
# Enforcement, Business Associates and Breach Notification. Oh my!

May 10, 2016

HealthInsight

# This Webinar is Brought to You By….

HealthInsight

HIPAAOne
PROTECT YOUR ePHI

Mountain-Pacific Quality Health

HealtHIE NEVADA
YOUR HEALTH INFORMATION EXCHANGE

# Who We Are

- 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: Nevada, New Mexico, Utah, Montana, Wyoming, Hawaii and Alaska. As part of our efforts to assist hospitals and providers with HIPAA compliance, HealthInsight and Mountain-Pacific Quality Health have formed **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

# Let’s Talk About…

HIPAA and the Patient Care Model

# Enforcement Key Points

- OCR Director Jocelyn Samuels indicated that OCR will continue to focus on breaches that demonstrate systemic deficiencies to send a message to organizations that fail to conduct risk analysis, ignore known threats or have insufficient workforce training. That's a warning that the practice of imposing large fines and resolution agreements on organizations OCR believes have disregarded HIPAA rules will continue.

***Health Data Management magazine (Feb. 2015)***

# Fine Amounts

| 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 |

# 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**

# Enforcement Key Points

- Generally speaking, where **multiple individuals are affected by an impermissible use or disclosure**, such as in the case of a breach of unsecured protected health information, the **number of identical violations** of the Privacy Rule standard regarding permissible uses and disclosures would be counted by the **number of individuals affected.**

# Enforcement Key Points

- The Secretary must formally investigate complaints indicating violations due to willful neglect and impose civil penalties upon finding said violations. The investigation is triggered if the initial facts show the "possibility" of willful neglect (i.e. no finding of probability is required).

# Enforcement Key Points

- The definition under 160.312 allows the Secretary to move directly to a civil penalty without exhausting informal resolution efforts, particularly in cases involving willful neglect.

# Enforcement Key Points

- HHS, on a case-by-case basis, may expand any preliminary review and conduct additional inquiries for purposes of identifying a possible violation due to willful neglect
- The HHS Secretary can coordinate with other law enforcement agencies on actions (e.g. State Attorney Generals and the FTC)

# Enforcement Key Points

- An organization's history of HIPAA compliance is relevant to the determination of the civil money penalty
- “Good faith effort” is losing strength and is being replaced by “demonstrable proof of compliance”

# Business Associates

- This term has broad applicability and includes, **other than a health care provider's employees**, "partners" that may provide legal, actuarial, accounting, consulting, data aggregation, management, administration or financial services wherein the services require the disclosure of individually identifiable health information.

# Business Associates

- Business associates (BAs) are directly liable under the Omnibus Final Rule of 2013 for uses and disclosures that violate the Privacy Rule (PR) or are in breach of the Business Associate Agreement
- Their failure may result in harm to your reputation

# Business Associates

- BAs are not permitted to use or disclose protected health information (PHI) if it would be a Privacy Rule violation for a covered entity (CE) to do so, except that a BA may use PHI for its own management and administration.

# Business Associates

- A person/entity becomes a BA by definition, and NOT because there happens to be a BA contract in place; therefore liability attaches immediately when a person “creates, receives, maintains or transmits PHI on behalf of a CE.”

# Business Associates

**BAs are now directly liable under the HIPAA rules:**

(1) For impermissible uses and disclosures

(2) For failure to provide breach notification to the CE

(3) For failure to provide access of ePHI to the CE

(4) For failure to disclose PHI to the Secretary

(5) For failure to provide an accounting of disclosures

(6) For failure to comply with the requirements of the Security Rule

# Business Associates

- BAs must comply with the “Minimum Necessary” principle.
- BAs are required to have business associate agreements with their sub-contractors who use PHI on their behalf
- BAs must monitor their business associate agreements with their sub-contractors
- Requirements in business associate agreements “cascade down” to sub-contractors and sub-contractors of sub-contractors (i.e. to ALL downstream sub-contractors)

# What Do You Need to Know?

- Do you have a BA management program in place to ensure documentation of and compliance with the requirements of HIPAA's Privacy and Security Rules by your Business Associates as required by 45 CFR §164.502(e) and 45 CFR §164.308(b)?
- Have you identified all of your BA arrangements to establish an action plan to address any deficiencies in documentation or compliance?
- Have you developed new BA agreements to strengthen the language in accordance with the Omnibus Final Rule?

# Breach Notification

- Refer to CFR 45 164.400, Subpart D of final regulation
- Page 71 of the HIPAA Full Regulation Text available on our website at:

http://healthinsight.org/hipaapass#resources

# Breach Notification

- **164.402 -** Identifying when a breach occurs
- **164.402 -** Securing protected health information
- **164.404 -** Notice to individuals, including timing, content and providing substitute notice
- **164.408 -** Notice to HHS, including annual and immediate notices to HHS, timing and content. The HHS electronic **reporting** process may be accessed through the OCR's HIPAA website: https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true

# Notification Requirements for Breaches of Unsecured PHI

- **164.406 -** Notice to the media, including form, timing and content
- **164.410 -** Notice by business associates, including timing and
- required information
- **164.412 -** Delay in **notice** at request of law enforcement

# What Do You Need to Know?

- In accordance with 45 CFR §164.402 revised by the Omnibus Final Rule, have you reviewed your breach notification policies and procedures in anticipation of the revised definition of breach determination from an assessment of the "risk of harm" to one of a "low probability of compromise"?
- Have you developed a methodology for assessing the determination of the "low probability of compromise", using at least the four factors provided in the Breach Notification Rule?
- Do you have a written policies and procedures, and a process in place for notifying affected individuals, the media and the Secretary of HHS of breaches within the required timeframe, with the required content and methods as required by the Breach Notification Rule?

# HIPAA PASS Webinar Series

Our next free webinar will be held in June, watch our website and your email for more information and registration details in the coming weeks:

***Building and Governing Your HIPAA Compliance Program***

# One-day HIPAA Boot Camps

Mark your calendar for one of three

**One-Day HIPAA Boot Camps: Training for Privacy and Security Officers**

Ogden – June 14

Provo – June 15

Salt Lake City – June 16

For more information call or email Mark Norby at: (307) 258-5322 or mnorby@healthinsight.org and watch your email for registration information coming soon!

# 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!