North Carolina Optometric Society
2018 Spring Congress

HIPAA UPDATE: 2018

Saturday
June 9, 2018
2:00pm – 4:00 pm

PRESENTED BY:
Stephen A. Burt, BS, MFA
President, Healthcare Compliance Resources
an affiliate of Woods Rogers Consulting
10 S. Jefferson Street, Suite 1400
Roanoke, Virginia 24011
Phone: 540-983-7750 Mobile: 540-529-2258
2:00pm – 3:00pm  Introduction to the HIPAA Privacy, Security, and Omnibus Rules

- Review of the Latest Large Breaches and the "Wall of Shame"
- Stronger Enforcement of HIPAA Violations and Imposition of Penalties
- The Privacy Rule and the Security Rule
- Administrative, Physical and Technical Safeguards
- Written Policies and Procedures

3:00pm – 4:00pm  Assuring Compliance with HIPAA

- Security vs. Privacy vs. Confidentiality
- Breaches "Redefined"
- Breach Risk Assessment Protocol
- The Breach Notification “Refined”
- The Security Rule Risk Assessment: An Absolute Must Do
- Tips and Suggestions to Stay Out of HIPAA Trouble

4:00pm - Until  QUESTIONS, ANSWERS AND THE SHARING OF WISDOM

Brief Description

This 2 hour program will provide Optometrists with tools to ensure your Practice is in compliance with requirements of the Health Insurance Portability and Accountability Act (HIPAA). On Jan. 17, 2013, the Department of Health and Human Services (HHS) released the Omnibus Final Rule pursuant to the Health Information Technology for Economic and Clinical Health Act (HITECH Act) and the Genetic Information Nondiscrimination Act of 2008 (GINA). The Final Rule modified and expanded the statements that optometry offices must include in the Notice of Privacy Practices (NOPP), the HIPAA-mandated notice that apprises patients of their rights with regard to protected health information (PHI), and the limits imposed upon an Optometrist's uses and disclosures of PHI. The Final Rule expanded the requirements to provide individuals with a better understanding of

(i) a patient’s right to restrict disclosures;

(ii) the types of uses and disclosures that require individual authorization;

(iii) a patient’s right to opt out of certain disclosures;

(iv) rights to notice in the event of a breach; and

(v) rights with respect to the use of their genetic information for health plan underwriting purposes.
The 2018 HIPAA Update for the North Carolina Optometric Society

A Review of the Latest Large Breaches and the "Wall of Shame"

February 1, 2018 - Five breaches add up to $3.5 million in settlement costs for Fresenius Medical Care (FMC) for that failing to heed HIPAA’s risk analysis and risk management rules. On January 21, 2013, FMC filed five separate breach reports for separate incidents occurring between February 23, 2012 and July 18, 2012 implicating the ePHI of five separate FMC owned covered entities. In addition to a $3.5 million monetary settlement, a corrective action plan requires the FMC covered entities to complete a risk analysis and risk management plan, revise policies and procedures on device and media controls as well as facility access controls, develop an encryption report, and educate its workforce on policies and procedures.

January 17, 2018 - Aetna agreed to pay $17 million to settle a class action lawsuit brought against the insurer for a privacy breach affecting 12,000 patients who took medication to treat or prevent HIV. In July, 2017, Aetna mailed customer notices in envelopes with transparent windows. The transparent windows potentially allowed third parties to see the patient was using HIV medication.

January 9, 2018 - Charles River Medical Associates reported that a hard drive containing information on individuals who received a bone density scan at a radiology lab was lost. The hard drive possibly held PHI on 9,387 individuals who received a scan at the facility’s Framingham lab in the last eight years. The device had no encryption protections and was updated once per month with bone density records to back up the records. Data included social security numbers, insurance ID info, address and phone numbers.

January 4, 2018 - St. Louis, Missouri-based SSM Health recently reported that it experienced a potential data breach after an employee accessed patient records without authorization. The employee was working in the customer service call center. At the time, the employee had PHI access to perform regular job functions. The former employee accessed patient information from multiple states but the focus of his illegal activities involved the medical records of a small number of patients with a controlled substance prescription and a primary care physician within the St. Louis area.

December 28, 2017 - 21st Century Oncology, Inc. (21CO) has agreed to pay $2.3 million in lieu of potential civil money penalties to the HHS Office for Civil Rights (OCR) and adopt a comprehensive corrective action plan to settle potential violations of the HIPAA Privacy and Security Rules. On two separate occasions in 2015, the FBI notified 21CO that PHI was illegally obtained by an unauthorized third party and produced 21CO patient files purchased by an FBI informant. As part of its internal investigation, 21CO determined that the attacker may have accessed 21CO’s network SQL database as early as October 3, 2015, through the remote desktop protocol from an exchange server within 21CO’s network. OCR’s subsequent investigation revealed that 21CO failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the ePHI; failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level; failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports; and disclosed PHI to third party vendors without a written business associate agreement.

May 23, 2017 - St. Luke’s-Roosevelt Hospital Center has paid HHS $387,200 to settle violations of the HIPAA Privacy Rule and agreed to implement a comprehensive corrective action plan. In 2014, OCR received a complaint alleging that a staff member impermissibly disclosed the HIV status, sexually transmitted diseases, medications, sexual orientation, mental health diagnosis, and physical abuse.
THE "WALL of SHAME" - THE NUMBERS OVER 500 in NORTH CAROLINA: The Secretary of Health and Human Services (HHS) must post a list of breaches of unsecured protected health information affecting 500 or more individuals publically – it is known as the "Wall of Shame". These breaches are now posted in a new, more accessible format that allows searching and sorting of the posted breaches. Additionally, this new format includes brief summaries of the breach cases that the Office of Civil Rights (OCR) has investigated and closed, as well as the names of private practice providers who have reported breaches of UPHI to the Secretary. ([https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf))

The following breaches have been reported to the HHS Secretary from Providers in North Carolina:

<table>
<thead>
<tr>
<th>Covered Entity</th>
<th>Individuals Affected</th>
<th>Breach Date</th>
<th>Type of Breach</th>
<th>Location of Breached Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coastal Cape Fear Eye Associates, P.A.</td>
<td>925</td>
<td>02/01/2018</td>
<td>Hacking/IT Incident</td>
<td>Desktop Computer, Network Server</td>
</tr>
<tr>
<td>UNC Health Care System</td>
<td>27,113</td>
<td>12/08/2017</td>
<td>Theft</td>
<td>Desktop Computer</td>
</tr>
<tr>
<td>Carolina Oncology Specialists</td>
<td>1,551</td>
<td>10/16/2017</td>
<td>Unauthorized Access/Disclosure</td>
<td>Electronic Medical Record</td>
</tr>
<tr>
<td>Morehead Memorial Hospital</td>
<td>66,000</td>
<td>09/15/2017</td>
<td>Hacking/IT Incident</td>
<td>Email</td>
</tr>
<tr>
<td>ABB, Inc.</td>
<td>28,012</td>
<td>09/11/2017</td>
<td>Hacking/IT Incident</td>
<td>Email</td>
</tr>
<tr>
<td>The Dermatology Center of Raleigh PA</td>
<td>3,000</td>
<td>07/05/2017</td>
<td>Unauthorized Access/Disclosure</td>
<td>Email</td>
</tr>
<tr>
<td>Jones Family Practice, P.A.</td>
<td>742</td>
<td>05/05/2017</td>
<td>Unauthorized Access/Disclosure</td>
<td>Network Server</td>
</tr>
<tr>
<td>UNC Health Care</td>
<td>1,298</td>
<td>03/20/2017</td>
<td>Unauthorized Access/Disclosure</td>
<td>Paper/Films</td>
</tr>
<tr>
<td>Appalachian Gastroenterology, P.A.</td>
<td>11,000</td>
<td>12/10/2016</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>The Outer Banks Hospital</td>
<td>1,000</td>
<td>08/19/2016</td>
<td>Loss</td>
<td>Other Portable Electronic Device</td>
</tr>
<tr>
<td>Uncommon Care, P.A.</td>
<td>13,674</td>
<td>06/21/2016</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>Vidant Health</td>
<td>897</td>
<td>03/10/2016</td>
<td>Unauthorized Access/Disclosure</td>
<td>Other</td>
</tr>
</tbody>
</table>

Enforcement and Penalties for Noncompliance: The HHS Office for Civil Rights (OCR) reported that as of February 28, 2018, OCR has received over 173,426 HIPAA complaints and has initiated over 835 compliance reviews. They have resolved ninety-eight percent of these cases (168,780). OCR has investigated and resolved over 25,167 cases by requiring changes in privacy practices and corrective actions by, or providing technical assistance to, HIPAA covered entities like your medical office. To date, OCR has settled 52 such cases resulting in a total dollar amount of $72,929,182!

THE NUMBERS OVER 500: Nationally, approximately 177,433,159 people have been affected by 2,224 HIPAA breaches through February 28, 2018, according to data released by the HHS Office for Civil Rights (OCR). The lion’s share of all compromised records was stored or found on network servers. One incident
alone, the hacking attack against health insurer Anthem Inc. in 2016, accounted for 78.8 million of those victims.

### Health Data Breaches (>500) as of February 28, 2018

<table>
<thead>
<tr>
<th># of Breaches</th>
<th>Breach Type</th>
<th># of Individuals Affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>945</td>
<td>Theft</td>
<td>41,858,598</td>
</tr>
<tr>
<td>466</td>
<td>Unauthorized Access</td>
<td>21,978,913</td>
</tr>
<tr>
<td>269</td>
<td>Loss</td>
<td>15,502,131</td>
</tr>
<tr>
<td>185</td>
<td>Hacking/IT Incident</td>
<td>88,815,689</td>
</tr>
<tr>
<td>154</td>
<td>Improper Disposal</td>
<td>12,382,959</td>
</tr>
<tr>
<td>88</td>
<td>Other</td>
<td>4,970,345</td>
</tr>
</tbody>
</table>

(Note: Often breaches are attributed to multiple reasons, so the numbers attributed to any one cause will overstate the total in any one category) Source: HHS

OCR has investigated complaints against many different types of entities including: national pharmacy chains, major medical centers, group health plans, hospital chains, and small provider offices. The privacy areas investigated most often were:
- Impermissible uses and disclosures of protected health information;
- Lack of safeguards of protected health information;
- Lack of patient access and rights to copy their protected health information;
- Uses or disclosures of more than the minimum necessary protected health information; and
- Lack of administrative safeguards of electronic protected health information.

The most common types of covered entities that had to take corrective action were:
- Private Practices (Physicians and Dentists);
- General Hospitals and Nursing Homes;
- Outpatient Facilities;
- Pharmacies; and,
- Health Plans (group health plans and health insurance issuers).

**Stronger Enforcement of HIPAA Violations and Imposition of Penalties**

The HIPAA Enforcement Rule include the provisions affecting compliance and investigations by the Office for Civil Rights (OCR), the imposition of civil money penalties, liability of your Optometry practice for acts or actions by your Business Associates, and mandatory civil monetary penalties for violations due to willful neglect. The HIPAA Enforcement Rule defines "willful neglect" as conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated."

There are two types of HIPAA violation: NEGLIGENT and INTENTIONAL. Examples of negligent violations include the following:
- Disposing of sensitive information without destroying it.
- Connecting unapproved devices like flash drives to the secure network.
- Leaving sensitive information on answering machines.
- Forgetting to log out of the electronic patient record.
Faxing documents containing protected health information to the wrong number in error.

Sending emails with unencrypted attachments.

The other types of violations are those that are **intentional**. These include the following:

- **Snooping** - a violation of the *minimum necessary standard* which dictates that PHI should not be accessed or shared at all unless it is necessary to satisfy a particular function of care.
- Accessing PHI of any kind and sharing it in any way unless it is necessary to satisfy a particular function of care.

**Criminal Penalties: The HITECH Act** clarifies that criminal penalties apply personally to *an individual* or *an employee* of a health care provider that obtains PHI without proper authorization. This provision appears to focus on the improper perusing of health records by employees of the health care entity. Any person, be it a physician, a dentist, a housekeeper, or the Practice Manager, who violates the confidentiality section of HIPAA faces rather strong consequences. The DOJ interpreted the "**knowingly**" element of the HIPAA statute for criminal liability as requiring only knowledge of the actions that constitute an offense. Specific knowledge of an action being in violation of the HIPAA statute is not required.

**OCR has referred 668 cases to the Justice Department for criminal prosecution.** The Justice Department has not calculated how many of the referrals have resulted in action or how many had been returned to OCR. However, the Justice Department has shown more interest in using HIPAA as a criminal enforcement tool as the FBI and federal prosecutors become more comfortable with the law – particularly after the HITECH Act clarified that the criminal penalties apply to *individual employees*!

- If the individual knowingly obtains or discloses individually identifiable health information faces a fine of $50,000 and up to 1-year imprisonment;
- The criminal penalties increase to $100,000 and up to 5-years imprisonment if the wrongful conduct involves false pretenses; and,
- $250,000 and up to 10-years imprisonment if the wrongful conduct involves the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm.

**Post Omnibus Rule HIPAA: The Three Pillars of HIPAA Compliance**

Since April 14, 2003, HIPAA’s Privacy Rule has been the law. Joining in on April 20, 2005 was HIPAA’s Security Rule dealing primarily with electronic health information. On February 17, 2009, with the enactment of the “HITECH” Act, officially the Health Information Technology for Economic and Clinical Health Act of 2009, the rules of the game substantially changed. After much speculation, rumor, innuendo and anticipation, HHS released the final HIPAA Omnibus Rule on January 25, 2013, which significantly amends the original HIPAA Privacy, Security, Breach and Enforcement Rules and formalizes and legitimizes the HITECH Act.

All optometry offices need to stay vigilant with respect to the **Three Pillars** of HIPAA compliance: Privacy Rule Policies and Procedures, current Security Rule Risk Assessments, and workforce training regarding both the Privacy and Security Rule of HIPAA.

**Permitted Uses and Disclosures:** You are permitted, but not required, to use and disclose PHI, **without an individual’s authorization**, for the following purposes or in the following situations:

- To HHS (OCR);
- To the Individual or their Personal Representative;
➢ For Treatment, Payment, and Health Care Operations (TPO);
➢ Opportunity to Agree or Object;
➢ Incident to an otherwise permitted use and disclosure;
➢ Public Interest and Benefit Activities; and
➢ Limited Data Set for the purposes of research, public health or health care operations. Employees may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make.

**Authorization:** You must obtain the individual’s, or their guardian’s, written authorization for any use or disclosure of PHI that is not for treatment, payment or health care operations or otherwise permitted or required by the Privacy Rule. An authorization must be written in specific terms. It may allow use and disclosure of PHI by the covered entity seeking the authorization, or by a third party. All authorizations must be in plain language and contain specific information regarding the PHI to be disclosed, the person disclosing and receiving the information, expiration, and right to revoke in writing. There are very specific elements that must be in an authorization to make it valid, they include:

- A description of the information to be used or disclosed that provides a clear description.
- Name or other specific identification of the person(s), or class of persons, authorized to request use or disclosure of protected health information (PHI).
- Name or other specific identification of the individual that the practice may make the requested use or disclosure.
- An expiration date/event relating to the individual or purpose of use/disclosure.
- Statement of the individual’s right to revoke the authorization.
- Description of how to revoke authorization.
- Statement that the PHI disclosed may be subject to redisclosure and no longer covered by HIPAA.
- Date and signature of the individual authorizing release.
- If signed by other than the individual whose records are being released, a description of the representative’s authority to act for said individual.

**Limiting Uses And Disclosures To The Minimum Necessary:** A central aspect of the Privacy Rule is the principle of “minimum necessary” use and disclosure. Minimum necessary applies when using or disclosing PHI or when requesting PHI from another covered entity or business associate, your Practice must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. Your Practice should have developed and implemented policies and procedures to reasonably limit uses and disclosures to the minimum necessary. When the minimum necessary standard applies to a use or disclosure, you may not use, disclose, or request the entire medical record for a particular purpose unless it can specifically justify the whole record as the amount reasonably needed. Minimum necessary does not apply to:

- Disclosures to or requests by a health care provider for treatment;
- Uses or disclosures made to the patient, as permitted or as required;
- Uses or disclosures made pursuant to an authorization;
- Disclosures made to the Secretary of HHS;
- Uses or disclosures that are required by law; and
- Uses or disclosures which are required for compliance with applicable requirements of HIPAA.

**Access and Uses:** For internal uses, you should have developed and implemented policies and procedures that restrict access and uses of PHI based on the specific roles of the members of their workforce. These policies and procedures identify the persons, or classes of persons, in the workforce who need access to
protected health information to carry out their duties, the categories of protected health information to which access is needed, and any conditions under which they need the information to do their jobs.

**Notice of Privacy Practices (NOPP):** Your optometry office must provide an updated notice of your privacy practices to all your patients on the next visit to your office after you make any changes to the NOPP. The notice must describe the ways in which you may use and disclose PHI. The notice states your duties to protect privacy, provide a notice of privacy practices, and abide by the terms of the current notice. The notice must describe individuals’ rights, including the right to complain to HHS and to complain if they believe their privacy rights have been violated. The notice must include a point of contact, the appointed **Privacy and Security Officer**, for further information and for making complaints. Specifically, it must contain the following language as proscribed by the U.S. Department of Health and Human Services (HHS), prominently displayed in the beginning of the notice:

> **“THIS NOTICE DESCRIBES HOW HEALTH INFORMATION ABOUT YOU (AS A PATIENT OF THIS PRACTICE) MAY BE USED AND DISCLOSED, AND HOW YOU CAN GET ACCESS TO YOUR INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION. PLEASE REVIEW THIS NOTICE CAREFULLY.”**

- It has a statement that your Practice is committed to health information privacy and confidentiality.
- You should state that you have the right to amend or revise this notice if your privacy practices change.
- You must give detailed accounting with examples of how PHI may be used by your Practice.
- You must inform the patient of his/her right to:
  - Receive a copy of your Notice.
  - Authorize disclosure of health information.
  - Restrict certain uses and disclosures of PHI.
  - Restrict disclosure to a health plan if the patient pays for the service in full, out of pocket, at the time of the service.
  - Receive confidential communications – even in email format.
  - Inspect and copy his/her PHI.
  - Amend his/her PHI.
  - Be notified of breaches of unsecured PHI
  - An accounting of PHI disclosures for other than treatment, payment, and health care operations (TPO) and for all disclosures of electronic medical records.
  - Complain about alleged privacy violations by your medical office – or its employees - to the HHS.

**Access and Copy:** Individual patients have the right to access, review and obtain a copy of their PHI maintained by your optometry practice in their “designated record set”. This is the group of records used to make decisions about individual patients, or that is your provider’s medical and billing records about individual patients or a health plan’s enrollment, payment, claims adjudication, and case or medical management record systems. This includes the right to inspect or obtain a copy, or both, of the PHI, as well as direct you to transmit a copy to a designated person or entity of the individual’s choice. Individuals have a right to access this PHI for as long as the information is maintained by your Practice, regardless of the date the information was created; whether the information is maintained in paper or electronic systems onsite, remotely, or is archived; or where the PHI originated.

Remember that you can deny an individual access in certain specified situations, such as when a Provider believes access could cause harm to the individual or another. In addition, two categories of information are expressly excluded from the right of access:

- Psychotherapy notes, and
• Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

**Amendment:** The Rule gives your patients the right to have you amend their PHI in a designated record set when they feel that the information is inaccurate or incomplete. If you accept an amendment request you must make reasonable efforts to provide the amendment to persons that the individual has identified as needing it and to persons that you know might rely on the information to the individual’s detriment. If the request is denied, you must provide the individual with a written denial and allow the individual to submit a **statement of disagreement** for inclusion in the record.

The request can be denied for one of the following reasons:

• The record was not created by your optometry practice, unless the individual provides a reasonable basis to believe that the originator of the protected health information is no longer available to act on the request.
• The information is not a part of the designated record set.
• It would not be available under inspection.
• It is accurate and complete.
• It is accurate and complete.

**Disclosure Accounting:** Individuals have a right to an accounting of the disclosures of their PHI for the previous six years. You do not have to report disclosures due to TPO or initiated by a patient authorization. Since you use an electronic health record (EHR), the patient will have the right to receive an accounting of **ALL** disclosures made during the three years prior to the date of the request. Changes required by the **HITECH Act** make if necessary to provide access and a copy of PHI in electronic format if requested.

**Restriction Request:** Individuals have the right to request that you restrict the use or the disclosure of PHI for treatment, payment or health care operations, disclosure to persons involved in the individual’s health care or payment for health care, or disclosure to notify family members or others about the individual’s general condition, location, or death. You **do not** have to agree to the patient’s request.

**Health Plan Submission Restriction:** The **HITECH Act** requires your optometry practice to comply with an individual’s request to not disclosure PHI to a health plan for payment where you have been **paid in full, out of the pocket, at the time of the service.**

**School Immunizations:** The Rule no longer requires a written authorization for your Practice to disclose immunization records to schools. There is a new provision that permits your Practice (if appropriate) to disclose proof of immunization to a school **where** state or other law requires the school to have such information prior to admitting the student. While written authorization will no longer be required to permit such disclosures, your Practice will still be required to obtain oral agreement from a parent or guardian or, if the individual is an adult or an emancipated minor, from the individual.

**Decedent’s PHI:** Optometry practices are now permitted to disclose a decedent's PHI to a family member or other individual who was **involved in the care**, or payment for care, of the decedent prior to death, so long as the disclosure is not inconsistent with any prior expressed preference of the decedent of which you or your staff may be aware. If in doubt, have the requestor obtain legal paper to access the decedent’s records.

**Confidential Communications Requirements:** Individuals may request an alternative means or location for receiving communications of PHI by means other than those that we typically employ. You **should** try
to accommodate feasible requests. However, you must accommodate reasonable requests if the individual indicates that the disclosure of all or part of the PHI could endanger the individual.

**A FEW MORE PRIVACY RULE ADMINISTRATIVE REQUIREMENTS**

- **Privacy Personnel:** You should have an appointed Privacy and Security Officer who is responsible for developing and implementing policies and procedures and is the contact person for receiving complaints and providing individuals with information on the facility’s HIPAA practices.
- **Workforce Training and Management:** All workforce members must be trained on your privacy policies and procedures, as necessary and appropriate for them to carry out their functions.
- **Data Safeguards:** Your Practice must also maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of PHI in violation of HIPAA and to limit its incidental use and disclosure pursuant to otherwise permitted uses.
- **Employee Sanctions:** Your Practice must have and apply sanctions against employees who violate HIPAA policies and procedures – including termination.
- **Complaints:** Your optometry practice should have implemented procedures for individuals to complain about compliance with HIPAA policies and procedures. There can be no retaliation against a person for exercising rights provided by HIPAA, for assisting in an investigation by HHS, or for opposing an act or practice that the person believes in good faith violates HIPAA.
- **Mitigation:** Your Practice must also mitigate, to the extent practicable, any harmful effect we learn was caused by use or disclosure of protected health information by our workforce or our business associates in violation of our privacy policies and procedures.

**The HIPAA Security Rule Standards**

The Security Rule, which took effect April 20, 2005, requires your Practice to have in place written policies and procedures to prevent unauthorized access to patients’ electronic protected health information (ePHI) and to detect, contain, and correct security violations. Unlike the privacy rule, which governs all forms of PHI the security rule applies only to information that is stored and/or transmitted electronically.

**Security vs. Privacy vs. Confidentiality:** The word "security" should not be confused either with "privacy" or "confidentiality." Privacy refers to the right of an individual to control his personal information and not to have it divulged or used by others against his wishes. "Confidentiality" only becomes an issue once an individual’s PHI has been received by another entity. Confidentiality is a means of protecting that information, usually by safeguarding it from unauthorized disclosure. Security applies to the spectrum of physical, technical and administrative safeguards that are put in place to protect the integrity, availability and confidentiality of information.

**Security Threats:** The Security Rule focuses both on external and internal security threats and vulnerabilities. Threats from "outsiders" include breaking through network firewalls, e-mail attacks through interception or viruses, compromise of passwords, posing as organization "insiders, "computer viruses, and modem number prefix scanning. These activities can result in denial of service, such as the disruption of information flow by "crashing" or overloading critical computer servers. The outsider may steal and misuse proprietary information, including individual health information. Attacks can also affect the integrity of information, by corrupting data that is being transmitted.

Internal threats are of equal concern, and are far more likely to occur according to many security experts. Your Practice must protect against careless staff or others who are unaware of security issues, and curious
or malicious insiders who deliberately take advantage of system vulnerabilities to access and misuse personal health information.

**Overall Approach to HIPAA Security:** Any individually identifiable information created or received by a covered entity is Protected Health Information (PHI), regardless of the media form in which it is (or was) stored. PHI is protected under HIPAA, and the data has many “life forms”:

- **PHI Can Be Stored and At Rest:** Electronically on servers, hard drives, I-phones and flashsticks – or on paper.
- **PHI Can Be in Use:** On your desk as a paper chart, an x-ray on a view box, or reviewing patient information on your computer screen.
- **PHI Can Be in Transit:** Attached in emails, faxes, or in a briefcase.
- **PHI Can Be Destroyed:** Hard drives can be crushed, paper shredded or disk scratched.

**GOALS of the HIPAA SECURITY RULE:** PROTECT and PROVIDE “C”, “I”, “A”

The goals of the security rules are to ensure the confidentiality, integrity and availability of all electronic protected health information, and to protect against anticipated disclosures and threats to the security of the information. The final regulations are divided into "required" and "addressable" standards. While the "required" standards are just that, the "addressable" standards may be mandatory as well.

**THE THREE SAFEGUARDS — The Components of the Security Standards:** The safeguards that comprise HIPAA-mandated security focus on protecting the "confidentiality, integrity, and availability" of individually identifiable health information through the following:

- **Administrative Safeguards** (§164.308) - documented, formal policies, procedures and practices to manage the selection and execution of security measures
- **Physical Safeguards** (§164.310) - protection of computer systems and related buildings and equipment from hazards and intrusion
- **Technical Safeguards** (§164.312) - processes that protect and monitor information access and prevents unauthorized access to data

**Administrative Safeguards** guide personnel, staff and management in regards to PHI and requires your Practice to reasonably safeguard (administrative, technical and physical) information and electronic systems. The cornerstones are risk assessment and risk management—both are "required" standards. Critical and thorough risk analysis must take place before any attempt at regulatory compliance is made.

Particularized vulnerabilities are the focal considerations for all resultant security policies implemented to reduce detected risks. Additional "required" administrative safeguards include:

- Sanctions for workforce noncompliance.
- Tracking of security "incidents," and documented policies and procedures for dealing with incidents. Resulting harm must be mitigated.
- Appointment of a Security Officer.
- Allowing workforce access to ePHI only where appropriate, and putting policies in place to prevent unauthorized persons from gaining access.
- Termination procedures to be used when terminating employees or users to prevent continued access to health information.
- Training workforce on security issues, scaled to the organization.
- Contingency plans for emergencies that damage systems with ePHI, including provisions for data...
back-up, a recovery plan and a mode for continuing critical business processes for the protection of the security of ePHI during emergency operation.

➢ Periodic evaluations of security preparedness, conducted either internally or externally. **Physical Safeguards** are implemented to protect computer servers, systems and connections, including the individual workstations. This category of security standards is focused on preventing unauthorized individuals from gaining access to electronic information. Physical safeguards are concerned with access both to the physical structures of a covered entity and its electronic equipment and covers security concerns related to physical access to buildings, access to workstations, data back-up, storage and obsolete data destruction. ePHI and the computer systems upon which it resides must be protected from unauthorized access, in accordance with defined policies and procedures. The "Required" physical safeguards include:

- **Assigned Security Responsibility** - officially assigning responsibility for information security.
- **Media Controls** - setting up formal procedures for controlling and tracking the handling of hardware and software, and for data backup, storage and disposal.
- **Physical Access Controls** - developing a facility security plan, and setting up disaster recovery, emergency modes, and other access and handling controls.
- **Work Station Use** - policies and procedures to prevent unauthorized access to protected information on workstations and terminals.
- **Security Awareness Training** - awareness training for all employees and others with physical access to protected health information.

**Technical Safeguards** may be the most difficult part of the security regulations to comprehend and implement for those lacking technical savvy. "Technical safeguards" affect PHI that is maintained or transmitted by any electronic media and addresses issues involving authentication of users, audit logs, checking data integrity, and ensuring data transmission security. Technology safeguards are often governed by the particular technologies and data systems in use. Your Practice is expected to balance the need for timely access to needed health information with the need to protect its confidentiality and integrity. "Required" technical safeguards:

- **Access Control** - Establishing policies limiting software program access to only those with authorized access.
- **Audit Controls** - Setting up and maintaining system mechanisms that record and monitor activity ("audit logs") of all systems that contain ePHI.
- **Data Authentication** - Policies to protect and ensure that data is not altered, destroyed or inappropriately processed.
- **Authorization Control** - Obtaining and tracking the consents of patients for use and disclosure of their health information.
- **Entity Authentication** – Developing and employing mechanisms such as automatic logoff, passwords, PINs and biometrics, which identify authorized users and deny access to unauthorized users. Unique log-ins, either numeric or by name, are required - automatic log-offs are not – but certainly demonstrate “prudent practice”.

**Additional Technical Security Safeguards:** Any Practice that transmits health information over open networks must keep it from being easily intercepted by third parties via external entry points. Many transmissions occur when insurance claims are sent to a clearinghouse for processing. Communications and network controls include:

- **Integrity Controls** - internal verification that data that is being stored or transmitted is valid.
- **Message Authentication** - assurance that the messages sent and received are the same messages.
- **Either Access Controls** - such as dedicated, secure communications lines -- or Encryption --
transforming text into unintelligible ciphers thru use of special algorithm processes.

➢ Alarms, Audit Trails, Entity Authentication and Event Reporting.

**BREACHES and BREACH NOTIFICATION “REFINED”**

HHS has eliminated the harm threshold that provided notice of a security breach would only be required if the breach posed a significant risk of harm to affected individuals. It has provided instead that *any use or disclosure* of protected health information (PHI) that is not permitted by the Privacy Rule will be presumed to be a reportable breach.

**Definition:** A breach is defined as the “acquisition, access, use, or disclosure of protected health information in a manner not permitted under the privacy rule which compromises the security or privacy of the protected health information.” The breach notification requirement is only for PHI which is “unsecured” – that is unencrypted or not shredded and disposed of correctly. There has also been a change in the “harm threshold” which must be determined by your Practice’s Security Officer.

HHS has added language to the definition of Breach to clarify that an impermissible use or disclosure of PHI is *presumed to be a Breach unless your medical office demonstrates that there is a low probability that the PHI has been compromised.* HHS emphasized that the burden is on the facility to prove that there is a *low probability* that the information has been compromised.

**The Breach Risk Assessment Protocol That Replaces the “Harm” Standard**

HHS has abandoned the “harm standard” in favor of a four-factor risk assessment approach that focuses more objectively on the risk that the PHI has been compromised. To determine whether there is a *low probability* that the information has been compromised, your Practice must conduct a breach risk analysis and assessment.

The assessment must consider at a minimum, the following four factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.
   a. Identifying financial and demographic data: Social Security number, credit cards, bank checks, financial data
   b. Clinical data: Diagnosis, treatment, medications
   c. Behavioral health, substance abuse, sexually transmitted diseases

2. The unauthorized person who used the PHI or to whom the PHI was disclosed.
   a. Does the person have obligations to protect privacy and security – like a Provider?
   b. Does the person have the ability to re-identify the PHI?

3. Whether the PHI was actually viewed or accessed.
   a. For example, was a stolen laptop later recovered and IT analysis found that PHI was never accessed, viewed, transferred or otherwise compromised, although opportunity existed?
   b. Was the PHI in a sealed envelope or folder that did not have the seal broken?

4. The extent to which the risk to the PHI has been mitigated.
   a. Can the person who received the PHI provide satisfactory assurances that the PHI will not be further used or disclosed or that it will be destroyed?
b. What level of effort has been expended to prevent future related issues and or to lessen the harm of the actual breach?

Your Practice must then evaluate the overall probability that the PHI has been compromised by considering all the factors in combination. HHS emphasizes that it expects such risk assessments to be thorough and completed in good faith, and the conclusions reached to be reasonable. If an evaluation of the factors discussed above fails to demonstrate that there is a low probability that the PHI has been compromised, Breach Notification is required.

**Breach Notification Requirements:** Following a breach of unsecured protected health information, your Practice must provide notification of the breach to affected individuals, the Secretary of Health and Human Services, and, in certain circumstances, to the media. Remember, business associates must notify you that a breach has occurred.

**Individual Notice:** Your Practice must notify affected individuals following the discovery of a breach of unsecured protected health information. You must provide each individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach.

All Breach Notifications must include, to the extent possible:
- A description of the breach;
- A description of the types of information that were involved in the breach;
- The steps affected individuals should take to protect themselves from potential harm;
- A brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches; and
- The contact information for the covered entity.

Additionally, for substitute notice provided via web posting or major print or broadcast media, the notification must include a toll-free number for individuals to contact your Practice to determine if their protected health information was involved in the breach.

**Imminent Harm:** Notice must be given by telephone or other means may be made, in addition to written notice, in cases deemed by your Practice's Security Officer to require urgency because of the possible imminent misuse of unsecured protected health information.

**Media Notice:** Offices that experience a breach affecting more than 500 residents are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction. Your office will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. That means television, newspaper, and radio at a minimum. Like individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

**Notice to HHS:** In addition to notifying affected individuals and the media (where appropriate), your facility must notify the Secretary of HHS of breaches of unsecured protected health information. Your medical office must notify the Secretary by visiting the HHS web site and filling out and electronically submitting the appropriate breach report form. If a breach affects 500 or more individuals, you must notify
the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, your medical office must notify the Secretary of such breaches within sixty days of the ending of the year in which the breach occurred.

**HIPAA RISK ASSESSMENT: SECURITY RULE AND MEANINGFUL USE**

More than 25 OCR resolution agreements and corrective action plans cite the failure of a covered entity to perform an adequate information security risk analysis. OCR’s finding that 83% of their audits found serious problems with the organization’s risk analysis points out the health care industry has a lot of work to do in taking those first steps to safeguarding the information systems that handle PHI. It is just as alarming that 94% audited could not demonstrate they have an effective information security risk management plan.

**Required by the HIPAA Security Rule:** “Risk Analysis (Required): Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.” §164.308(a)(1)(ii)(A)

**MACRA (Medicare Access and CHIP Reauthorization Act):** Conducting a Meaningful Use security risk assessment is REQUIRED for any Optometry practice attesting to Meaningful Use (MU) and MACRA/MIPS in 2017 in order to receive positive or downward payment adjustments. Buried within MACRA lies a key requirement for eligibility and that is the security risk assessment (SRA). Failure to perform an SRA could result in zero scores, which would have a substantial impact on the MACRA fee adjustment, and overall Medicare reimbursement. Conducting an SRA is one of the 3 required core measures that must be met starting in 2017.

It is part of the Advancing Care Information Performance Category and it clearly states two objectives:

1. ****"Protect electronic protected health information (ePHI) created or maintained by the CEHRT through the implementation of appropriate technical, administrative, and physical safeguards."

2. ****"Conduct or review a security risk analysis in accordance with the requirements in 45 CFR 164.308(a)(1), including addressing the security (to include encryption) of ePHI data created or maintained by CEHRT in accordance with requirements in 45 CFR164.312(a)(2)(iv) and 45 CFR 164.306(d)(3), implement security updates as necessary, and correct identified security deficiencies as part of the MIPS eligible clinician’s risk management process."

The HHS/OCR “**Guidance on Risk Analysis Requirements under the HIPAA Security Rule**” relies on the NIST Security framework and specifically NIST SP800-30 Revision 1 Guide for Conducting Risk Assessments. According to both documents and NIST SP800-30:

“**A Risk Analysis is the process of identifying, prioritizing, and estimating risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, ... resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.**”

Even though HIPAA has been around for over a decade, it is making news daily with health data breaches and the upcoming HIPAA audits. With many healthcare organizations, HIPAA is not and has not been a
The 2018 HIPAA Update for NC Optometrists

Top priority within the organization. In fact, many healthcare organizations implemented HIPAA in 2003 and 2005 as required by the compliance dates of the HIPAA Privacy and Security Rule and haven’t done any additional work on compliance.

5 Steps to Conduct a Thorough Risk Analysis

When conducting a HIPAA risk analysis, a checklist of the regulations may be used as a guide, but it is important to understand that a checklist SHOULD NOT be the only item used when conducting a HIPAA Risk Analysis. A checklist can be a good guide as you evaluate your current level of compliance, but other aspects of HIPAA compliance should also be evaluated during a HIPAA Risk Analysis process. In addition to a checklist, healthcare organizations should also follow these simple steps to conduct a complete risk analysis:

1. **Conduct Physical Walk-throughs** – Part of the HIPAA regulations focus on the physical features of an organization. A walk-through should be conducted to determine: How information is being processed, where information may be improperly used, what safeguards are established for electronic equipment, how you are protecting paper records, if people are logging out of computers or systems when they are walking away. These are some basic areas to review during a walkthrough. A simple walkthrough checklist can be helpful during the process.

2. **Collect Supporting Evidence of Compliance** – An organization should collect evidence to support compliance with privacy and security policies and procedures established. For example, if you state that you will conduct information activity review on a bi-monthly basis, an organization will want to ensure that they have evidence of the bi-monthly information activity reviews.

3. **Conduct Workforce Interviews** – Workforce members are the first line of defense with safeguarding and protecting PHI. It is important to understand the workforce’s knowledge and comfort with using and protecting PHI throughout the normal course of business. Ask workforce questions to understand the comfort and adherence to organizational policies and procedures.

4. **Review Unauthorized Uses and Disclosures of PHI (and Data Breaches)** – One area of non-compliance can be from the history of data breaches or unauthorized uses and disclosures of PHI. During the risk analysis process, an organization should evaluate the recent issues with the use and disclosure of PHI to trend issues and evaluate if potential risks exist. For example, if 4 unauthorized disclosures are due to wrong faxes sent, there could be an indication a risk exists with employee education on faxing PHI. Taking time to review this activity can help trend and understand the issues and potential risks within your organization.

5. **Evaluate Conducting Network Security Testing (Penetration Testing)** – While not a requirement, it is a good idea to have penetration testing done to determine if there are security risks within your network infrastructure. Network security testing involves electronically evaluating the current network infrastructure to determine if there are weaknesses in the network. Network weakness can lead to unauthorized intrusion and hacking into a network. Penetration testing will look very different depending on the size and complexity of the network established.

There’s a fair amount of confusion about what constitutes a legitimate HIPAA risk analysis. Healthcare Compliance Resources has found that the NIST SP 800-30 Revision 1: Guide for Conducting Risk
Assessments document to be the best source for conducting a comprehensive Security Rule Risk Assessment. The NIST Risk Analysis process is illustrated on the next page:
The 2018 HIPAA Update for NC Optometrists

Risk Assessment Methodology Flowchart
NIST SP 800-30

**Input**
- Hardware
- Software
- System interfaces
- Data and information
- People
- System mission
- History of system attack
- Data from intelligence agencies, NIIPC, OIG, FedCIRC, mass media
- Reports from prior risk assessments
- Any audit recommendations
- Security requirements
- Security test results
- Current controls
- Planned controls
- Threat-source motivation
- Threat capacity
- Nature of vulnerability
- Current controls
- Mission impact analysis
- Asset criticality assessment
- Data criticality
- Data sensitivity
- Likelihood of treat exploitation
- Magnitude of impact
- Adequacy of planned or current controls

**Risk Assessment Activities**

1. **Step 1. System Characterization**
2. **Step 2. Threat Identification**
3. **Step 3. Vulnerability Identification**
4. **Step 4. Control Analysis**
5. **Step 5. Likelihood Determination**
6. **Step 6. Impact Analysis**
   - Loss of Integrity
   - Loss of Availability
   - Loss of Confidentiality
7. **Step 7. Risk Determination**
8. **Step 8. Control Recommendations**
9. **Step 9. Results Documentation**

**Output**
- System Boundary
- System Functions
- System and Data Criticality
- System and Data Sensitivity
- Threat Statement
- List of Potential Vulnerabilities
- List of Current and Planned Controls
- Likelihood Rating
- Impact Rating
- Risks and Associated Risk Levels
- Recommended Controls
- Risk Assessment Report

- History of system attack
- Data from intelligence agencies, NIIPC, OIG, FedCIRC, mass media
- Reports from prior risk assessments
- Any audit recommendations
- Security requirements
- Security test results
- Current controls
- Planned controls
- Threat-source motivation
- Threat capacity
- Nature of vulnerability
- Current controls
- Mission impact analysis
- Asset criticality assessment
- Data criticality
- Data sensitivity
- Likelihood of treat exploitation
- Magnitude of impact
- Adequacy of planned or current controls

**Input Risk Assessment Activities Output**
Ten Most Common HIPAA Gaps Observed in Optometry Offices

1. **Devices with Patient Information Being Stolen:** This is a common HIPAA violation for many offices. It’s important to ensure the devices your Practice uses, like USB flash drives, mobile devices, I-phones, and laptops, are carefully handled and securely stored to prevent them and the patient information on them from being stolen.

2. **Losing a Device with Patient Information:** Along the same lines as above, it’s also easy (and common) for an employee to lose those kinds of devices. USB flash drives and mobile devices are smaller items, so it’s easy to misplace them. When that happens, it’s easy for sensitive patient information to end up in the wrong hands and if it is not encrypted, vulnerable to discovery.

3. **Improperly Disposing of Papers and Devices with Patient Information:** When it comes time to get rid of papers or devices containing PHI, be sure you properly dispose of them. Crumpling paper in a ball and throwing it in the trash isn’t the correct way to do things nor is shutting down a device and then tossing it in the garbage. Use a ¼” crosscut paper shredder (at least p-5 level) and physically destroy portable media devices before disposing of them.

4. **Not Restricting Access to Patient Information:** "Minimum Necessary" is an absolute rule! Unauthorized access to a patient’s protected health information will get you in serious trouble with HIPAA. Patients trust your office with their PHI, so be smart when handling such information so other patients, employees and relatives who aren’t allowed access don’t come across it.

5. **Hacking/IT Incidences:** Most PHI is now stored on hard drives, server, mobile devices, and in the cloud. Today’s technology allows healthcare practices to more easily communicate and share PHI on these devices. The downfall of this technology is the people who are just as smart, or smarter, than your technology and can easily hack into your devices or systems to get to your PHI. Make sure every device has some type of passcode or authentication, install encryptions and enable personal firewalls and security software. Be sure to keep all security software up-to-date.

6. **Sending Unsecured Sensitive Patient Information through Email:** While it’s no longer a violation to send these kinds of emails, it is a violation if the email is intercepted and/or read by someone without authorized access. Use encryptions and double check that whoever you’re sending the email to is supposed to be receiving the email. You must give informed knowledge to the patient about the dangers of unencrypted, unsecured email transmissions.

7. **Leaving Too Much Patient Information over A Phone Message:** A patient may give you the A-Okay to call them, but be sure you don’t leave a message disclosing too much of their information. A friend or family member could check your patient’s message and hear things they shouldn’t, making said patient upset, or equally as bad, you could call the wrong number and say more than you should, which would probably make your patient even more upset with you. Your safest bet when calling a patient and they don’t answer is to leave a message for them to call you back.

8. **Not Having A “Right To Revoke” Clause:** When your Practice creates its HIPAA Authorization forms, you have to give your patients the right to revoke the permissions they’ve given to disclose their private medical or dental information to certain parties. Not providing this information means your HIPAA forms are invalid and releasing subsequent information to another party puts you in breach of HIPAA. Remember - any HIPAA forms without the patient’s signature is invalid, so releasing information would be a violation.
9. **Employees Sharing Stories About Patient Cases:** People talk. It’s a simple fact. Employees talk with one another and they also talk to patients every workday. Remind them, though, that discussing a patient’s information to an employee lacking authorized access or to other patients is unprofessional and puts your whole practice at risk of being fined by HIPAA.

10. **Employees Snooping Through Files:** It might seem shocking — or maybe not to some — but employees have been caught snooping through patient and co-worker files before. They do this to find out information for themselves but also because relatives or friends ask them to find things out about a certain person. Snooping is wrong and unprofessional on all levels. Make sure your employees are clear on this and that they understand how bad the consequences can be for them and your office for doing so.

**TIPS FOR MITIGATING A HIPAA VIOLATION**

Here are some tips to keep your optometry practice compliant:

- Always use a cover sheet when faxing protected health information
- Email protected health information using secure, encrypted email only or your patient portal
- Assign different levels of security clearance to specific people. Role-based security prevents employees from accidentally changing or seeing information that does not pertain to their specific duties.
- Never share passwords among staff members – your password is a legal signature!
- Properly dispose of information containing PHI by shredding paper files (1/4” cross-cut)
- Make sure computers have updated antivirus scanning software installed. This insures that your practice is reasonably guarded against malicious software
- It's important to make sure any vendors or other businesses associated with your practice are properly following HIPAA standards as well – audit them!
- Always consult a HIPAA compliance attorney for any legal advice or questions concerning HIPAA. You can never be too careful!