Updated HIPAA Regulations
What Optometrists Need to Know Now

The U.S. Department of Health & Human Services’ Office for Civil Rights recently released updated regulations regarding the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rule. Most optometrists implemented HIPAA compliance protocols in their practices years ago. Those patient privacy protection processes have now become routine for doctors, staff members, and patients. Following the issuance of the new regulations, now is the time to update your compliance procedures. HHS has changed some of the requirements and you face bigger penalties for not paying attention. The frequently asked questions below will help you begin to understand the new regulations and identify the changes that may need to be made in your own practice. Please note, the AOA provides guidance on HIPAA by citing relevant provisions of the HIPAA regulations. This guidance should not be construed as legal advice. You are encouraged to contact an attorney for legal guidance.

HIPAA Overview

What is HIPAA?
The Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules are federal law. The Privacy Rule gives individuals rights over their health information and sets rules and limits on who can look at and receive health information. The Security Rule delineates safeguards to protect health information in electronic form and helps to ensure that electronic protected health information is secure.

Who has to comply with HIPAA?
Individuals, organizations, and agencies that meet the definition of a “covered entity” must comply with HIPAA. An optometrist is considered a “covered entity” if he/she transmits any information in an electronic form in connection with a transaction for which HHS has adopted a standard. For example, submitting an electronic claim to Medicare or another payer is such a transaction. HHS has a tool for determining if you are a covered entity available here: http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/AreYouaCoveredEntity.html

Notice of Privacy Practices

What is a Notice of Privacy Practices (NPP)?
Most covered entities (including optometrists) are required to have a Notice of Privacy Practices (NPP). An NPP describes uses and disclosures of protected health information a covered entity is allowed to make. The NPP also includes the covered entity’s legal duties and privacy practices with respect to protected health information. An patient’s rights with regard to protected health information is also included in an NPP.
Will I need to update my Notice of Privacy Practices (NPP) based on the new HIPAA regulations?

Yes, the new regulations will require you to update your Notice of Privacy Practices (NPP) by September 23, 2013. Below is an overview of changes:

- The NPP must contain a statement indicating that uses and disclosures of protected health information for marketing purposes, and disclosures that constitute a sale of protected health information require authorization, as well as a statement that other uses and disclosures not described in the NPP will be made only with authorization from the patient.
- If the optometrist intends to contact patients to raise funds for the optometry practice, then the NPP must include a statement regarding fundraising communications and a patient’s right to opt out of receiving such communications. The NPP is not required to include the mechanism for patients to opt out of receiving fundraising communications but optometrists can include this information too.
- The NPP must include information informing patients of their new right to restrict certain disclosures of protected health information to a health plan where the patient pays out of pocket in full for the health care item or service.
- NPPs must include a statement of the right of affected patients to be notified following a breach of unsecured protected health information. HHS has noted “a simple statement in the NPP that a patient has a right to or will receive notifications of breaches of his or her unsecured protected health information will suffice for purposes of this requirement.” (Emphasis added by AOA to remind members that encrypted EHRs are not “unsecured” and thus not subject to the same notifications.) HHS also indicates that they “do not intend for this requirement to add undue complexity or length to a covered entity’s NPP. Thus, the statement need not be entity-specific, such as by describing how the covered entity will conduct a risk assessment, include the regulatory descriptions of “breach” or “unsecured PHI,” or describe the types of information to be provided in the actual breach notification to the patient. However, covered entities that wish to include additional or more detailed information may do so.”
- The NPP is not required to include a list of all situations requiring authorization.

Am I required to distribute new Notice of Privacy Practices (NPP) based on the changes required by the new regulations?

Yes, current regulations indicate that when an optometrist with a direct treatment relationship with a patient revises the Notice of Privacy Practices (NPP), the optometry practice must make the NPP available upon request on or after the effective date of the revision and have the NPP available and posted at a clear and prominent location where care is provided.

Do I need to issue a new Notice of Privacy Practices (NPP) to every patient?

No. HHS has specifically indicated, “providers are not required to print and hand out a revised NPP to all patients seeking treatment; providers must post the revised NPP in a clear and prominent location and have copies of the NPP at the delivery site for patients to request to take with them. Providers are only required to give a copy of the NPP to, and obtain a good faith acknowledgment of receipt from, new patients.”

Can I post a summary of the new Notice of Privacy Practices (NPP) and just direct patients to ask for a copy of the full policy from my front desk receptionist?

No.
No. HHS notes that "while health care providers are required to post the NPP in a clear and prominent location at the delivery site, providers may post a summary of the notice in such a location as long as the full notice is immediately available (such as on a table directly under the posted summary) for individuals to pick up without any additional burden on their part. It would not be appropriate, however, to require the individual to have to ask the receptionist for a copy of the full NPP."

**If I already revised my Notice of Privacy Practices (NPP) after the enactment of the HITECH Act and my NPP includes all of the information required by the new regulations, do I need to distribute another NPP to my patients?**

No. If a provider's current Notice of Privacy Practices (NPP) is in accordance with the most recent final rule and patients have been already been informed of the revisions made to the NPP, you would not be required to revise and distribute another NPP.

**Does AOA have a template Notice of Privacy Practices (NPP) I can use?**

A specific template is not currently available. There are many ways a practice can meet the requirements of the regulations and a single approach might not be suitable for every practice.

**Business Associate Agreements**

**What is a business associate agreement?**

According to HHS, “The HIPAA Rules generally require that covered entities and business associates enter into contracts with their business associates to ensure that the business associates will appropriately safeguard protected health information. The business associate contract also serves to clarify and limit, as appropriate, the permissible uses and disclosures of protected health information by the business associate, based on the relationship between the parties and the activities or services being performed by the business associate. A business associate may use or disclose protected health information only as permitted or required by its business associate contract or as required by law. A business associate is directly liable under the HIPAA Rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of protected health information that are not authorized by its contract or required by law. A business associate also is directly liable and subject to civil penalties for failing to safeguard electronic protected health information in accordance with the HIPAA Security Rule.”

**Who is considered a “business associate?” Are subcontractors considered business associates?**

HHS defines a “business associate” as “a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information. A “business associate” also is a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of another business associate.” As noted in the HHS definition, subcontractors are considered business associates under the new regulations.

**Can AOA provide a sample business associate agreement that I can use as a template?**
The Department of Health and Human Services has provided a sample that is available online at:
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

I currently have business associate agreements in place with a number of organizations. Do I need to update all of those BAAs now?

For agreements that were made before January 25, 2013 you have until September 23, 2014 to update the agreements to be compliant with the new regulations. If an agreement is entered into following January 25, 2013 those agreements have to comply with the new regulations by September 23, 2013.

Are business associates required to comply with the Security Rule?

Yes, business associates are required to comply with the Security Rule and business associates will be held directly liable for violations. For more information on compliance with the Security Rule please visit: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule

Breaches of Protected Health Information

What is a breach?

“Breach” is defined, generally, as the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information.

There are three exceptions to this definition that encompass situations Congress intended not to be considered a breach:

(i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted
(ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted
(iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Unless one of the three exemptions noted above applies, HHS indicates that “an acquisition, access, use, or disclosure of protected health information...is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

(i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
(ii) The unauthorized person who used the protected health information or to whom the disclosure was made;
(iii) Whether the protected health information was actually acquired or viewed; and
(iv) The extent to which the risk to the protected health information has been mitigated.”

If the protected health information is secured by encryption, then the security or privacy is
generally not considered compromised and the incident is not considered a breach, so the risk
assessment and subsequent reporting is not required.

What do I need to do if I have had a breach of protected health information in my office?

A risk assessment would first need to be performed to determine whether there was a low
probability that the protected health information had been compromised. The risk assessment
process is outlined above. If it is determined that there was not a low probability of patient
information being compromised, you would be required to notify the impacted patients of the
breach. For a breach of unsecured protected health information involving more than 500 residents,
you must notify prominent media outlets serving the impacted area. This media notice is in
addition to, not a substitute for, the notice to patients. Covered entities, including optometrists, are
also required to report breaches affecting 500 or more patients to the Department of Health and
Human Services immediately, and to maintain a log of breaches affecting fewer than 500 patients
during a year and annually submit the log to the Secretary. HHS has posted instructions for filling
out and submitting the breach form on its Web site at
http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

What information should be included in a breach notification to patients that have been
impacted?

By statute, the following information must be included in a breach notification to impacted patients:

(1) a brief description of what happened, including the date of the breach and the date of the
discovery of the breach, if known;
(2) a description of the types of unsecured protected health information that were involved in the
breach (such as whether full name, social security number, date of birth, home address, account
number, diagnosis, disability code, or other types of information were involved);
(3) any steps individuals should take to protect themselves from potential harm resulting from the
breach;
(4) a brief description of what the covered entity involved is doing to investigate the breach,
mitigate the harm to individuals, and to protect against any further breaches; and
(5) contact procedures for individuals to ask questions or learn additional information, which shall
include a toll-free telephone number, an e-mail address, Web

Does AOA have a breach notification template?

AOA does not have breach notification template, but HHS has indicated that they anticipate
providing additional guidance on breach notifications in the future. This additional guidance may
include templates and examples. AOA will make this information available to members once
released.

How long do I have to notify impacted patients that a breach has occurred?

By statute, optometrists are required to notify patients of a breach “without unreasonable delay”
and no later than 60 calendar days from the discovery of the breach. There may be some instances which are exempt from this timeframe if law enforcement has requested a delay.

**If a breach occurs do I need to include in the notice the names of my employees that were involved?**

Breach notifications are not required to include the names of the employees involved in the breach.

**What if I notify the media that a breach has occurred but they don’t publish my notice?**

HHS has indicated that the media is not obligated to print information regarding breaches of protected health information. Your obligation is to directly notify a prominent media outlet serving the State or jurisdiction where the affected patients live regardless of whether the media publishes or reports the breach to the public. To fulfill the requirement to notify the media of breaches impacting more than 500 people, you would be required to.

**If I’m involved in a breach of PHI that impacts more than 500 people would I fulfill the requirement to notify the media by posting a press release regarding the breach on my website?**

No, HHS indicates that posting the notice on your website would not be sufficient media notification.

---

**Patient Access to Health Records**

**Do patients have additional access to their health records under the new regulations?**

Yes. The new regulations allow patients to request electronic copies of their patient health information. The new regulations specifically require health care providers to provide electronic information to a patient in the electronic format requested by the patient, if it is readily producible, or, if not, in a readable electronic format as agreed to by the health care provider and the patient.

**How quickly do I need to respond to patient requests for their health records?**

Optometrists have 30 days to provide access. You are also allowed a one-time extension of 30 days to respond to the patient’s request. If an extension is needed, written notice must be given to the patient indicating the reasons for delay and the expected date by which the entity will provide the requested information.

**Can I charge patients for providing electronic copies of their health records?**

You are allowed to charge a fee for costs associated with labor and supplies for creating an electronic copy. If the electronic copy is saved to a portable device, such as a flash drive, optometrists may also charge for postage if an patient requests that the optometrist mail the electronic copy. Optometrists are not required to use portable devices that patients provide, if the optometrist conducts a risk analysis and believes there may be a security risk. However, optometrists are also forbidden from requiring patients to purchase a flash drive or other portable device. It’s also important to note that optometrists are prohibited from including fees associated with maintaining systems, retrieval costs, or infrastructure costs in the fee they charge to provide an electronic copy.
**Patient Rights When Paying Out of Pocket for Services Rendered**

If a patient pays out of pocket for treatment can they prohibit me from disclosing their health information to a health plan?

Yes. The regulations require that optometrists agree in most cases to an patient’s request to restrict disclosure to a health plan of the patient’s protected health information that pertains to a health care service for which the patient has paid the health care provider in full out of pocket.

Do I need to create a separate health record to record information related to services that the patient paid for out of pocket and does not want disclosed?

You are not required to create a separate health record, but you are required to ensure an patient’s restriction request is honored. Optometrists will have to decide how to flag information that should not be disclosed.

Can I email a patient’s health record to them if they request an electronic copy of it?

Optometrists are permitted to send patients unencrypted emails if the patient is advised of the risk and the patient still would like the information via email despite the potential risk.

When do I need to make all these changes?

Optometrists have until September 23, 2013 to come into compliance unless an exception applies.

**Selling Patient Information**

Can I sell protected health information to a company?

Selling protected health information would require a patient’s authorization.

A contact lens manufacturer reimburses me for passing information onto my patients regarding their products. Are there any HIPAA concerns with this?

Patient authorization is required before making communications by phone, mail or email regarding products for which the provider is receiving financial remuneration. The authorization required can be general in nature and is not required to relate to a single product or services or even the services of just one specific company. The authorization must, however, describe the intended purpose of the use of the patient information. Communications regarding a drug currently being prescribed to the patient would be exempt from the authorization requirement.

If I talk to my patient about a product from a company that I receive financial remuneration from do I need an authorization?

No. HHS indicates that optometrists may talk with a patient about a product for which the optometrist receives financial remuneration without obtaining patient authorization.
I use a Health Insurance Exchange (HIE) and I pay fees to use the HIE. Is this considered selling patient health information?

No. HHS has indicated that the exchange of health information through an HIE that is paid for is not a sale of protected health information.

What if I only sell a limited data set?

Even sale of a limited data set of protected health information requires prior authorization.

**Penalties and Additional Protections**

What if my state has additional patient privacy protection laws?

If your state has additional privacy protections that are more stringent than the federal regulations then you are also required to comply with those state provisions.

How much are the penalties for non-compliance?

The penalties range from $100 to $50,000 for each violation. A maximum of $1,500,000 will be assessed for violations of the same provision in one calendar year. HHS will take in account a number of factors in determining the financial penalty. Issues such as the extent of the violation, the harm of the violation and other factors will be considered.

How long after a patient has died is a patient’s health information considered protected?

Individually identified patient health information belonging to a person who has been dead for more than 50 years is not considered to be protected health information. It is important to note that this provision is not a record retention requirement.