Preparing for a HIPAA Audit

August 30, 2016

HealthInsight

This Webinar is Brought to You By….

HealthInsight

HIPAAOne
PROTECT YOUR ePHI

Mountain-Pacific Quality Health

HealtHIE NEVADA
YOUR HEALTH INFORMATION EXCHANGE

PASS

About HealthInsight and Mountain-Pacific Quality Health

- HealthInsight and Mountain-Pacific Quality Health are private, non-profit, community-based Quality Improvement Organizations (QIO) that have dedicated more than three decades to improving health and health care and are composed of locally governed organizations in: Alaska, Hawaii, Montana, Nevada, New Mexico, Oregon, Utah and Wyoming. As part of our efforts to assist hospitals and practices with HIPAA compliance, HealthInsight and Mountain-Pacific Quality Health teamed together to form **HIPAA Privacy and Security Solutions**, or ***HIPAA PASS***, to offer affordable, easy and comprehensive Risk Analysis and Risk Management services.

About HIPAA One®

- Following a thorough search for the best software to assist our practices and hospitals to achieve HIPAA compliance, HIPAA One® emerged as the clear solution.
- For more information about HIPAA One® please visit:

https://www.youtube.com/watch?v=9G_B7U_pnuo&feature=youtu.be

Mark Norby, CHP

- 15 Years of IT experience
- Eight Years as the CIO of the Community Health Center of Central Wyoming and University of Wyoming Family Medicine Residency Program
- Six Years as a HIPAA Compliance Officer
- Four Years as a HIPAA Compliance Consultant
- Provided help to more than 150 hospitals and clinics

Disclaimers

- The presenter is not an attorney and does not give legal advice
- There are many different interpretations of HIPAA regulations
- Materials referenced are meant to serve as examples and may not be suitable for every organization

The Four Ways to an Audit

- Complaint
- Breach
- Random Audit (mandatory as of 2010)
- State Attorney General Action

- Desk audits are underway!
- Comprehensive onsite audits of both covered entities (CEs) and business associates (BAs) will begin in early 2017

Examples of Fines

Violation Category	Penalty Per violation	Annual Cap on penalty for all identical violations	Can penalty be waived by OCR?
Did Not Know	$100-50,000	$1.5 million	Yes
Reasonable Cause	$1,000-50,000	$1.5 million	Yes
Willful Neglect, Promptly Corrected	$10,000-50,000	$1.5 million	No
Willful Neglect, Not Corrected	$50,000	$1.5 million	No

Violations Due to Willful Neglect

- Violations resulting from willful neglect, defined to mean the conscious, intentional failure or reckless indifference to the obligation to comply with the regulations, will trigger the highest levels of penalties
- Penalties arising from willful neglect cannot be waived

Desk Audits

- Communications from Office for Civil Rights (OCR) will be sent via email and may be incorrectly classified as spam. If your entity's spam filtering and virus protection are automatically enabled, you are expected to check you junk or spam email folder for emails from OCR.
- Of the 176 potential audit items the first covered entities will have to provide documentation proving their compliance with the following seven HIPAA sections

Desk Audit HIPAA Controls

Privacy Rule Controls	Breach Notification Rule Controls	Security Rule Controls
Notice of Privacy Practices and Content Requirements [§164.520(a)(1) & (b)(1)]	Timeliness of Notification [§164.404(b)]	Security Management Process – Risk Analysis [§164.308 (a)(1)(ii)(A)]
Provision of Notice- Electronic Notice [§164.520(c)(3)]	Content Notification [§164404 (c)(1)]	Security Management – Risk Management [§164.308 (a)(1)(ii)(B)]
Right to Access [§164.524(a)(1), (b)(1), (b)(2), (c)(2), (c)(3), (c)(4), (d)(1), (d)(3)]		

Document Requests and Responses Expectations

Depending on the type of entity, each auditee is expected to:

- Provide only the policies and procedures that are relevant to the controls requested

  E.g., CEs must extract the relevant language from larger compendiums of policies and procedures if needed

- It is the auditee's responsibility to provide clear, complete, and responsive documentation to OCR
- Entities will not receive "credit" for a later document submission

- If a CE does not have the requested documentation, it must submit an explanation for the deficiency in its response

Notice of Privacy Practice and Content Requirements

- Verify that your Notice of Privacy Practices (NPP) has been updated to the 2013 HIPAA Omnibus Final Rule
- Upload a copy of all notices posted on website and within the facility, as well as the notice distributed to individuals
- Include a readable picture of any NPP's hanging on walls
- The notice must contain the name or title and contact information for those that need more information or would like to file a complaint
- The notice must contain an effective date

Provision of Notice – Electronic Notice

- Post your NPP prominently on your website
- Upload the URL for the entity web site and the URL for the posting of the entity notice, if any
- If the entity provides electronic notice, upload policies and procedures regarding provision of the notice electronically
- Upload documentation of an agreement with the individual to receive the notice via e-mail or other electronic form

Right to Access

- Upload policies and procedures for individuals to request access to protected health information (PHI)
- Upload all documentation related to the first five access requests which were granted, and evidence of fulfillment, in the previous calendar year (remove PHI if possible)
- Upload all documentation related to the last five access requests for which the entity extended the time for response to the request (remove PHI if possible)
- Upload any standard template or form letter required by or used by the CE to document access requests

Breach Notification Rule

- Many practices claim that they have never had a breach and OCR does not believe you
- Your practice has never handed a patient the wrong lab result or record?
- Mailed a bill to the wrong person?
- Sent a fax to the wrong number?
- Even the breach of just one patient must be reported to the patient and OCR
- Do you have a log of breaches?

Breach Notification – Timeliness of Notification

- Obtain and review the policies and procedures for notifying individuals of breaches and determine whether such policies and procedures are consistent with §164.404, including providing notification without unreasonable delay and in no case later than within 60 days of discovery of a breach.
- Obtain and review a list of breaches, if any, in the specified period and documentation indicating the date individuals were notified, the date the covered entity discovered the breach, and the reason, if any, for delay in notification to determine whether all individuals were notified consistent with §164.404(a), (b).
- Upload documentation of five breach incidents for the previous calendar year affecting fewer than 500 individuals, documenting the date individuals were notified, the date the covered entity discovered the breach, and the reason, if any, for a delay in notification.

Breach Notification – Content of Notification

- Upload documentation of five breach incidents affecting 500 or more individuals for the previous calendar year
- Upload a copy of a single written notice sent to affected individuals for each breach incident
- If the entity used a standard template or form letter, upload the document

Security Management Process
Risk Analysis

- Upload policies and procedures regarding the entity's risk analysis process
- Consistent with 164.316(b)(2)(i), upload documentation demonstrating that policies and procedures related to the implementation of this implementation specification were in place and in force six years prior to the date of receipt of notification
- Upload documentation of the current risk analysis and the most recently conducted prior risk analysis
- Upload documentation of current risk analysis results

Security Management Process
Risk Management

- Upload policies and procedures related to the risk management process
- Consistent with 164.316(b)(2)(i), upload documentation demonstrating that policies and procedures related to the implementation of this implementation specification were in place and in force six years prior to the date of receipt of notification
- Upload documentation demonstrating the efforts used to manage risks from the previous calendar year
- Upload documentation demonstrating the security measures implemented to reduce risks as a result of the current risk analysis or assessment (Upload documentation demonstrating that current and ongoing risks reviewed and updated)

Desk Audit Reporting Process

After review of submitted documentation:

- OCR will develop and share draft findings with the entity
- Entity may respond to draft findings—such written responses will be included in the final audit report
- Final audit reports will describe how the audit was conducted, present any findings, and contain entity responses to the draft findings
- Under OCR's separate, broad authority to open compliance reviews, OCR could decide to open a separate compliance review in a circumstance where significant threats to the privacy and security of PHI are revealed through the audit

Are Your Business Associates Prepared?

- Desk audits of BAs will begin this fall
- Have they completed their Risk Analysis?
- Can they provide proof of their Risk Management Plan?
- Have they established Breach Notification procedures?
- Does your BAA outline the BA's obligations to the Privacy Rule?

Business Associates are at Risk!

- Raleigh Orthopedic Clinic was fined $750K for releasing x-rays to a third party without a BAA in place
- North Memorial Health Care was fined $1.55M for failure to have a BAA in place with a contractor that lost a laptop
- Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS) has agreed to pay $650K after the theft of a CHCS mobile device compromised the PHI of 412 of nursing home residents. CHCS provided management and information technology services as a business associate to six skilled nursing facilities

Links to Resources

- **OCR 2016 HIPAA Desk Audit Guidance on Selected Protocol Elements:**
https://www.hhs.gov/sites/default/files/2016HIPAADeskAuditAuditeeGuidance.pdf

- **HIPAA Privacy, Security & Breach Notification Compliance Audits phase 2**
http://www.hhs.gov/sites/default/files/OCRDeskAuditOpeningMeetingWebinar.pdf

- **OCR 2016 HIPAA Desk Audits – Audited Entity Questions and Answers**
https://www.hhs.gov/sites/default/files/Phase2AuditOpeningMeetingWebinarQ%26A.pdf

- **HIPAA Full Regulation Text**
http://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf

- **Model Notices of Privacy Practices**
http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/

Join Us!

Our next free webinar

Mobile Technology in Health Care

Privacy and Security Considerations Webinar

September 14, 2016

1-2 p.m. MT

To register visit:

https://events-na8.adobeconnect.com/content/connect/c1/1103494218/en/events/event/shared/default_template/event_registration.html?sco-id=1929570621&_charset_=utf-8

Questions?

Mark Norby, Certified HIPAA Professional

HIPAA Counselor

307.258.5322

mnorby@healthinsight.org

Visit our website:

healthinsight.org/hipaapass

for more information about our Privacy and Security Solutions!

Thank you and have a wonderful day!!