HIPAA and Meaningful Use (MU) Governmental Program Audits

The Audits are coming!

The Audits are coming!

1

Audit Readiness Meaningful Use and HIPAA

- Both CMS and the Office for Civil Rights (OCR) have been actively auditing Meaningful Use and HIPAA compliance. Much is at stake between these two audit programs.
- This session will highlight the role of compliance in MU and its relationship to HIPAA

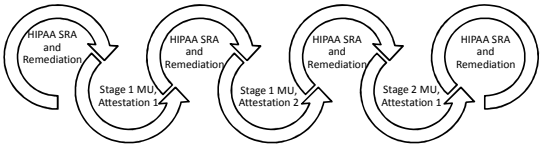
2

Electronic Information Protection

- HIPAA was intended to make the health care system more efficient by standardizing health care transactions.
- Increased use of electronic transactions had concomitant increased security requirements – ***HIPAA Security Rule***
- The HITECH Act was intended to make the healthcare system safer and more efficient by promoting the use of Certified Electronic Health Record Technology (CEHRT)
- The escalation of electronic health record technology has a concomitant escalation in enforcement of the HIPAA Security Rule – ***Meaningful Use Objective and Omnibus Rule***

3

Meaningful Use and HIPAA Compliance Steps



- Each attestation to Meaningful Use requires an updated HIPAA Security Risk Analysis and Remediation Plan.

4

Meaningful Use and Proxy Attestation

- What is the relationship between your organization and its employed physicians?
  - Do your contracts require MU?
  - Does your organization have proxy rights to attest on behalf of the employed physicians?
  - Does your organization disburse or keep incentive funds?
  - Does your organization indemnify your physicians in instances where your infrastructure prevents achievement of meaningful use?
  - What happens when physicians change employment?

5

Meaningful Use Audit Readiness

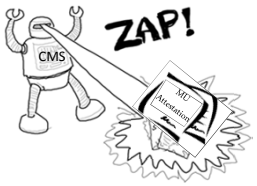
- The HITECH Act mandated that CMS implement an audit program for the EHR Incentive Program – it has started.
- MU attestations are auditable for up to 6 years.
- If one element of a MU attestation is discovered to be unsubstantiated, the entire incentive payment will be revoked.

6

MU Audit FAQ

How many providers are being audited?

- CMS is targeting 5% to 10% of providers who are getting payments for audit
  - That is approximately 1 in 20 providers attesting to MU.



7

MU Audit FAQ

What types of MU audits are being conducted?

- post-pay audits started in mid-2012
- pre-pay audits started mid-2013
- They're really the same thing, but CMS works with the pre-payment auditees more quickly, to prevent payment delays

"We're going to parachute in and do a surprise audit, but I want to keep the whole thing low key."

8

MU Audit FAQ

Are the Medicare, Medicaid and dual-eligible audits the same?

- dual-eligible and Medicare hospitals are the same
- all Medicare EPs are the same
- Medicaid EP and Medicaid-only hospital audits are run by the states

9

MU Audit FAQ

How does CMS select those who will be audited?

- If you are selected you will not be given information as to why. The audit sample:
  - is stratified to look across types of providers and geographic locations
  - includes some randomization
- Employs protocols that identify "suspicious" attestations, for instance:
  - an entire practice in which all professionals have the exact same scores on everything
  - a providers with 100% on every MU objective
  - denominators that ought to be the same but are different

10

MU Audit FAQ

What happens when an eligible provider or eligible hospital doesn't pass the audit? Do they have a period of time to remediate the situation?

- no remediation period; the auditee has to return the payment

11

MU Audit FAQ

Have many auditees needed to return their payment?

- the vast majority passed
- a few failed
- a few got the audit letter and sent back their check (either they knew they wouldn't pass the audit or they didn't have an EHR at all!)
- a few health care providers with adverse audit notices are starting the appeals process and some providers are facing investigation for possible fraud

12

MU Audit FAQ

What is the audit process?

1. You will receive a letter requesting you to post documented evidence that supports your attestation to their web portal within 2 weeks
   - If you need more time, call the auditor and explain why
2. The auditor reviews the documentation

- if everything checks out you do not need to do anything else
- if there are issues, the auditor will ask for further evidence
- If there is disagreement between the auditor and provider about documentation sufficiency, the auditor brings the issue to the CMS staff for a decision
- CMS is making a lot of decisions on a case-by-case basis

13

MU Audit FAQ

What are the most common problematic audit findings to date?

- noncompliance with the requirement that health care providers conduct a proper security risk analysis, which also is a requirement under HIPAA
- lack of adequate documentation to support responses to some of the "yes or no" meaningful use requirements

"I haven't found anything wrong with your books yet, but it's OK for you to go ahead and worry a bit longer."

14

What do you need to be ready?

15

MU Audit Readiness

1. Review the Meaningful Use attestation requirements
   - CMS manual http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/RegistrationandAttestation.html
2. Work with your MU team to plan the content and structure for your Audit Archive
3. Review your provider's audit readiness prior to attesting, as a step in the attestation workflow
4. Retain audit materials for up to 6 years
5. Be prepared to partner with your information systems lead to respond to an audit

16

HIPAA: Meaningful Use Audit Archive

CONTENTS

- SRA, per location, listing deficiencies (note: conducted prior to the end of the reporting period)
  - ❖ NOTE: ensure there is evidence that the SRA was conducted after all of the 2014 CEHRT upgrades were completed
- Deficiency remediation plan, with clearly assigned accountabilities and resolution timelines
- Minutes from Privacy/Security committee meetings evidencing discussion of deficiencies and decision-making about mitigation
- Have available: DR Plan, BC Plan, Breach Notification Plan, example BA Agreement

17

HIPAA Compliance

"Somehow your medical records got faxed to a complete stranger. He has no idea what's wrong with you either."

18

HIPAA Requirements

New rule to strengthen the privacy and security protections

January 17, 2013

- The U.S. Department of Health and Human Services (HHS) announced a new rule to strengthen the privacy and security protections for health information established under 1996 HIPAA.
- The final omnibus rule greatly enhances a patient's privacy protections, provides individuals new rights to their health information, and strengthens the government's ability to enforce the law.

19

HIPAA Requirements

Final modifications to the HIPAA Privacy, Security, and Enforcement Rules, as mandated by the HITECH Act:

- Make business associates of covered entities directly liable for compliance
- Strengthen the limitations on the use and disclosure of protected health information for marketing and fundraising purposes, and prohibit the sale of protected health information without individual authorization
- Expand individuals' rights to receive electronic copies of their health information and to restrict disclosures to a health plan concerning treatment for which the individual has paid out of pocket in full
- Require modifications to, and redistribution of, a covered entity's notice of privacy practices
- Modify the individual authorization and other requirements to facilitate research and disclosure of child immunization proof to schools, and to enable access to decedent information by family members or others
- Adopt the additional HITECH Act enhancements to the Enforcement Rule not previously adopted in the October 30, 2009, interim final rule such as the provisions addressing enforcement of noncompliance with the HIPAA Rules due to willful neglect

20

Penalties

HIPAA Enforcement: What has changed under the final omnibus rule?

- Strengthened civil and criminal enforcement
- New categories for civil monetary penalties
- The penalties vary according to the nature, extent and resulting harm of the violation
- The door has explicitly been left open for additional provisions in future rulemaking

21

Penalties

HIPAA Enforcement: What are the Penalties under HITECH?

- In addition to monetary penalties, the HITECH Act provides for the Department of Justice (DOJ) to pursue criminal penalties for vic individuals who break the law, including:
  - fines of $50,000 to $250,000
  - receive up to ten years in prison
- If the DOJ declines to act on a violation, the Office of Civil Rights may still pursue civil penalties for the same violation

	Type of Offense	Penalty Per Violation	Annual Max	Imprisonment
(A)	Did not know - The person who committed the violation exercised reasonable diligence and did not know that he or she committed a violation.	$100 – $50,000	$1,500,000	(None)
(B)	Reasonable cause - The person who committed the violation did so knowingly, but not due to willful neglect (i.e., a careless and cavalier attitude).	$1,000 – $50,000	$1,500,000	Max 1 yr
(C)(i)	Willful neglect: corrected - The violation was a result of willful neglect but was corrected in a timely manner.	$10,000 – $50,000	$1,500,000	Max 5 yrs
(C)(ii)	Willful neglect: not corrected - The violation was a result of willful neglect, and it was not corrected in a timely manner.	$50,000	$1,500,000	Max 10 yrs

22

Willful Neglect

What Does "Willful Neglect" Mean Under HITECH/ HIPAA?

- "willful neglect" means being unmindful of or cavalier about your compliance strategy

Who Has the Burden of Proof to Demonstrate the Status of a Breach?

- Covered Entities have the burden of proof that willful neglect is NOT the case.

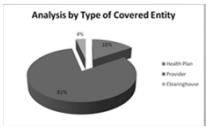
"That woke *me* up, too!"

23

OCR's HIPAA Audit Program

The Office for Civil Rights' (OCR) audit program (mandated by HIPAA) released preliminary findings on June 6, 2012.

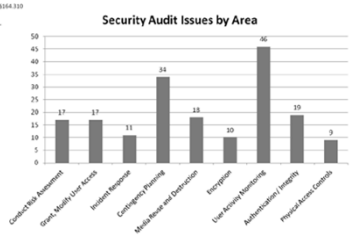
- The majority of the findings were related to the *Security Rule.*
- 50% of the audited entities were healthcare providers;
- 81% of the deficiency findings were attributed to providers.
- Without going into detail, KPMG noted that few covered entities had done a "real" security risk analysis.
- Most of those that did a risk analysis failed to follow up with remediation or mitigation of the risks discovered, automatically qualifying them for "willful neglect".
- In terms of MU, being found deficient on any one measure will cause a provider to be out of compliance, in which case CMS will recoup the entire stimulus for the reporting period in question.



Source: 2012 HIPAA Privacy and Security Audits, OCR, 6/2012

24

OCR's HIPAA Audit Program



The biggest security issues include:

- Risk Analysis and Remediation
- User activity monitoring
- Contingency planning
- Media reuse and destruction
- Granting and modifying user access

Source: 2012 HIPAA Privacy and Security Audits, OCR, 6/2012

25

HIPAA: OCR Audits

OCR WILL BEGIN PHASE 2 OF HIPAA AUDIT PROGRAM IN FALL 2014

Focus:

- areas of greater risk to PHI security
- pervasive noncompliance based on OCR's Phase I Audit findings and observations
- identify technical assistance that it should develop for covered entities and business associates
  - ❖ In circumstances where an audit reveals a serious compliance concern, OCR may initiate a compliance review of the audited organization that could lead to civil money penalties.

26

HIPAA: OCR Audits

HIPAA PHASE 2 AUDIT PROGRAM TARGETS

- risk analysis and risk management (adequate Remediation Planning)
- content and timeliness of breach notifications; notice of privacy practices
- individual access
- device and media controls
- transmission security
- encryption and decryption requirements
- facility access control
- breach reports and complaints
- business associates' risk analysis and risk management and breach reporting to covered entities

27

HIPAA: OCR Audits

What Should You Do to Prepare for the Phase 2 Audits?

1. ensure and document that reasonable and appropriate safeguards in place for PHI that exists in any form, including paper and verbal PHI
2. completed an up-to-date, comprehensive SRA
3. document that remediation of items identified in the SRA have been completed or are on a reasonable timeline to completion
4. regarding *addressable* Security Standards' that are not implemented for any information systems, document:
   - why the standard was not reasonable and appropriate
   - alternative security controls implemented
5. document inventory of information system assets, including mobile devices (even in a bring your own device environment)

28

HIPAA: OCR Audits

What Should You Do to Prepare for the Phase 2 Audits?

6. confirm and document that all systems and software that transmit electronic PHI employ encryption technology
7. confirm and document a facility security plan for each physical location that stores or otherwise has access to PHI, in addition to a security policy that requires a physical security plan
8. review and update HIPAA security policies and procedures
9. inventory business associates and their security posture
10. implement a breach notification policy that accurately reflects the content and deadline requirements
11. ensure a compliant Notice of Privacy Practices is in place
12. document that workforce members have received training on the HIPAA Standards

29

Electronic Health Information Exchange and HIPAA Privacy and Security enforcement will grow together

"Ok, so it's carved in stone, but still open to interpretation, right?"

30

"THAT'S THE LAST BOX TICKED – HAS ANYONE ANYTHING FURTHER TO RAISE?"

31