MCRH Webinar Sept 14, 2017

HIPAA Update
Increased Enforcement and Lessons Learned

Presented by
Elizabeth Callahan-Morris, Esq.
Hall, Render, Killian, Heath & Lyman, P.C.

Recent OCR Settlements

Type of Entity	Amount	Individuals Affected	State/Territory	Year	Key Facts
Health System	$[illegible]	858	IL	2017	[illegible] affected individuals within 60 days • Lack of compliant procedures & policies • Fine settlement based on breach notification rule violation
Insurance	$2,204,182	2,209	PR	2017	[illegible] • Failure to conduct risk analysis & implement risk management plans • No security awareness training
Hospital	$3,217,000	6,262	TX	2017	• Two separate breaches involving theft of [illegible] • Unauthorized employees received access to PHI • Lack of policies regarding receipt & removal of hardware containing PHI
Health System	$5,500,000	115,143	FL	2017	• Two unrelated breaches one involving a handheld employee the other involving employees of an affiliated physician's office • Lack of review for modifying/terminating access to PHI • Lack of review of information system activity records

2

Recent OCR Settlements

Type of Entity	Amount	Individuals Affected	State/Territory	Year	Key Points
Health System	$400,000	3200	CO	2017	• Hacker obtained ePHI through phishing incident • Failure to conduct risk analysis • Lack of compliant procedures & proper security measures to reduce risks
For-Profit Health Clinic	$31,000	10,728	IL	2017	• No signed Business Associate Agreement (BAA) prior to Oct. 12, 2015 • Failure to include policies concerning BAAs
Wireless Health Service Provider	$2,500,000	3,610	PA	2017	• First settlement involving wireless health service provider • Stolen unencrypted laptop outside employee residence • Insufficient risk analysis & lack of procedures regarding receipt/removal of hardware
Health System	$2,400,000	1	TX	2017	• Patient poses as employee using fraudulent I.D., reported and arrested • Patient's name disclosed to press following arrest
Hospital	$387,200	2	NY	2017	• PHI was released to complainants' employers • PHI faxed instead of sent to P.O. Box as requested • PHI contained highly sensitive HIV related info

3

HIPAA Audits Phase II

- 167 covered entity desk audits (2016)
  - Privacy: Access & notice of privacy practices
  - Security: Risk analysis & risk management
  - Breach: Content & timing of notice
- 33 business associate desk audits (2017)
- Onsite audits of CEs & BAs (tbd)
- Revised audit protocol
  - http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html

4

Recent OCR Guidance

- Privacy Rule Waivers for Hurricanes Harvey & Irma
  - https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/index.html
- Get it. Check it. Use it.
  - https://www.hhs.gov/hipaa/for-individuals/right-to-access/index.html
- HIPAA Breach Reporting Tool (HBRT)
  - https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
- International Cyber Threats & Ransomware Campaigns
  - https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html

5

Client FAQs

- Access requests & copy fees
- Law enforcement requests
- Marketing communications
- Friends & family
- Breach risk assessments
- Business associate agreements
- Social media
- Mental health & substance abuse

6

Please visit the Hall Render Blog at http://blogs.hallrender.com for more information on topics related to health care law.

Elizabeth Callahan-Morris
248.457.7854 direct
ecallahan@hallrender.com

HEALTH LAW IS OUR BUSINESS.
Learn more at hallrender.com

HALL RENDER
KILLIAN HEATH & LYMAN

HIPAA Incident and Breach Notification Risk Assessment – Sample

I. Breach Notification Rule

Pursuant to the HIPAA Breach Notification Rule, a breach mean the acquisition, access, use or disclosure of protected health information ("PHI") in a manner not permitted under the Privacy Rule which that compromises the security or privacy of the PHI.

An unpermitted acquisition, access, use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors: (1) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (2) The unauthorized person who used the PHI or to whom the disclosure was made; (3) Whether the PHI was actually acquired or viewed; and (4) The extent to which the risk to the PHI has been mitigated.

II. Description of Incident

Risk Assessment Date:

Discovery Date:

Incident Date(s):

Involved parties:

Description:

III. Assessment

Factor 1: The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.

Describe:

Risk factor: High, Medium Low

Factor 2: The unauthorized person who used the PHI or to whom the disclosure was made.

Describe:

Risk factor: High, Medium Low

Factor 3: Whether the PHI was actually acquired or viewed.

Describe:

Risk factor: High, Medium, Low

Factor 4: The extent to which the risk to the PHI has been mitigated.

Describe:

Risk factor: High, Medium, Low

IV. Conclusion

In reviewing the risk factors in totality, the risk assessment finding for this HIPAA incident is that it created no more / more than a low probability of compromise.

In conclusion, this HIPAA incident is / is not considered to be a reportable Breach.

1685226v1

Permissible Fees for HIPAA Access Requests

	EMR	Paper Medical Record
Electronic copy	(1) actual labor costs for copying plus supplies and postage (2) **schedule of costs** (flat rate) based on average labor costs for copying, plus supplies and postage (3) **$6.50 flat rate** (or less) inclusive of labor, supplies and postage	(1) actual labor costs for copying plus supplies and postage (2) **schedule of costs** (flat rate) based on average labor costs for copying, plus supplies and postage (3) ***per page fee*** based on average labor costs or actual costs, plus supplies and postage
Paper copy	(1) actual labor costs for copying plus supplies and postage (2) **schedule of costs** (flat rate) based on average labor costs for copying, plus supplies and postage	(1) actual labor costs for copying plus supplies and postage (2) **schedule of costs** (flat rate) based on average labor costs for copying plus supplies and postage (3) ***per page fee*** based on average labor costs or actual costs, plus supplies and postage
Written Summary or Explanation	(1) actual labor costs for preparing summary, plus supplies and postage	(1) actual labor costs for preparing summary, plus supplies and postage
View and Inspect	None	None

Reference: 45 CFR 164.524; OCR Guidance http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html

Office for Civil Rights
HIPAA Privacy, Security, & Breach Notification Audit Program

Draft Report

*Entities must **provide any responses within 10 business days** of the date of this document in order for OCR to include them in the final audit report. Entities may provide responses via email to OSOCRAudit@hhs.gov:*

1. *in the body of an email, or*
2. *using a MS Word attachment.*

Please identify each response with the corresponding element number and name, as presented in this report, auditor analysis and findings section. Do not submit new documentation, as it will not be considered.

Scope and Methodology

In carrying out the desk audits, OCR assesses the submitted policies, procedures and other requested documentation against the inquiries specified in the audit protocol. The audit protocol used for this assessment is available on the OCR audit webpage; http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit.

Results of Review

Any preliminary findings of indications of noncompliance are listed below. In addition, OCR assessed a relative level of entity compliance efforts for each audited element on a scale of 1 through 5. The scores indicate OCR's assessment of the comprehensiveness and effectiveness of these efforts and the magnitude of related risk: See *Compliance Effort Ratings – Legend*, below, for more information. While audited entities should remediate all findings, higher scores indicate that OCR believes that timely and complete corrective action by the entity is essential.

Auditor Ratings

The auditor assessed entity efforts to comply with the selected elements using the following guidelines.

Compliance Effort Ratings—Legend	
Rating	**Description**
1	The audit results indicate the entity is in compliance with both goals and objectives of the selected standards and implementation specifications.
2	The audit results indicate that the entity substantially meets criteria; it maintains appropriate policies and procedures, and documentation and other evidence of implementation meet requirements.

Compliance Effort Ratings—Legend	
Rating	**Description**
3	Audit results indicate entity efforts minimally address audited requirements; analysis indicates that entity has made attempts to comply, but implementation is inadequate, or some efforts indicate misunderstanding of requirements.
4	Audit results indicate the entity made negligible efforts to comply with the audited requirements - e.g. policies and procedures submitted for review are copied directly from an association template; evidence of training is poorly documented and generic.
5	The entity did not provide OCR with evidence of serious attempt to comply with the Rules and enable individual rights with regard to PHI.

Element #	SECTION	KEY ACTIVITIES
P55	§164.520(a)(1) & (b)(1)	Notice of Privacy Practices Content requirements
Preliminary Finding	1) The entity fails to include each required element.	
Preliminary Auditor Analysis	The Notice of Privacy Practices fails to include several elements, specifically: 1. The entity failed to provide a statement that it can release certain information to avert a serious threat to health or safety without first getting authorization or agreement from the individual . 2. The entity failed to provide a statement that it can release certain information for specialized government functions without first getting authorization or agreement from the individual . 3. The notice provided did not include a statement that the entity is required to disclose PHI to the Secretary of HHS. 4. The notice did not include a statement that the entity is required to disclose PHI upon request of the individual or to another named by the individual. 5. The notice does not include a statement that the use or disclosure of PHI for the purposes of sale of information requires individual authorization. 6. The Notice of Privacy Practices does not contain a description of how the individual may obtain a copy of the individual's health and claims records, and to direct the covered entity to send these records to a third party. 7. The Notice of Privacy Practices does not contain a description of how the individual may request and obtain a list of disclosures made for certain purposes not related to treatment, payment, or health care operations, or without individual authorization. 8. The Notice of Privacy Practices does not contain a description of how the individual may obtain a paper copy of the privacy notice.	
Preliminary Rating	3	
Effect	Failure to adequately and comprehensively provide individuals with a notice of privacy practices for protected health information could result in individuals not knowing how their protected health information is used or disclosed; not knowing what individual rights they have with respect to their protected health information; and/or not knowing the extent of the entity's legal duties with respect to the protected health information.	

Element #	SECTION	KEY ACTIVITIES
P58	§164.520(c)(3)	Provision of Notice - Electronic Notice
Preliminary Finding	1) None.	
Preliminary Auditor Analysis	The entity maintains a website with an electronic version of its Notice of Privacy Practices that is easily accessible and prominently posted under a drop down menu on the homepage. Because the entity does not provide its Notice to patients via email, the requirement to have an agreement with the individual to receive notice electronically is not applicable.	
Preliminary Rating	1	
Effect	Failure to provide electronic notice of privacy practices may result in an individual not being informed of his/her rights, or the entity's duties, regarding the use and disclosure of the individual's protected health information.	