HHS Office for Civil Rights 2016 Phase 2 HIPAA Audit Program: An Update for Audiologists

Michael Dybka, Ph.D

Chair, Practice Compliance Committee

American Academy of Audiology

Audiology NOW!

INDIANAPOLIS, IN

CONVENTION: APRIL 5–8, 2017 | EXPOSITION: APRIL 5–7, 2017

#AUDIOLOGYNOW17

AMERICAN ACADEMY OF AUDIOLOGY

Committee Members

Debbie Abel, Au.D

Sarah Crow, Au.D

Margaret Kettler, Au.D

Sarah Kahley, Au.D

Kristin Krotz, Au.D

Gretchen Magee, Au.D

Cassie Thomas, Au.D

Sarah Sydlowski, Au.D, Ph.D, AAA Board Liaison

Kitty Werner, MPA, AAA Staff Liaison

CONNECT. RECONNECT. INNOVATE IN INDY!
CONVENTION: APRIL 5–8, 2017 | EXPOSITION: APRIL 5–7, 2017
AMERICAN ACADEMY OF AUDIOLOGY
Audiology NOW!

Audiologists today are faced with confusing and seemingly unending compliance regulations, rules, and requirements.

Practice Compliance Committee Charge: Identify and communicate to the membership compliance regulations, statutes and rules that impact the practice of audiology.

Develop and provide resources for audiologists to maintain compliance with existing requirements and provide the resources to remain in compliance as changes occur or as new regulations are developed.

Health Insurance Portability and Accountability Act-1996 (HIPAA)

The Privacy Rule, 2003

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

The Security Rule , 2005

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

The Breach Notification Rule, 2010

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

HHS Office for Civil Rights (OCR) is Responsible for Enforcing the Privacy, Security Rules and the Breach Notification Rule

OCR became responsible for enforcing the Privacy Rule in 2003

OCR became responsible for enforcing the Security Rule in 2009

OCR became responsible for enforcing the Breach Notification Rule in 2010

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

OCR Enforces the Privacy, Security, and Breach Notification Rules in Several Ways:

- Investigating complaints

- Conducting compliance reviews to determine if covered entities are in compliance,

- Performing education and outreach to foster compliance with the rules requirements.

- OCR also works in conjunction with the Department of Justice (DOJ) to refer possible criminal violations of HIPAA.

OCR 2016 Phase 2 HIPAA Audit Program.

- In July, 2016-OCR announced its 2016 Phase 2 HIPAA Audit Program. 167 randomly selected covered entities were selected

- The first set of audits were desk audits of covered entities followed by a second round of desk audits of business associates. Auditees were notified of the subject(s) of their audit in a document request letter These audits examined compliance with specific requirements of the Privacy, Security, or Breach Notification Rules.
    - https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html

OCR 2016 Phase 2 HIPAA Audit Program

- In cases of noncompliance, the initial document review may turn into a formal site visit and a more complete HIPAA audit.

- All desk audits in this phase were completed by the end of December 2016.

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

OCR 2016 Phase 2 HIPAA Audit Program.

A third set of audits will be onsite and will examine a broader scope of requirements from the HIPAA Rules than desk audits. Some desk auditees may be subject to a subsequent onsite audit. The number of providers that will be selected for onsite audits is unknown and subject to change.

- Not being chosen for a desk audit does not mean that an entity will not be audited. OCR is expected to start onsite audits sometime in 2017.

- Moreover, OCR has indicated that the phase 2 audits are the start of a more permanent audit program, so while the first batch of desk audits is completed, one should continue to prepare for future audits. http://www.psychiatrictimes.com/career/phase-2-hipaa-audits-strategies-clinicians/page/0/3

OCR 2016 Phase 2 HIPAA Audit Program.

Audits are primarily a compliance improvement activity. OCR will review and analyze information from the final reports.

- Generally, OCR will use the audit reports to determine what types of technical assistance should be developed and what types of corrective action would be most helpful

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

What does The HHS Office for Civil Rights (OCR) 2016 Phase 2 HIPAA Audit Program Mean For Audiologists

Audiologists can no longer be complacent regarding HIPAA regulations, activities, and the move from documentation to enforcement and audits.

- Ongoing privacy and security health-care audits may be moving from education to enforcement, and providers need to ensure that their compliance and operational teams are working together to detect vulnerabilities. jswann1@bna.com.

- The desk audit is not going to be an opportunity for a conversation, there is not going to be an opportunity for a give and take. There will not be an opportunity to develop new policies and procedures or conduct a risk assessment in the short time in which you get the [audit] letter to when you must respond to the audit request, David Holtzman, vice president of compliance services at Cynergistek,

  http://www.physicianspractice.com/mgma14/preparing-hipaa-audit-tips-and-resources

What Practices Should Do

- A good place to start in preparing for a HIPAA audit is to know what areas auditors are likely to focus on most closely, and what areas have tripped up practices in the past.
- Phase 1 of the audit program indicated that many practices fall short when it comes to security rule compliance
- Consider whether your practice has recently conducted a security risk analysis and whether it has appropriate risk management procedures in place.
- **http://www.physicianspractice.com/mgma14/preparing-hipaa-audit-tips-and-resources**

What Practices Should Do

- A security risk assessment is required under the HIPAA Security Rule. Learn about planning, conducting and reviewing the risks and vulnerabilities in your healthcare organization, and how regular risk assessments can protect your practice and your patient data.

Security Risk Analysis

- **https://www.healthit.gov/providers-professionals/video/security-risk-analysis**

- **http://www.physicianspractice.com/mgma14/preparing-hipaa-audit-tips-and-resources**

What Practices Should Do

Consider whether your practice has modified its policies and procedures to comply with the breach notification rules.

- Does your practice have appropriate device and media controls systems in place.
- Is data is encrypted appropriately?
- Do you have appropriate facility access controls?

http://www.physicianspractice.com/mgma14/preparing-hipaa-audit-tips-and-resources

What Practices Should Do

Consider whether your staff and physicians have been trained appropriately on HIPAA rules, and make sure that training is documented.

- The OCR is continually seeing examples in compliance reviews where organizations have trained individuals once when they were first hired, or when the HIPAA privacy rules became law in 2003, and they've done no or little training since

http://www.physicianspractice.com/mgma14/preparing-hipaa-audit-tips-and-resources

What Your HIPAA Program Should Look Like Today

- While audits can seem complex, the OCR does focus on a few core areas that you can use to ensure your practice or organization are ready to prepare for a coming audit.
- Do we have **written** policies and procedures that address HIPAA standards and vulnerabilities?
- Are we performing regular risk assessments? Are those assessments being documented?
- Do we have an incident response plan in case there is a breach of PHI?

https://getreferralmd.com/2015/11/getting-ready-for-hipaa-audits-in-2016-are-you-ready/

What Your HIPAA Program Should Look Like Today

- How are we addressing data security? Does it cover mobile devices and storage media?
- Are patients receiving Notices of Privacy Practices? Is it available to our patients on our portal/practice website?
- Do we have a training program in place that properly informs new staff members and periodically refreshes existing workers on HIPAA compliance

https://getreferralmd.com/2015/11/getting-ready-for-hipaa-audits-in-2016-are-you-ready/

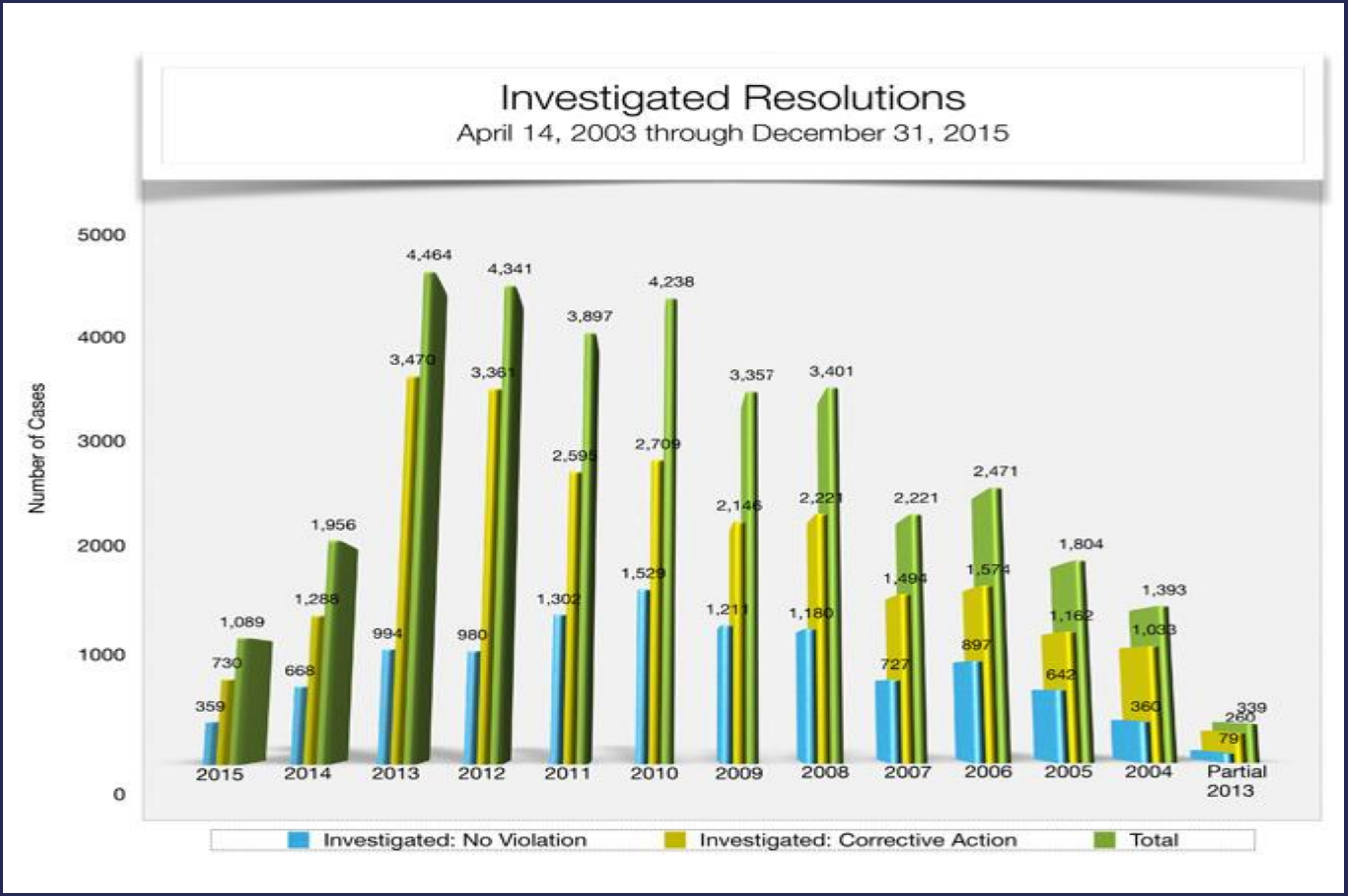
What Your HIPAA Program Should Look Like Today

Cautions

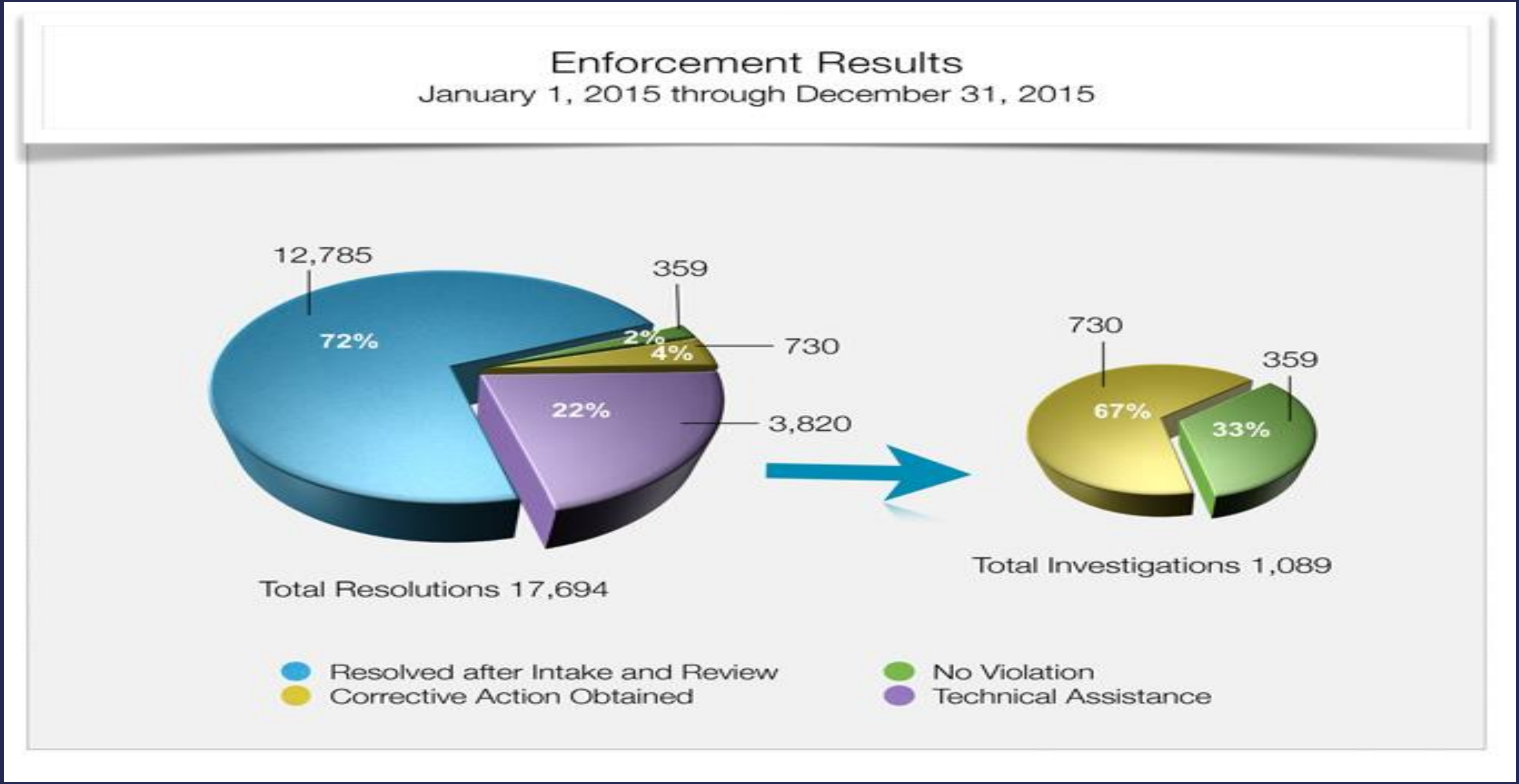
- Do not share sensitive PHI with staff, patients, or family members who should not have access.
- Keep email transmission of PHI to a minimum.
- Backup all disks and storage devices that contain PHI (you may even want to consider a cloud solution).
- Consider a role-based security plan for your employees.
- Keep computers and other hardware updated with the most recent anti-virus scanning software available.

https://getreferralmd.com/2015/11/getting-ready-for-hipaa-audits-in-2016-are-you-ready/

Audits and Fines Are Here to Stay



Audits and Fines Are Here to Stay



Audits and Fines Are Here to Stay

The compliance issues investigated most often are:

- Impermissible uses and disclosures of protected health information
- Lack of safeguards of protected health information
- Lack of patient access to their protected health information
- Use or disclosure of more than the minimum necessary protected health information
- Lack of administrative safeguards of electronic protected health information.

https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html

Audits and Fines Are Here to Stay

The most common types of covered entities that have been required to take corrective action to achieve compliance are:

- Private Practices
- General Hospitals
- Outpatient Facilities
- Pharmacies
- Health Plans (group health plans and health insurance issuers.

https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html

Consequences

VA, CVS Health top list of providers with most HIPAA privacy violations

- ProPublica reported that both the Department of Veterans Affairs and CVS Health received more than 200 privacy complaints that led the HHS Office for Civil Rights to provide corrective action plans or technical assistance from 2011 to 2014,
- The OCR, which received more than 17,000 complaints in 2014, also issued private letters regarding privacy violations to Kaiser Permanente, the Military Health System and Planned Parenthood,

https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html

Consequences

A cancer center notified 22,000 patients of a breach discovered in August 2016.

- Hackers had access to the practice's server between February and July of 2016, local ABC affiliate reported. The files contained names, Social Security numbers, addresses, phone numbers, dates of birth, CPT codes and insurance information.

- The cancer center reported the data breach to the Department of Health and Human Services' Office of Civil Rights on Oct. 21st. However, patients were being notified, five months later. The cancer center didn't provide a reason for the delay.

- Under OCR guidance, all organizations are required to report a breach within 60 days of discovery – not only to the OCR, but to patients and the media.

- In the letter sent to patients, the cancer said the provider couldn't verify whether the data was compromised. Officials also said they don't believe the unauthorized users were after the patient data – but didn't state the reason for that thinking.

Consequences

- A Metropolitan Hospital has been fined $2.2 million under sanctions handed down by the HHS Office for Civil Rights and has entered into a corrective action plan for unauthorized filming of two patients while participating a television series.

- It was the second HIPAA violation for the Hospital, which two years ago paid $3.3 million for a data breach in 2010 in which protected health information on a shared data network was found to be accessible on Google and other Internet search engines.

- The HHS Office for Civil Rights said the latest violation was a result of flaws in the hospitals judgment in allowing filming of the TV series.

Consequences

- A Metropolitan children’s hospital has been fined $3.2 million by the HHS Office for Civil Rights due to the losses of an unencrypted BlackBerry device and laptop in 2009 and 2013, respectively, that contained the unsecured electronic protected health information of about 6,260 individuals.

- The OCR investigation also found the hospital has been noncompliant "over many years regarding multiple standards of the HIPAA Security Rule."

Consequences

- American Medical News reports that a five-doctor practice was **fined $100,000** for a HIPAA violation.
- Posted a publicly available online calendar that showed the dates of surgeries for its clients.
- Failed to document HIPAA training procedures.
- Failed to perform a risk analysis.
- Failed to identify an employee to lead risk analyses and oversee HIPAA compliance.
- Translation: the small practice made little effort to protect patient data and didn't implement the infrastructure that makes day-to-day security possible.

Consequences

- OCR has agreed to a $650,000 settlement with a university resolving HIPAA violations related to a malware infection in 2013.
- In early 2013, malware was installed on a workstation in the Center for Language, Speech, and Hearing. The infection resulted in the impermissible disclosure of the electronic protected health information of 1,670 individuals. Those individuals had their names, addresses, social security numbers, birth dates, health insurance information, diagnoses, and procedure codes disclosed to the those behind the malware attack.

The Practice Compliance Committee is Committed to Monitoring Changes in the Compliance Landscape and Providing the Membership with the Necessary Resources to Remain Current and up to Date

Thank You

Health Insurance Portability and Accountability Act (HIPAA)

The Academy offers a wealth of resources to ensure audiologists and audiology practices maintain compliance with applicable federal regulations and are aware of new regulatory requirements as that information becomes available.

The HHS Office for Civil Rights enforces the HIPAA Privacy Rule, which protects the privacy of individually identifiable health information; the HIPAA Security Rule, which sets national standards for the security of electronic protected health information; and the confidentiality provisions of the Patient Safety Rule, which protects identifiable information being used to analyze patient safety events and improve patient safety, as well as the HITECH Act. These regulations surround the transaction and code sets, privacy, NPI, EIN/TIN (unique identifiers) and security requirements.

HIPAA Privacy Rule- https://www.hhs.gov/hipaa/for-professionals/privacy/

HIPPA Security Rule- https://www.hhs.gov/hipaa/for-professionals/security/

HIPAA Breach Notification- https://www.hhs.gov/hipaa/for-professionals/breach-notification/

HHS Security Risk Assessment Tool

Overview of HIPAA and HITECH Act

HHS Office for Civil Rights

https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/phase2announcement/

HIPAA Resources

www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement- highlights/index.htmlHI)

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

https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html#when

https://www.healthit.gov/providers-professionals/video/security-risk-analysis

http://www.physicianspractice.com/mgma14/preparing-hipaa-audit-tips-and-resources

https://getreferralmd.com/2015/11/getting-ready-for-hipaa-audits-in-2016-are-you-ready/

http://www.hipaajournal.com/category/hipaa-compliance-news/