Compliance *Pro* Solutions™

Automating Privacy Compliance

OCR HIPAA Audit Program 2015 and Beyond What We Know So Far

Kelly McLendon, RHIA, CHPS
Managing Director CompliancePro Solutions™

Agenda

- 2015 and Beyond OCR Audit Program
- Requirements for HIPAA Risk Analysis
- Security Risk Analysis
- Privacy Risk Analysis
- Increasing Risks for Privacy and Security Non-Compliance
- Actions to Reduce Liabilities & Risks

2015 and Beyond OCR Audit Program

OCR HIPAA Audit Program 2014 and Beyond

- Per the Director of OCR and one of their Enforcement staff at the 2015 HIPAA Summit in March 2015, the audit program is coming, but no definite date yet
- The OCR Audit Programs utilize 'protocols' for their audits (the subject matter areas for privacy, security and breach from which the audit questions are generated)
- 2012 were the last protocols issued, but we expect new ones before the launch of the 2015 audit program
- These protocols (the most recent version available) can and should be included within your own internal Security and Privacy Risk Analysis (or 'audit internal programs' for privacy and security, but they are not exactly the same as those questions might be
- In the 2015 audit program OCR brings the audits back in-house, KPMG not being used this time
- 2015 and beyond program builds on findings from previous audits

OCR HIPAA Audit Program 2014 and Beyond

- Out of the tens or hundreds of thousands in the universe of CE and BA – old stats, still valid??
  - 550 - 800 will get introductory 'surveys' that will identify
  - 350 CE's (110 healthcare providers, 45 health plans and 5 clearing houses)
  - 50 BA's to be audited
- CEs begin sometime in 2015...when??
- BAs in 2016?? (35 IT related BAs and 15 non IT related BAs)

 5

OCR HIPAA Audit Program 2014 and Beyond

- Will utilize desktop audits, (remote via e-mail /phone and similar communication focused on hot-spots identified in previous pilot audits such as:
  - HIPAA Security Analysis and Risk Management
  - Breach notification, including timeliness of notification
  - NPP (Notice of Privacy practices)
  - Patient access to their PHI
- Comprehensive on-site, full scope, on-site audits, unsure how many of these might occur vs desktop audits??

 6

Per OCR Director Samuels...2015 and Beyond Audit Program

- Audit program objectives;
  - Identify best practices and uncover risks and vulnerabilities not identified through other enforcement tools; encourage consistent attention to compliance
- Phase 1 - 115 audits (2012) Completed
- Phase 2 – is coming, no dates yet??
- Eventually there will be BA audits and audit protocols, but for now BA's should use CE audit protocols
-

Common Gaps Found in OCR Audits

1. Irregular, undocumented **Workforce Training**
2. Outdated, Incomplete **Policy Documentation**
3. Missing or incomplete **Risk Assessment**
4. Improper/undocumented **Incident Management**

2012 Audit Requirements for Audit Sites

Selected Entities Will	Selected Entities Will Not
Receive advanced notice of at least a week to coordinate personnel and prepare responses to any minor, clearly-defined requests.	Receive any additional findings or observations as part of this evaluation.
Have open lines of communication for any questions and to avoid any surprise requests.	Be expected to provide extensive documents or resources as the evaluation will mostly leverage documents from the pilot audits.
Contribute to improving the audit program through their feedback, helping make a more efficient and effective audit program.	Be subject to on-site visits.
Have the opportunity to convey efforts taken to remediate findings or observations from the pilot audit.	Be provided opportunities to refute findings noted in their audit report.

 4/21/2015 9

OCR Audit Protocols and Program

- OCR website for audit program
- Not yet updated from 2012
- http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html
- Kelly can provide copies of the KPMG 2012 audit protocols, request from:
  kmclendon@complianceprosolutions.com

 4/21/2015 10

OCR Audit Program Phase 2 Previous Announcements

- Audits supposed to target specific high risk issues
- Covers CE's, (health plans, health care providers and clearinghouses BAs
- Coverage of areas identified in 2012 Phase 1 audits
- Risk analysis and risk management (Security Rule)
- Notice of privacy practices and access rights (Privacy Rule)
- Content and timeliness of breach notification (Breach Notification Rule)
- Device and media controls and transmission security (Security Rule)
- Safeguards and training on policies and procedures (Privacy Rule)
- Audits of business associates focused on risk analysis and risk management (Security Rule) and breach reporting to the covered entity (Breach Notification Rule).

2012 Audit Protocols – Privacy, Security and Breach

1	§164.308	Required	§164.308(a)(1) Security Management Process §164.308(a)(1)(ii)(A) - Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health infor...	Conduct Risk Assessment	Inquire of management as to whether formal or informal policies or practices exist to conduct an accurate assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI. Obtain and review relevant doc...
2	§164.308	Required	§164.308(a)(1)(i) Security Management Process - Although the HIPAA Security Rule does not require purchasing any particular technology, additional hardware, software, or services may be needed to adequately protect information. Consideration...	Acquire IT Systems and Services	Inquire of management as to whether formal or informal policy and procedures exist covering the specific features of the HIPAA Security Rule information systems §164.306(a) and (b). Obtain and review formal or informal policy and procedures and eval...
3	§164.308	Required	§164.308(a)(1)(ii)(D) Security Management Process - Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	Develop and Deploy the Information System Activity Review Process	Inquire of management as to whether formal or informal policy and procedures exist to review information system activities, such as audit logs, access reports, and security incident tracking reports. Obtain and review formal or informal policy and p...

2012 Audit Protocols – Security

Sample question: Inquire of management as to whether formal or informal policies or practices exist to conduct an accurate assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI. Obtain and review relevant doc...

Sample question: Inquire of management as to whether an encryption mechanism is in place to protect ePHI. Obtain and review formal or informal policies and procedures and evaluate the content relative to the specified criteria to determine that encryption standards ...

 4/21/2015 13

2012 Audit Protocols – Privacy

Sample question: Inquire of management as to whether the process for disclosing PHI to a coroner or medical examiner is appropriate. Obtain and review disclosures about decedents to determine disclosures are appropriate. Based on the complexity of the entity, eleme...

Sample question: Inquire of management as to whether a process exists to permit certain disclosures of PHI by workforce members who are victims of a crime and the conditions under which they may disclose PHI. Obtain and review the process and evaluate the content in...

 4/21/2015 14

2012 Audit Protocols – Breach

Sample question: Inquire of management as to whether a risk assessment process exists to determine significant harm in a breach.

Sample question: Inquire of management as to whether a process exists for notifying individuals within the required time period. Obtain and review key documents that outline the process for notifying individuals of breaches. Verify, if any breaches have occurred, t...

How to Prepare for 2015 OCR Audits?

1. Perform the Privacy and Security Risk Analysis you already are required to complete to be in compliance!
2. Be careful top understand the depth of an audit, very detailed and requires pulling up information as documentation to be provided
3. Your privacy and security risk analysis may or may not be at an 'audit' depth. That is up to you and your available resources

Requirements for HIPAA Risk Analysis

HIPAA Risk Analysis Requirements

- HIPAA Privacy and Security are two separate, but related topics
- Privacy and Security Risk Analysis ideally should be performed together
- Security Risk Analysis is required for Meaningful Use participants annually
- Privacy Risk Analysis is not required by Meaningful Use but is equally important
- For HIPAA there is no specific timeline spelled out in regulation, but ample evidence tells us that Privacy and Security Risk Analysis should be performed *annually* with continuous monitoring and updating in between
- Plus documentation needs to be kept surrounding these analyses for 6 years

HIPAA Requirements for Risk Analysis

- **§164.308(a) Security Risk Analysis**
  - Security Management Process standard, at § 164.308(a)(1)(i)) in the Administrative Safeguards section of the Security Rule, requires covered entities to "implement policies and procedures to prevent, detect, contain, and correct security violations."
  - Required **implementation specification at § 164.308(a)(1)(ii)(A), for Risk Analysis,** requires a covered entity to, "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."
  - Required **implementation specification at § 164.308(a)(1)(ii)(B), for Risk Management,** requires a covered entity to "implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a) [(the General Requirements of the Security Rule)]."
  - **www.HealthIT.gov/security-risk-assessment**

 19

Meaningful Use Requirements for SRA

- In Stage 1, eligible professionals must conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a) (1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process.
- In Stage 2, eligible professionals need to meet the same security risk analysis requirements as Stage 1, but must also address the encryption/security of data at rest.
- Note: a security risk analysis needs to be conducted or reviewed during each reporting period for Stage 1 and Stage 2

 20

HIPAA Requirements for Risk Analysis

- **164.530 (c)(1) & (i) (1)-(5) Privacy Risk Analysis**
- **(1) *Standard: Safeguards.*** A covered entity must have in place **appropriate administrative, technical, and physical safeguards** to protect the privacy of protected health information.
- **(1) *Standard: Policies and procedures.*** A covered entity must **implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements** of this subpart and subpart D of this part. The policies and procedures must be reasonably designed, taking into account the size and the type of activities that relate to protected health information undertaken by a covered entity, to ensure such compliance.

 21

NIST Security Guidance

NIST National Institute of Standards and Technology U.S. Department of Commerce

- Much of the HIPAA Security Rule is built on NIST guidance, other security regulations are as well, therefore following NIST guidance forms a good basis for compliance across multiple enforcement bodies and for civil liabilities
- Security Risk Analysis originates in NIST guidelines and are adopted for HIPAA
- Recently there has been a new 'Framework' from NIST: Improving Critical Infrastructure Cybersecurity' which reaches across multiple verticals, including healthcare
  - 'Consists of standards, methodologies, procedures, and processes that align business and technological approaches to address cyber risks

 22

Security Risk Analysis

HIPAA Security Risk Analysis

- A review of all current policies, procedures, plans and other documentation that support an organizations' HIPAA information Security Compliance Plan
- A detailed organizational assessment based on NIST SP 800 – 66, An Introductory Resource Guide for Implementing the HIPAA Security Rule
- A comprehensive HIPAA Security Gap type Risk Analysis includes for each HIPAA Security *standard*, *implementation specification*, and *requirement*
- Document key data and compliance measurements, identify gaps, assess risk, and mutually define a Action Item (mitigation plan) based on prioritization according to 'Risk'
- 'Risk' = 'Threat' + 'Vulnerability' + 'Impact'
- Remember to also be reasonable and appropriate for smaller operations…

Security Rule Sections

The following sections are created by statue within the Security Rule, they are also the foundation for designing a SRA tool (Framework)

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

 25

SRA Components

Areas to cover within a SRA include:

- Policies & procedures (P&P) to prevent, detect and correct security violations and define appropriate sanctions
- Assigned security responsibility (i.e. Security Officer and Governance)
- Appropriate and authorized access to PHI and clear termination procedures (and de-provisioning of access)
- Security awareness and training for entire workforce

 26

SRA Components

- Security incident procedures
- Contingency and back-up plans
- Periodic evaluation and monitoring of security compliance with continual feedback and remediation
- Ensure compliance of BAs
- Facility access controls
- Workstation use
- Workstation security
- Device and media controls
- Access controls
- Audit controls
- Integrity
- Person or entry authentication
- Transmission security

 27

Privacy Risk Analysis

 28

Privacy Risk Analysis

- Since there are both HIPAA Privacy and Security rules, analysis of your Compliance Program must address each rule
- Therefore Privacy Risk Analysis (PRA) are equally important to Security Risk Analysis, where a MU participant or not
- Although OCR audit criteria breaks privacy and breach into two sets, an overarching privacy analysis, in my opinion, breach can be rolled into privacy most easily, so I address privacy and breach together
  - With some breach addressed by the technical side of a SRA

 29

Privacy Risk Analysis

- Unlike the Security Rule, the HIPAA Privacy Rules do not contain the ingredients for creation of a Privacy Risk Analysis
- Therefore you must find a source that understands the rules well enough to create a PRA tool ('Framework') that manages the process
- Once the PRA tool and methodology are identified, perform the analysis
- From the analysis create a prioritized 'Action Item' list of items to mitigate to work on in order of priority
- Although not required' the prioritization of the mitigation items identified should be based upon logical criteria similar to what is used for a SRA
- Update the assessment on a routine (annually?) basis
- The actual assessment tool may be MS-Excel or internet based, be sure to keep the copies for the required 6 years

 30

Privacy Risk Analysis Components

A ROBUST Privacy Risk Analysis (PRA) contains questions that explore:

- Details about the organization's Privacy Compliance Program
- Privacy (and Breach) policies and procedures and communication
- Workforce privacy training
- Designated Record Sets
- Incident Management and Breach Notification
- Incident History
- BA Management
- Research
- Privacy Compliance Technology

4

 31

Increasing Risks For Privacy and Security Non-Compliance

 32

CMS Audits for Security Risk Analysis

- Since the Meaningful Use program requires a Security Risk Analysis (SRA) which mirrors what HIPAA requires, each participant has to preform a SRA annually;
- And attest that they have remediated *all* of the identified Action Items in a prioritized manner
- Based on my experience there was widespread non-compliance with this requirements
- CMS Auditors, Figliozzi and Associates have been auditing MU recipients and in some cases demanding the money be repaid
- If a MU participant pay particular attention to this requirement and ensure your documentation is complete

 33

Resolution Agreements and CMPs

Over $28 Million in Resolution Agreements & Fines

Enforcement Highlights:

Covered Entity	Amount
Adult & Pediatric Dermatology, P.C. of Massachusetts *(Dec. 2013)*	$150,000
Affinity Health Plan *(Aug 2013)*	$1,215,780
WellPoint *(July 2013)*	$1,700,000
Shasta Regional Medical Center *(June 2013)*	$275,000
Idaho State University *(May 2013)*	$400,000
Hospice of North Idaho $50,000 *(Dec 2012)*	$50,000
Massachusetts Eye and Ear Institute *(Sept 2012)*	$1,500,000
Alaska DHSS *(June 2012)*	$1,700,000
Phoenix Cardiac Surgery *(Apr 2012)*	$100,000
BCBS Tennessee *(March 2012)*	$1,500,000
UCLA Health System *(July 2011)*	$865,500
Massachusetts General Hospital *(Feb 2011)*	$1,000,000
Cignet Health CMP *(Feb. 2011)*	$4.3 Million
Summary Judgment US District Court for Cignet *(Aug 2013)*	$4,782,845
Management Services Organization of Washington *(Dec 2010)*	$35,000
Rite Aid Corporation *(July 2010)*	$1,000,000
CVS Pharmacy, Inc. *(Jan 2009)*	$2,250,000
Providence Health & Services *(July 2008)*	$100,000

** Data as of February 2014*

 34

States Get Into Regulations and Enforcement

State now active in issuing Regs and Penalties as they ramp up Enforcement

- HITECH gave State Attorneys General the authority to bring civil actions on behalf of state residents for violations of the HIPAA Privacy and Security Rules.
- OCR trained States on HIPAA Enforcement
- At least 47 States have passed forms of privacy and security regulation with penalties. Many of these are for 'General Industry' and many supersede HIPAA
- But...use of HIPAA rules for breach determination s is still the Gold Standard and useful for the States

A lot of State activity as the result of the Target breach

 4/21/2015 35

FTC and FCC step up to Regulate in Addition to HIPAA

- The FTC (Federal Trade Commission) has begun enforcement of general industry privacy and security, but also some in healthcare
- FCC says don't forget about us too!
- This trend is sure to increase as privacy and security are universally supported by patients and consumers *and* their politicians
- This represents a vast expansion of enforcement power that is much wider in scope than HIPAA
- Part of an overlapping strategy to increase privacy / security across all sectors, not just healthcare

 36

Actions to Reduce Liabilities & Risks

Actions to Reduce Liability & Risks

- Utilize consistent, robust Security and Privacy Risk Analysis tools (Frameworks) and complete, at least every year, continually managing mitigation and remediation items until they are no longer issues
- Stick to your prioritized Action Items mitigation plans as much as possible
- Update privacy and security incident response plans and procedures
- Automate privacy and security incident investigation, tracking and management
- Automate your HIPAA compliance program, especially if managing PHI with attached 'patient's rights'
- Upgrade BAA (Business Associate Agreements) and working to ensure BA and Subcontractor compliance
- Build advanced security technology for cyber protection and monitoring capabilities
- Acquire cyber liability insurance

Conclusion

- HIPAA Privacy and Security increasingly are being enforced by the Federal Government and via related State regulations
- Meaningful Use requires a Security Risk Analysis be completed and attested to each year, get organized and use a SRA tool and methodology
- Privacy is equally important as security for HIPAA compliance, therefore use of a formal PRA tool and methodology is highly recommended
- Remember Business Associates have the same rules to comply by performing both privacy and security risk analysis as a part of their Privacy and Security Compliance Programs

Resources

- Office for Civil Rights (OCR)
  http://www.hhs.gov/ocr/privacy/
- HIPAA Security Final Rule 2003
- HIPAA Privacy Rules Updated for Omnibus
- NIST 800-66 Introductory Resource for HIPAA Security Rule
- NIST 800-30 Risk Management Guide for IT Systems
- ONC Published free tools
- OCR published FAQs and on-line guidance

CompliancePro Solutions™
Automating Privacy Compliance

For Questions, Comments and Requests, please contact:

Kelly McLendon, RHIA, CHPS

E-mail: *kmclendon@complianceprosolutions.com*

Web: *www.complianceprosolutions.com*

Phone: 321-268-0320

 41

Product and Service Sheet

- "The Legal Health Record: Regulations, Policies, and Guidance Available through AHIMA.org" by Kelly McLendon, RHIA, CHPS

CompliancePro Solutions

- Security and Privacy Risk Assessments and Remediation.
- A full suite of Privacy / Security Training and Education Templates.
- Subject Matter Expertise and Consulting for Privacy and Security.

PrivacyPro

- Full lifecycle support for wrongful disclosures, including investigation, breach analysis, risk assessment, and final reporting.
- Workflow automation for amendments, restrictions, accounting of disclosures, and other HIPAA events.
- A Reference Library containing over 100 industry regulations, best practices, customizable privacy and security policy and other form templates.
- Links to Fair Warning Privacy Monitoring.

 42