safeguards, covered entities should analyze their own needs and circumstances, such as the nature of the protected health information it holds, and assess the potential risks to patients' privacy. Covered entities should also take into account the potential effects on patient care and may consider other issues, such as the financial and administrative burden of implementing particular safeguards.

Minimum Necessary

Covered entities also must implement reasonable minimum necessary policies and procedures that limit how much protected health information is used, disclosed, and requested for certain purposes. These minimum necessary policies and procedures also reasonably must limit who within the entity has access to protected health information, and under what conditions, based on job responsibilities and the nature of the business. The minimum necessary standard does not apply to disclosures, including oral disclosures, among health care providers for treatment purposes. For example, a physician is not required to apply the minimum necessary standard when discussing a patient's medical chart information with a specialist at another hospital. See 45 CFR 164.502(b) and 164.514(d): see the fact sheet and frequently asked questions on this website about the minimum necessary standard, for more information.

An incidental use or disclosure that occurs as a result of a failure to apply reasonable safeguards or the minimum necessary standard, where required, is not permitted under the Privacy Rule. For example, the minimum necessary standard requires that a covered entity limit who, within the entity, has access to protected health information, based on who needs access to perform their job duties. If a hospital employee is allowed to have routine, unimpeded access to patients' medical records, where such access is not necessary for the hospital employee to do his job, the hospital is not applying the minimum necessary standard. Therefore, any incidental use or disclosure that results from this practice, such as another worker overhearing the hospital employee's conversation about a patient's condition, would be an unlawful use or disclosure under the Privacy Rule.

Administrative Simplification Provisions

- To improve the efficiency of health care delivery by standardizing the electronic data exchange

- To protect the privacy of health care information by setting standards for privacy and security of individually identifiable information

- To empower patients with new rights related to their individually identifiable health information

There are significant penalties for violation of this act.

Offices Affected

Offices that are affected include those that use any form of electronic media, internet, dial-up lines, leased lines, private networks, move PHI from one location to another using magnetic tape, disk, CD media, FAX, and/or has an arrangement with a clearinghouse or any other form of transmitting private information.

PHI is protected health information and includes any and all patient information. PHI is the subject of the HIPAA Privacy Rule.

Permitted Disclosure of PHI

- *With no express permission from the individual*
  - For treatment, payment or for health care operations (TPO)
  - PHI released to the patient
  - PHI released to DHHS
  -
- *With Opportunity to agree or object:*
  - Orally inform the patient of disclosure
    - Verbal consent is OK, but note it in chart who was present and that the patient gave consent
  - Patient allowed to prohibit or restrict
    - Facility directory (i.e. hospital)
    - Disclose to clergy and visitors knowing name
    - Disclose to certain individuals involved in the care
    - Disclose to notify of location or death
    - Disclose to disaster relief agencies

- *With Authorization:*
  - For all uses and disclosures not otherwise permitted
    - Marketing
    - Some fundraising
  - Use approved forms

Not considered marketing if it involves:

- Provider's own health-related products or services
- Treatment
- Case management or care coordination
- Remuneration that is irrelevant
- Face-to-face contact
- Promotional gifts of nominal value

Minimum Necessary Rule

A practice may only use, disclose, or ask for the minimum amount of PHI necessary to accomplish any task, in or out of office. It does not apply to treatment use of PHI.

What Is a Business Associate?

A "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of or provides services to, a covered entity.

- A member of the covered entity's workforce is not a business associate

- A covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity.

- Some specified services listed:
  - Attorneys
  - Accountants
  - Consultants
  - Managers
  - Claims processing or administration
  - Data analysis, processing or administration
  - Utilization review
  - Quality assurance
  - Billing
  - Benefit management
  - Practice management
  - Repricing

Who Must Comply?

- Health plan
- Healthcare clearinghouse
- Health care provider who transmits health information electronically for which there is a HIPAA standard. This can't be avoided by using a billing company.

Your Practice Is NOT A Covered Entity

- If you don't send any claims electronically
- If you don't employ or engage someone else, such as a billing agency or clearinghouse to send electronic claims or other electronic transactions to payers or health plans on your behalf
- If you employ fewer than 10 people

The HIPAA Privacy Rule gives individuals a fundamental new right to be informed of the privacy practices of their health plans and of most of their health care providers, as well as to be informed of their privacy rights with respect to their personal health information. Health plans and covered health care providers are required to develop and distribute a notice that provides a clear explanation of these rights and practices. The notice is intended to focus individuals on privacy issues and concerns and to prompt them to have discussions with their health plans and health care providers and to exercise their rights.

New and established staff should sign a patient confidentiality form for HIPAA and office policy. It should state that any discussion of patient and patient care could be a cause of termination.

Greatest Risk of Potential Violation

- Communication at check-in desk
- Sign-in sheets
    - Allowed, but what information is asked?
        - For example:
            - Name
            - Which doctor are you here to see?
            - Appointment time/arrival time?
    - Forms should be easily read
    - No identifiable information is to be included
        - Examples: Social Security number, phone number, address
    - History taking should be performed confidentially

- Public patient education
    - Viewing videos in waiting areas
    - Handing out printed materials

Tips

- Are doors closed versus open?
- Confidentially order tests, surgery and follow-up visits
- Don't make patients feel uncomfortable about questions
- Make sure patients answer questions by asking permission
- Don't share information with another patient
- Sharing information with a family member is allowed only if the patient has specifically named them and signed the agreement
- Document in the chart who is present during any visit
    - Related
    - Not related
- Ask permission of patient for someone else to be present
- Minor children whose parents are divorced
    - Custodial parent gets information only
    - Unless custodial parent gives permission for the non-custodial parent to receive information
    - Regardless of insurance coverage
- Parents of 18 years or older patient cannot receive information unless the form is signed by the patient
- Sharing information with another office
    - Faxing information is allowed
    - Guarantee information is secure
    - Get a signed patient release of information

Allowed

You may call out a patient's name in a reception area. You may put charts in an exam room chart holder; however, you may not put a detailed schedule in the exam room in plain view. You should place charts so that no identifiable information can be viewed by anyone not allowed to treat the patient. You may share information with a malpractice carrier as well as with a collection agency.

Individual Patient Rights

Patients have a right to a copy of the business/practitioner's Notice of Privacy Practice.

Patients also have a right to:

- Access to and review of their medical records
- Reasonable charges for a copy of forms are allowed
    - Must be stated in Notice of Privacy Practice. Should include that there is a charge but not the amount, which can vary

- Amending records
    - Patients may request a change of records
    - Request change must be submitted in writing
    - Request becomes part of the patient's file
    - Practice may deny the request or note changes in file document
    - Practice may charge for amending the file
    - Again, this must be stated in Notice of Privacy Practice
- Reasonable accommodation issues
- Use and disclosure accountings
- Know who has accessed their health records and for what purpose (documentation)

A good policy may be to review with the patient immediately and have them sign.

Notice of Privacy Practices

The office's Notice of Privacy Practices should be placed in the reception area or some prominent location.

- This represents your practice's public statement about how you handle patient's confidential information
- Anyone, even if they are not a patient, can request to see your Notice of Privacy Practices
- Under the Privacy Rule, you may not use or disclose PHI in a manner inconsistent with your Notice of Privacy Practices
- The comfort level of the patient reflects on the practice and doctor

Your Notice of Privacy Practices should be representative of your business and should include a statement that allows for future changes such as:

> "We reserve the right to make changes to this Notice and to make such changes effective for all PHI we may already have about you. If and when this Notice is changed, we will post a copy in our office in a prominent location. We will also provide you with a copy of the revised Notice upon your request made to our Privacy Officer."

Other information may include:

- How we may use and disclose protected health information about you
- Treatment
- Payment
- Health care operations
- Communication from our office
- Appointment reminders
- Recall notices
    - Postcards
    - Letters

If a patient doesn't like something in your Notice of Privacy Practices, it must be documented and provisions must be taken to comply or not.

Your Notice of Privacy Practices should also include:

- How we may use and disclose protected health information about you
- Individuals involved in your care or payment for your care
- Uses and disclosures we can make without your written authorization
    - Public health activities
    - Abuse, neglect or domestic violence
    - Health oversight activities
    - Lawsuits
    - Coroners, medical examiners, funeral directors
    - Organ and tissue donation
    - Research
- Uses and disclosures of protected health information requiring your authorization
- Right to request restriction
- Right to receive confidential communications
- Right to inspect and copy
- Right to amend
- Right to receive an account of disclosures
- Right to a paper copy of this notice
    - Should not charge for this copy

All business/practitioners must have a designated privacy officer. You must have your staff trained. You must have workforce agreements in place. You must have a non-retaliation policy for whistleblowers.

2013 Changes to HIPAA

There have been significant changes to some of the rules for privacy including violations/penalties. For that reason, we are including the basic changes here. This section is updated and is included for information only and not intended to be considered legal advice.

This omnibus final rule is comprised of the following four final rules:

- Final modifications to the HIPAA Privacy, Security, and Enforcement Rules mandated by the Health Information Technology for Economic and Clinical Health (HITECH) Act, and certain other modifications to improve the Rules, which were issued as a proposed rule on July 14, 2010. These modifications:
    - Make Business Associates of Covered Entities directly liable for compliance with certain of the HIPAA Privacy and Security Rules' requirements
    - Strengthen the limitations on the use and disclosure of protected health information for marketing and fundraising purposes, and prohibit the sale of protected health information without individual authorization

    - Expand individuals' rights to receive electronic copies of their health information and to restrict disclosures to a health plan concerning treatment for which the individual has paid out of pocket in full
    - Require modifications to, and redistribution of, a Covered Entity's notice of privacy practice
    - Modify the individual authorization and other requirements to facilitate research and disclosure of child immunization proof to schools, and to enable access to decedent information by family members or others
    - Adopt the additional HITECH Act enhancements to the Enforcement Rule not previously adopted in the October 30, 2009, interim final rule, such as the provisions addressing enforcement of noncompliance with the HIPAA Rules due to willful neglect
- Final rule adopting changes to the HIPAA Enforcement Rule to incorporate the increased and tiered civil money penalty structure provided by the HITECH Act, originally published as an interim final rule on October 30, 2009
- Final rule on Breach Notification for Unsecured Protected Health Information under the HITECH Act, which replaces the breach notification rule's harm threshold with a more objective standard, and supplants an interim final rule published on August 24, 2009
- Final rule modifying the HIPAA Privacy Rule as required by the Genetic Information Nondiscrimination Act (GINA) to prohibit most health plans from using or disclosing genetic information for underwriting purposes, which was published as a proposed rule on October 7, 2009"

http://federalregister.gov/articles/2013/01/25/2013-01073/modifications-to-the-hipaa-privacy-security-enforcement-and-breach-under-the:

- The effective date of change – March 26, 2013
- The effective date of compliance – September 23, 2013

Omnibus Final 4 Rules-Summary

- Final modifications to the HIPAA Privacy, Security, and Enforcement Rules mandated by the Health Information Technology for Economic and Clinical Health or (HITECH) Act

- Final rule adopting changes to the HIPAA Enforcement Rule to incorporate the increased and tiered civil monetary penalty structure provided by the HITECH Act

- Final rule on Breach Notification for Unsecured Protected Health Information under the HITECH Act, which replaces the breach notification rule's harm threshold with a more objective standard

- Final rule modifying the HIPAA Privacy Rule as required by the Genetic Information Nondiscrimination Act (GINA) to prohibit most health plans from using or disclosing genetic information for underwriting purposes

Who is a Covered Entity for the Privacy Rule Changes?

- The Privacy Rule changes apply to health plans, healthcare clearinghouses, and to any health care provider who transmits health information in electronic form in connection with transactions for which the Secretary of HHS has adopted standards under HIPAA (the covered entities)

HIPAA - Security and Privacy Rules (1)

Business Associates and Subcontractors

- Before the HITECH Act, the Security and Privacy Rules did not apply directly to business associates of covered entities

- Now…Business Associates and their subcontractors are now directly liable for HIPAA Privacy and Security Requirements

Patient Rights

- Expanded an individual's right to receive electronic copies of health information at the patient's request

- Restricted disclosures to health plans concerning treatment for which the individual has paid the out-of-pocket amount in full

- Required modifications to, and redistribution of, a covered entity's notice of privacy practices

- Modified the individual authorization and other requirements to facilitate research and disclosure of child immunization proof to schools

- Enabled access to decedent information by family members or others. PHI protections cease 50 years from the date of death

HIPAA - Security and Privacy Rule (1)

Marketing Communications and Fundraising

- There are new use and disclosure regulations on using a patient's PHI (Protected Health Information) for Sales and Marketing, as well as for Fundraising

HIPAA – Enforcement Rule (2)

Enforcement of noncompliance

- There are increased penalties for those entities that do not comply with the new Breach Notification regulations

Violation Category	**Each Violation**	**Violation Cap.**
Did not know	$100-$50,000	$1.5 million
Reasonable cause	$1000-$50,000	$1.5 million
Willful neglect/corrected	$10,000-$50,000	$1.5 million
Willful neglect/uncorrected	$50,000	$1.5 million

HIPAA- Breach Notification Rule (3)

Breach Notification

- Risk of harm analysis has been removed from the data breach law
- Now…low probability of compromise risk assessment will be assumed unless proved otherwise
- Note: Any inappropriate or impermissible use or disclosure of PHI is a breach

HIPAA- GINA Privacy Rule (4)

- Modified the HIPAA Privacy Rule as required by the Genetic Information Nondiscrimination Act (GINA) to prohibit most health plans from using or disclosing genetic information for underwriting purposes
- Genetic information includes genetic tests, as well as individual's family health history

Compliance-To Do List

What needs to be completed in response to this new Rule?

- Complete updates to the Patient's Notice of Privacy Policy
- Complete updates to Business Associate Agreement, send BAAs to all Business Partners with a due date and confirm BAAs have been returned
- Workflow changes
- Update IT Policies and Procedures
- Train Staff on the changes

What should practices do next?

Notice of Privacy Policy

  - Update your Notice of Privacy Policy documents.
  - Begin the process to update the Patient's Notice of Privacy Policy.
- Once these changes are completed, incorporate them into the front desk workflow. Have all patients to review and sign the new practices
  - You can use the sample guide provided by HHS, see the link below or contact your legal counsel for guidance

http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/notice.html

- Note: This may involve printing a new sign to be posted in the waiting room or materials to be printed and/or laminated

Business Associate Agreements

- Begin sending out the updated Business Associate (BA) Agreements immediately, as it may take your Business Partners some time to review the new BA Agreements and send them back
- If a business partner does not agree to sign your BA Agreement, you should consult with your legal counsel. Place a due date on when the document needs to be returned
- Note: In some cases, you may need to locate new business partners that are equipped to work with healthcare clients

Workflow Changes

- Work with your EHR Vendor to create a workflow to identify visit encounters paid in full by patients
- Alert staff that changes allow a patient to keep "patient paid in full" encounters from review by their insurance company if requested by the patient

IT Policies and Procedures

- Update your IT Policies and Procedures manual with any necessary changes to reflect the new rules
- Develop an office procedure for providing an electronic copy of patient records for patients, upon requests only
- Note: You may need to consult with your IT Service Company for additional assistance

Staff Training

- Schedule time to train your staff on the HIPAA changes
- You can use the HHS Training Material link below for additional training resources:

http://www.hhs.gov/ocr/privacy/hipaa/understanding/training/index.html

Enforcement of HIPAA

The Office for Civil Rights (OCR) will be in charge of enforcing the new HIPAA Omnibus Rule. They are hiring new agents to work on enforcement of the rule. Note: It has been stated that the OCR is preparing to investigate both large and small reported breaches.

Source: http://www.healthcareitnews.com/news/get-set-new-hipaahas-teeth

Resources

- Federal Register, 1/25/2013 Publication
- https://www.federalregister.gov/articles/2013/01/25/2013-01073/modifications-to-thehipaaprivacy-security-enforcement-and-breach-notification-rules-under-the-HHS-website
- http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html
- http://www.hhs.gov/ocr/privacy/hipaa/understanding/training/index.html
- JAMA http://jama.jamanetwork.com/article.aspx?articleid=1660375
- Healthcare IT News
- Source: http://www.healthcareitnews.com/news/get-set-new-hipaa-has-teeth

Disclaimer: Information in this section is to be used for informational and planning purposes only. For specific wording of changes to be included on your organization's legal documents, including Business Associate Agreements or Notice of Privacy Practices, please consult your legal counsel.

National Academy of Opticianry
8401 Corporate Drive #605
Landover, MD 20785
800-229-4828 phone
301-577-3880 fax
www.nao.org