toll-free: (800) 368-1019
TDD toll-free: (800) 537-7697

Office for Civil Rights
U.S. Department of Health and Human Services
200 Independence Avenue, SW
Room 509F, HHH Building
Washington, D.C. 20201

http://www.hhs.gov/ocr/office/about/contactus/index.html

HIPAA Now 2018

Health Information Portability & Accountability Act

https://hs.utah.gov/

https://www.hhs.gov/hipaa/for-professionals/index.html

http://www.hipaasurvivalguide.com/hipaa-regulations/hipaa-regulations.php

HOT OFF THE PRESS!!! 6/4/2018

- A New York man claims that a CVS pharmacist violated his privacy by discussing his Viagra prescription with his wife, which allegedly led to the breakdown of his marriage. Michael Feinberg, of Long Island, said that he explained to the pharmacist that he would pay out-of-pocket for the pills rather than put it through insurance, the New York Post reported.
- But he claims that a few days later, his wife called the CVS, to discuss her own prescription, and a pharmacist brought up his Viagra script. Feinberg alleges that in doing so, the pharmacist "without solicitation, improperly informed [Feinberg's] wife that [his] prescription for Viagra was not being covered by insurance," and violated his privacy under HIPAA.

http://www.msn.com/en-us/health/medical/man-sues-cvs-after-wife-discovers-viagra-prescription/ar-AAyddNk?li=BBnbfcL&ocid=IDMD

Leaving The Wrong Message

- A hospital employee did not observe minimum necessary requirements when she left a telephone message with the daughter of a patient that detailed both her medical condition and treatment plan. An OCR investigation also indicated that the confidential communications requirements were not followed, as the employee left the message at the patient's home telephone number, despite the patient's instructions to contact her through her work number. To resolve the issues in this case, the hospital developed and implemented several new procedures. One addressed the issue of minimum necessary information in telephone message content. Employees were trained to provide only the minimum necessary information in messages, and were given specific direction as to what information could be left in a message. Employees also were trained to review registration information for patient contact directives regarding leaving messages. The new procedures were incorporated into the standard staff privacy training, both as part of a refresher series and mandatory yearly compliance training.

Disclaimer

- In 2014 *DHHS has changed some of the requirements and you face bigger penalties for not paying attention. Please note, guidance given on HIPAA is done by citing relevant provisions of the HHS HIPAA regulations. This guidance should not be construed as legal advice. You are encouraged to contact an attorney for legal guidance. I* ***will not*** *have all of the answers*

AOA Members

- **HIPAA resources**
- On the new HIPAA Compliance section of the AOA website (member login required to view):
- Updated *AOA HIPAA Security Regulation Compliance Manual* (available free of charge to AOA members)
- Sample *HIPAA Business Associate Agreement*
- Sample *HIPAA Notice of Privacy Practices*, developed by the AOA Office of Counsel for use in optometric practices, which are available in bulk from AOA Marketplace.
- On the AOAExcel™ HIPAA page (member login required to view): AOA White Paper: Updated HIPAA Regulations-What Optometrists Need to Know, with questions and answers about the privacy regulations

http://www.aoa.org/news/practice-management/not-optional-hipaa-compliance-deadline-is-sept-23?sso=y

Cross Country Education

- **Online Seminars (Online Continuing Education)**

Webinars Can't make it to our Live Seminars? Get your CE fast! All you need is a computer and a phone. Try our instructor led Q&A all in real time webinars. Click here to browse our Webinar list...

- **Audio CDs** In the car, on your break-anywhere-these audio materials are convenient ways to absorb information (and inspiration) at your own pace. Many of our conferences and one-day seminars are available in both formats. Click here for more info...

https://www.crosscountryeducation.com/cce/distance-learning/index.jsp

AXWAY

•Road to HIPAA compliance

https://www.axway.com/sites/default/files/infographic_files/axway_infographic_hipaa_compliance_web.pdf

Compliance Specialist

What Do We Do

We understand what you need to know about how Medicare, Medicaid and commercial insurers are profiling your practice through claims analysis. With complete confidentiality between CS EYE and your practice, we analyze your clinic's usage and risk, from an auditor's point of view. We analyze your compliance and your CPT usage to identify red flags and revenue opportunities. If you're doing well, we'll let you know. If you have issues, we'll let you know that too. We'll provide solutions, and a blue print of what you need to address, whether with us or on your own. **Retail price $4000 - call 866-551-0232 for partner pricing**

http://www.cseye.biz/Products.html

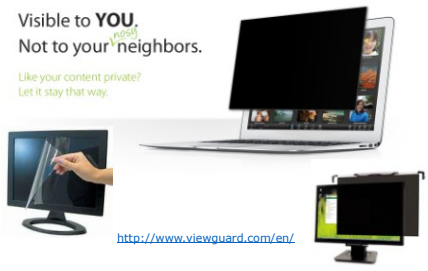
PCI HIPAA (well-priced)

Contact: Jarrod@pcihipaa.com

10 Steps

1. Perform required risk assessment (**on-line**)
2. Designate a HIPAA and Privacy Officer
3. Document all access
4. Update policies and procedures
5. Train employees and document
6. Execute Business Associate Agreements
7. Disaster recovery/ Incident response plan
8. Ensure privacy documents are updated and utilized
9. Email encryption/Data Back-up solutions
10. Obtain Data Breach Coverage

Privacy Screen Filters



http://www.viewguard.com/en/

A New Threat

Cyber attracts are on the rise and major hospitals and corporations are being attacked by these cyber criminals

- Have a good breach protocol
- Have a incident response plan with EMR comp
- You must be able to analyze the attack to ensure that patient privacy was not compromise
- Adequately document the incident

HIPAA Phase 2Audit Program

As a part of its continued efforts to assess compliance with the HIPAA Privacy, Security and Breach Notification Rules, the HHS Office for Civil Rights (OCR) has begun its next phase of audits of covered entities and their business associates. Audits are an important compliance tool for OCR that supplements OCR's other enforcement tools, such as complaint investigations and compliance reviews. These tools enable OCR to identify best practices and proactively uncover and address risks and vulnerabilities to protected health information (PHI).

Cont…

In its 2016 Phase 2 HIPAA Audit Program, OCR will review the policies and procedures adopted and employed by covered entities and their business associates to meet selected standards and implementation specifications of the Privacy, Security, and Breach Notification Rules. These audits will primarily be **desk audits**, although **some on-site** audits will be conducted.

Cont…

The 2016 audit process begins with verification of an entity's address and contact information. An email is being sent to covered entities and business associates requesting that contact information be provided to OCR in a timely manner. OCR will then transmit a pre-audit questionnaire to gather data about the size, type, and operations of potential auditees; this data will be used with other information to create potential audit subject pools.

Cont…

If an entity does not respond to OCR's request to verify its contact information or pre-audit questionnaire, OCR will use publically available information about the entity to create its audit subject pool. **Therefore an entity that does not respond to OCR may still be selected for an audit or subject to a compliance review**. Communications from OCR will be sent via email and may be incorrectly classified as spam. **If your entity's spam filtering and virus protection are automatically enabled, we expect entities to check their junk or spam email folder for emails from OCR**.

When???

Phase Two of OCR's HIPAA audit program is currently underway. **Selected covered entities received notification letters Monday, July 11, 2016. Business associate audits will commence in the fall.** OCR has begun to obtain and verify contact information to identify covered entities and business associates of various types and determine which are appropriate to be included in potential auditee pools. Communications from OCR will be sent via email and may be incorrectly classified as spam. If your entity's spam filtering and virus protection are automatically enabled, we expect you to check your junk or spam email folder for emails from OCR; OSOCRAudit@hhs.gov. Click here to view a sample email letter

#1 Reason for Audit Failure

Failure to provide written proof that a **security risk assessment** has been performed and implemented is the top reason for failing a compliance or HIPAA audit

http://www.cseye.biz/Products.html

Meaningful Use Audit Request

3. Core #15 Protect Electronic Health Information:

Provide proof that a security risk analysis of the Certified EHR Technology was performed prior to the end of the reporting period (i.e. report which documents the procedures performed during the analysis and the results of the analysis.) If deficiencies are identified in this analysis, please supply the implementation plan; this should include completion dates.

Audits On The Rise

- HIPAA audits are on the rise. You'll probably be surprised to learn that patient complaints are the number one driver behind being chosen for a HIPAA audit. And the people that most interact with your patients other than your provider are at your front desk.

Charging for Records

A patient alleged that a covered entity failed to provide him access to his medical records. After OCR notified the entity of the allegation, the entity released the complainant's medical records but also billed him $100.00 for a "records review fee" as well as an administrative fee. The Privacy Rule permits the imposition of a reasonable cost-based fee that includes only the cost of copying and postage and preparing an explanation or summary if agreed to by the individual. To resolve this matter, the covered entity refunded the $100.00 "records review fee."

Who is responsible for HIPAA?

Applies to Everyone

From the top down…

This is a "need to know only" program

HIPAA Statement

- Ask the individual to verify what contact number and address they want to use and if it is ok to leave a message at the number NOPP, … document the attempt
- Verify HIPAA currency at every visit

Important

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 all protect health information (PHI) to include information in any electronic forum.

- All covered entities must have a Security Officer

Who are covered entities?

All those who have to comply with HIPAA regulations. Those who have information which fall into the classification of covered information… **private patient information**

As Congress required in HIPAA, most covered entities have until **April 14, 2003** to come into compliance with these standards, as modified by the August, 2002 final Rule. Small health plans will have an additional year – until April 14, 2004 – to come into compliance.

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

Guidance… this is not new!

- HIPAA Regulations (Federal Law)
- State Laws
- DoD Guidance (Military)
- Accounting only applies to disclosures after April 14, 2003
- Identity theft experts say…

http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/AreYouaCoveredEntity.html

- The HIPAA Privacy Rule for the first time creates national standards to protect individuals' medical records and other personal health information.
- It gives patients more control over their health information.
- It sets boundaries on the use and release of health records.

- It establishes appropriate safeguards that health care providers and others must achieve to protect the privacy of health information.
- It holds violators accountable, with civil and criminal penalties that can be imposed if they violate patients' privacy rights
- And it strikes a balance when public responsibility supports disclosure of some forms of data – for example, to protect public health.

Patient Rights to:

- Receive the privacy notice
- Access, inspect, and have copy of records (30 days)
- Amend and correct medical records (60 days)
- Non-treatment use via valid authorization
- Accounting of disclosures of health information
- Request restrictions on use of information
- Request alternative channels of communication
- Complain to entity or HHS

Minors Becoming Adults – big deal

- Caution: when a patient becomes **18 years of age**, please make sure that patient signs release so that mom and dad get added to HIPAA release authorization

Texting

Texting and emailing HIPAA violations are not always caused by what you think. For example, the biggest violations generally occur between providers and staff, not communicating with patients. You can avoid getting hit with a HIPAA audit and violations with a few simple changes to your current processes. But you have to be able to identify the danger zones.

- Companies advertising (i.e. Qlipsoft.com)
- Is not secure and does require encryption

How long are pt rights 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.

more examples

Here are a few more examples of areas that could be ticking HIPAA time bombs at your front desk unless you take action immediately: * Social Media * Patient Information Access * Patient reminder calls * Release of Information (to both patients and other providers) * Family Member Request for Information * Prescription Pick-up * Charging patients to make copies * Addressing patients by name * Putting Charts Outside Exam Rooms * Fax Requests * Waiting Room Breaches * Etc.

Use and Disclosure

- Use: the sharing, employment, application, utilization, examination or analysis of Protected Health Information (PHI) within the covered entity
- Disclosure: the sharing or release of PHI in any manner outside the covered entity
- Use the term: "secure messaging"

Required Disclosures

- When the individual request it
- To secretary of HHS to determine compliance
- Legal subpoena
- Risk reduction must be a focus
- http://www.hhs.gov/about/regions/fdaser.html

Types of PHI Info

- Name
- Social Security Numbers
- Birthdates
- Addresses
- Driver license info
- Any pictured IDs
- Medical Record Number
- Patient conditions
- Any patient identifying data

Q: Why is the HIPAA Privacy Rule needed?

A: In enacting HIPAA, Congress mandated the establishment of Federal standards for the privacy of individually identifiable health information. When it comes to personal information that moves across hospitals, doctors' offices, insurers or third party payers, and State lines, our country has relied on a patchwork of Federal and State laws. Under the patchwork of laws existing prior to adoption of HIPAA and the Privacy Rule, personal health information could be

Cont…

distributed— without either notice or authorization —for reasons that had nothing to do with a patient's medical treatment or health care reimbursement. For example, unless otherwise forbidden by State or local law, without the Privacy Rule patient information held by a health plan could, without the patient's permission, be passed on to a lender who could then deny the patient's application for a home mortgage or a credit card, or to an employer who could use it in personnel decisions.

Cont…

- The Privacy Rule establishes a Federal floor of safeguards to protect the confidentiality of medical information. State laws which provide stronger privacy protections will continue to apply over and above the new Federal privacy standards.

- For the average health care provider or health plan, the Privacy Rule requires activities, such as:
- Notifying patients about their privacy rights and how their information can be used.
- Adopting and implementing privacy procedures for its practice, hospital, or plan.

Intent to Comply

During an inspection the question of compliance will surface and your office program must demonstrate an intent to comply

Knowledge and willful neglect

You must have a Security Officer!

Self Policing Policies

- All employers must have a sanction policy against non-compliant employees
- Documented breaches in compliance and sanctions must be evident
- The policy is tough and very ambiguous, there are areas you must rethink… construction
- It is difficult to say that no one ever breaks HIPAA guidelines, they made that impossible!

Sanctioning Program

- Denying access to non-compliant employees
- Covered in the organization's HIPAA Policy
- Enforced by leadership

- Training employees so that they understand the privacy procedures. Annual requirements. Within **14 days** of hire…
- Designating an individual to be responsible for seeing that the privacy procedures are adopted and followed
- Securing patient records containing individually identifiable health information so that they are not readily available to those who do not need them

Risk Management

- Loss of patient's confidence
- Loss of reputation
- Loss of accreditation
- Financial operation losses and cost for correcting mistake

Office Privacy Act Responsibilities

- Establish and maintain procedures consistent with the Privacy Act
- Prepare and publish notice of the existence and character of those systems consistent with guidance by GSA
- Establish reasonable administrative, technical, and physical safeguards
- Maintain an account system of all disclosures for six years
- Permit individuals to have access to personal records
- Permit individuals to request records amendments

Question

- **Who must comply with these new HIPAA privacy standards?**

- As required by Congress in HIPAA, the Privacy Rule covers:
- Health plans, Health care clearinghouses
- Health care providers who conduct certain financial and administrative transactions electronically. These electronic transactions are those for which standards have been adopted by the Secretary under HIPAA, such as electronic billing and fund transfers.

Organization Leadership must:

- Organized HIPAA Team

- Key personnel to consider:
  - HIPAA Consultant
  - HIPAA Attorney
  - HIPAA Computer Specialist - **???**

Risk Management Steps

- Determine what are reasonable and appropriate, cost effective, security & Privacy measures of an administrative, technical, or physical safeguards
- **Perform a Risk Assessment**
- Document the policy and procedure (7.6)
- Train and sanction work force
- Memorize it and move on to the next one…

Final Security Regulations

STDs	Section		STDs	
Security Mgt	164.308(a) 1		Facility Access	164.310(a)a
Assigned Responsibility	164.308(a) 2		Work Station Use	164.310(b)
Workforce Security	164.308(a) 3		Work Station Security	164.310(c)
Info Access Management	164.308(a) 4		Device and Media controls	164.310(d)1
Security Awareness Trng	164.308(a) 5		Access Control	164.312(a)1
Security Incident Procedures	164.308(a) 6		Audit Controls	164.312(b)
Contingency plan	164.308(a) 7		Integrity	164.312(c)1
Evaluation	164.308(a) 8		Authentication	164.312(d)
Business Associates Contracts (etc.)	164.308(b) 1		Transmission Security	164.312(e)1

HIPAA Security (CIA)

- **Confidentiality** accessed only by authorized people and processes
- **Integrity** is not altered or destroyed in an unauthorized manner
- **Availability** can be accessed as needed by an authorized person

Four Categories of Security

- **General**
- **Administrative**
- **Physical Safeguards**
- **Technical Safeguards**

Security Management

- Risk Analysis…potential risk (use the **Self-Assessment Tool**)
- Risk Management…risk reduction
- Sanction Policy… against non-compliant employees… must be in view
- Information System Activity Review (regular system reviews…logs, reports)

http://www.healthit.gov/providers-professionals/security-risk-assessment

Why A Security Officer?

- This is your in-house HIPAA protection, your first line of defense against violations
- Your office police to monitor and train your staff
- **The first person** an investigator will want to talk to
- Miss this, and you risk the entire practice

HIPAA Privacy Rule

- This rule overlaps Privacy Act of 1974
- Individuals have the right to receive an accounting of disclosures of PHI made by your office with the exceptions of:
- Treatment
- Payment
- Healthcare Operations
- Accounting must include disclosures made in the past six years of request date

Fundamentals of HIPAA

- Risk analysis and Risk Management
- Written policies and procedures
- Training and sanctioning
- Can have a significant impact on malpractice insurance protection
- Information system activity review
- Security reminders… protection from malicious malware … password mgt
- Suspected or known security breaches
- Back-up data plan

Cont…

- Audit controls … check EMR
- Computer system integrity
- Personal entity authentification
- Decedent family record access

Minimum Necessary Principle

- Requires office to take reasonable steps to limit the use or disclosure of, and request for, PHI to the minimum necessary to accomplish intended purpose

Basic HIPAA Release Rules

Rule #1

You cannot release any info unless you have a valid authorization

Rule #2

You may release pt health info without an authorization if…treatment, payment, operation, healthcare

Rule #3

You may release health info for certain public policy reasons without consent or authorization…

Implementing Standard

- Identify those in your office who need access to PHI to do their job
- Further identify anyone else who may need access
- Create policies and procedures for routine disclosures to achieve purpose of disclosure
- Limit the PHI disclosed by developing criteria
- Review request on individual basis against criteria

Considerations Prior to Disclosure

- Patient notification before release
- Mutually agreed upon alternative communications
- Mutually agreed upon authorizations
- Potential or serious threat or imminent danger to patient or public
- Authority of requestor
- Minimum amount of information necessary for purpose
- Can information be de-identified
- Documentation of release

Requirements for Document

- Date of disclosure
- Name, address, and identity of requestor
- Brief description of PHI disclosed
- Brief statement of the purpose of the disclosure that reasonably informs the individual of basis for disclosure or copy of written request
- Verified identity of requestor

Elements of Valid Authorizations

- Description of used/disclosed information
- Name of person authorized to make request
- Name of person to whom the requested use or disclosure
- An expiration date
- Signature of patient and date
- Statement that information may be subject to re-disclosure by the recipient, therefore, no longer protected under HIPAA
- Verification of requesting party
- Authorization must be written in plain English
- http://www.hhs.gov/news/press/2002pres/20020809.html.
-

PHI Violations Happen

- Employer must have access and termination policies in place … a disaster plan
- Civil penalties … fines to prison
- Ignorance of the law is no excuse
- Deception and false pretense
- Access not intended for patient care
- Personal gain
- Mismanagement of information
- Poor security of information
- Failure to oversight … no security officer

Work Station Policy/Security

- A work station use and security policies states the behavior required by the staff when using a work station (example: log-on/log off, screen saver, viewing protection and physical barriers are in place)… **must hold employee accountable**

- Workstation physical barriers are the responsibility of the employer

Violations and Fines

- Major pharmacy fined $1.44M … customer based on allegations that the customer's pharmacist accessed, reviewed, and shared the customer's prescription history with others who then used the information to intimidate and harass the customer. At the heart of the case was a tangled love triangle in which the pharmacist's husband had previously been romantically involved with the customer, resulting in the birth of a child. When the pharmacist learned of the relationship, she allegedly accessed the customer's prescription information and shared it with her husband, who then used the information to intimidate the customer when she began demanding child support payments.

Cont…

- A licensed practical nurse who pled guilty to wrongfully disclosing a patient's health information for personal gain faces a maximum penalty of 10 years imprisonment, a $250,000 fine or both… accessed a patient's private medical information on November 28, 2006, according to the indictment. She then shared that information with her husband, who on that same day, called the patient. Justin Smith reportedly told the patient he intended to use the information against the patient in an upcoming legal proceeding.

Cont…

- 3 individuals access a dead celebrity's medical record without a clinical need
- They all received a federal conviction for improperly accessing a deceased celebrity's PHI.
- They avoided a jail, but all have federal convictions on their record

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. "
- All Breaches MUST be reported within 60days of discovery!

Breach Guidelines

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

Breach Rules

- *Under 500 patients… notify the patients directly, and OCR/HHS annually*
- *Over 500 patients … notify the media and the patients, and OCR/HHS immediately*
- http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

Breach Notification Guidance

- (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

Violation Cost

- $100 per violation up to $25,000 per year
- Cost associated with correcting the deficiencies
- Most use First Class mail $.49

New 2013 rule protects patient privacy, secures health information

- The changes announced today expand many of the requirements to business associates of these entities that receive protected health information, such as contractors and subcontractors. Some of the largest breaches reported to HHS have involved business associates. Penalties are increased for noncompliance based on the level of negligence with a maximum penalty of $1.5 million per violation. The changes also strengthen the Health Information Technology for Economic and Clinical Health **(HITECH)** Breach Notification requirements by clarifying when breaches of unsecured health information must be reported to HHS.

Individual Request

http://www.hhs.gov/news/press/2013pres/01/20130117b.html

- Patient's can ask for their records in an electronic form
- When individuals pay cash, they instruct the provider not to share the information with their healthcare plan
- The individual can say NO to office marketing efforts…you cannot send them information without their permission
- Makes it easier to share info with other entities (i.e. child's school)

2013 Updates… 23 Sep 13 NLT

- Requires prior authorization for marketing
- Fund raising communications
- Individuals that paid in full & disclosure rights
- Must inform individuals of mandatory notification of breaches
- If you post a NPP (Notice of Privacy Practices) on your web site, it must be a current one
- Rights to restricted use and disclosure PHI
- The HITECH Act establishes rights for individuals to have access to EHR PHI (30 days)
- GINA prohibits health plans for using genetic info of individuals for denial of plan options
-

March 26, 2013: The Rules became effective

EMR Provider

- You must verify that your EMR Provider has verified that your EMR is HIPAA compliant
- Get something in writing
- Can your system be hacked?
- Reporting from your provider on the security of your EMR

Business Associates

- Much of HIPAA applies directly to business associates, and that business associates themselves have obligations relative to *their* business associates. Indeed, not only do "traditional" business associates have increased compliance obligations, but so do their vendors – many of whom might be entirely unaware of this fast-moving train barreling down the tracks.
- Access or use to the PHI

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

What is a Business Associate?

- Business Associates must notify the Covered Entity of a **breach of unsecured PHI** as described in Section 13402 of HITECH.
- The Business Associate is now directly subject to certain **HIPAA Security and Privacy provisions**.
- There is a reciprocal requirement that a Business Associate must take the same steps a Covered Entity must take, if it knows of a pattern or practice of the other party in material breach of the Business Associate Agreement.
- Business Associate Agreements must incorporate the definition of "Business Associate" under HITECH.
- Business Associate Agreements must include a provision that addresses modification of the Agreements in the event of an applicable change in the law.
- Business Associates must comply with general Security Rule Requirements, including:
- Ensure the confidentiality, integrity, and availability of all ePHI;
- Protect against any reasonably anticipated threats or hazards of ePHI;
- Protect against any reasonably anticipated uses or disclosures of ePHI not permitted or required under the Privacy Rule;
- Ensure your workforce complies with the Security Rule.

Business Associates must comply with specific sections of the Security Rule, including

- §164.308 Administrative safeguards
- §164.310 Physical safeguards
- §164.312 Technical safeguards
- §164.314 Organizational requirements
- §164.316 Policies and procedures and documentation requirements.

Public Hospital Corrects Impermissible Disclosure of PHI in Response to a Subpoena

- A public hospital, in response to a subpoena (not accompanied by a court order), impermissibly disclosed the protected health information (PHI) of one of its patients. Contrary to the Privacy Rule protections for information sought for administrative or judicial proceedings, the hospital failed to determine that reasonable efforts had been made to insure that the individual whose PHI was being sought received notice of the request and/or failed to receive satisfactory assurance that the party seeking the information made reasonable efforts to secure a qualified protective order. Among other corrective actions to remedy this situation, OCR required that the hospital revise its subpoena processing procedures. Under the revised process, if a subpoena is received that does not meet the requirements of the Privacy Rule, the information is not disclosed; instead, the hospital contacts the party seeking the subpoena and the requirements of the Privacy Rule are explained. The hospital also trained relevant staff members on the new procedures.

Identifying Business Associates

- Traditional business associates are easy to identify. Many providers outsource claims processing. Providers frequently engage professionals to provide legal, accounting, and various consulting services. When sensitive patient information is no longer needed, providers will often contract with a document shredding company to properly dispose of these records. Because these third parties provide services which involve creating, receiving, maintaining, or transmitting PHI for a HIPAA covered entity, they fall squarely within the definition of business associate.

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. **Clearinghouses must keep clients separate**

BAA Cont…

- 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."

Business Associate Agreements

- 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.
- Any contractor or sub-contractor must have a signed agreement that they will comply with the guidelines established in the law
- That includes marketing and fundraising
- http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

Updating BAA NLT 23 Sep 2013

- 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.

Is HIPAA required for BAA?

- 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
-

Samples of BAA

- Third Party Providers
- EMRs and EHRs
- HIPAA or Secure/Classified Document Couriers or Destruction Companies (Shred)
- Cloud-based systems where you store patient's information
- There are more…

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

- **$750,000 settlement highlights the need for HIPAA business associate agreements**

- Raleigh Orthopaedic Clinic, P.A. of North Carolina (Raleigh Orthopaedic) has agreed to settle charges that it potentially violated the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules by failing to execute a business associate agreement prior to turning over PHI of 17,300 to a potential business partner. Raleigh Orthopaedic is a provider group practice that operates clinics and orthopaedic surgery center in the Raleigh, North Carolina area. The settlement includes a monetary payment of $750,000 and a robust corrective action plan.

Marketing and Sale of PHI

- The Final Rule imposes additional burdens on covered entities and business associates that sell PHI or utilize PHI in furtherance of marketing activities. The Final Rule expands the types of communication that definition of marketing, such that, with limited exception, authorizations are required for all treatment and health care operations communications from a Third Party whose products or services are being described.

Notice of Privacy Practices

- Most covered entities are required to have a Notice of Privacy Practices (NoPP). An NoPP describes uses and disclosures of protected health information a covered entity is allowed to make. The NoPP 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 NoPP. The ophthalmic profession is a covered entity.

NoPP Cont…

- • The NoPP 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 NoPP will be made only with authorization from the patient.

NoPP Cont…

- If the office intends to contact patients to raise funds for the optometry practice, then the NoPP must include a statement regarding fundraising communications and a patient's right to opt out of receiving such communications. The NoPP is not required to include the mechanism for patients to opt out of receiving fundraising communications but optometrists can include this information too.

NoPP Cont…

- The NoPP 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.
- The NoPP **is not required to include a list of all situations** requiring authorization.

NoPP Cont…

- NoPPs 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 NoPP 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." (encrypted EHRs are not "unsecured") HHS also indicates this not intend for this requirement to add undue complexity or length to a covered entity's NPP.

Do I need to send a new NoPP to every patient?

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

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 To Comply With the Security Rule

- **Password Security**
- 1. Protect your user ID and password. Do not share, write down, or post your password under any circumstances!
- 2. Commit your password to memory.
- 3. At a minimum, when creating your password, incorporate a combination of letters and numbers. Avoid dictionary words and personal information.
- 4. Immediately change your password if it is accidentally exposed or compromised.

Cont…Comply With the Security Rule

- 5. Report all password exposures to your department Practice Manager or the Simpson Optical IT contact.
- 6. Adhere to established password management guidelines that may change from time to time.
- 7. Always keep computers password-protected and locked or logged off when not in use.

Security of Communications Containing PHI (E-Mail and Fax)

- Email systems are not secure unless you have explicit information that the system is encrypted or in other ways secure.
- 1. At this time, Simpson Optical does NOT have secure email for sending PHI as part of a regular email. DO NOT SEND PHI AS PART OF A REGULAR EMAIL WITHOUT THE DOCUMENTED PERMISSION OF THE PATIENT.
- 2. Be careful what you send via email. Do not send confidential information unless absolutely necessary. De-identify the information if possible. Warn patients who communicate with you via email that their confidentiality cannot be ensured.

Cont…

- 3. Use the same care in sending emails that you would with a letter. Do not write anything in an email that you might regret later. Assume emails are never erased.
- 4. Do not send attachments containing ePHI without encryption.
- 5. Add a Confidentiality Notice footer to your messages, such as:
- ***CONFIDENTIALITY NOTICE** This email communication and any attachments may contain confidential and privileged information for the use of the designated recipients named above. Distribution, reproduction or any other use of this transmission by any party other than the intended recipient is prohibited.*

Cont…

- 6. If you identify PHI that was sent in error, contact the sender. Do not extend the breach of information by forwarding the identified ePHI to others. Securely dispose of or destroy the information after alerting the sender.
- 7. If you are notified that you sent an email containing PHI to the wrong recipient, confirm that the recipient destroyed all copies and did not use or disclose the information. Immediately contact your Practice Manager for next steps

Health Information Technology for Economic and Clinical Health Act (HITECH)

- The Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009 (42 CFR Parts 412, 413, 422 and 495, and 45 CFR Subtitle A Subchapter D) widened the scope of privacy and security protections required under HIPAA to address such things as business associate services and marketing activities, widened and increased the potential liabilities and consequences for non-compliance including civil and criminal penalties and fines, and provides for enhanced enforcement of the Privacy and Security Rules.

Red Flag Rule

- The Federal Trade Commission, charged with protecting consumers, requires banking and other industries to implement "red flag" standards (12 CFR Part 681) to detect and prevent identity theft related to customer and service accounts. These red flag rules extend to health care institutions.

Action is Required!

- If you suspect:
  - A HIPAA violation
  - Policy violation by a staff member protecting PHI
  - A breach in confidentiality
  - Concerns about any potential PHI physical safeguards risks

2014 HIPAA Updates

- The Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Breach Notification Rules (the HIPAA Rules) protect individuals' identifiable health information held by covered entities and their business associates (called "protected health information" or "PHI"). Covered entities under HIPAA are health care clearinghouses, health plans, and most health care providers.

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

Cont…

- the application of the HIPAA Rules to workplace wellness programs depends on the way in which those programs are structured. Some employers may offer a workplace wellness program as part of a group health plan for employees. For example, some employers may offer certain incentives or rewards related to group health plan benefits, such as reductions in premiums or cost-sharing amounts, in exchange for participation in a wellness program. Other employers may offer workplace wellness programs directly and not in connection with a group health plan.

Cont…

- Where a workplace wellness program is offered as part of a group health plan, the individually identifiable health information collected from or created about participants in the wellness program is PHI and protected by the HIPAA Rules.

Cont…

- While the HIPAA Rules do not directly apply to the employer, a group health plan sponsored by the employer is a covered entity under HIPAA,[1] and HIPAA protects the individually identifiable health information held by the group health plan (or its business associates). HIPAA also protects PHI that is held by the employer as plan sponsor on the plan's behalf when the plan sponsor is administering aspects of the plan, including wellness program benefits offered through the plan

Cont…

- Where a workplace wellness program is offered by an employer directly and not as part of a group health plan, the health information that is collected from employees by the employer is not protected by the HIPAA Rules. However, other Federal or state laws may apply and regulate the collection and/or use of the information.

Nov 2014 Emergency Situations

- Ebola
- Privacy rules ARE NOT aside in case of emergencies
- HIPAA Balanced to ensure proper disclosure and uses of information
  - Necessary to treat patient
  - Necessary to protect the nation or other critical purpose
  - Access to Public Health Authorities: purpose of preventing and controlling disease
  - Share with other organizations like RedCross

http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/emergency/emergencysituations.pdf

Emergency Info Cont…

- May share with anyone to prevent imminent or serious danger
- Disclosure to the media confirming pt is in the facility

October 2014 Same Sex Marriage

- DOMA Act held unconstitutional
- Same sex marriages recognized by US gov…
- Family members have been recognized as legally married same-sex couples

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

Feb 2014 NICS

- National Instant Criminal Background Check System (NICS)
- To prevent guns from being sold to patients with felonies, domestic violence and mental health conditions
- Determined by a lawful authority
- Legal documentation must precede the release of this information

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

Thank you

martralyn@msn.com

https://www.crosscountryeducation.com/cce/product/ShowVideoDetails.do?seminarCode=4560