Preparing for the OCR:
Proactively Assess and Lessen the Burden in the Event of an Audit

CHS Community Health Systems

2

Agenda

- OCR Audit Protocol update
- Phase 2 HIPAA audits
- Benefits of preparing
- How did we prepare?

3

OCR Audit Protocol Update

- Website: http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/

Audit Type	Section	Key Activity	Established Performance Criteria	Audit Inquiry	Req-uired/ Address-able
Privacy	§164.502(a)(5)(i)	Prohibited uses and disclosures - Use and disclosure of genetic information for underwriting purposes	§ 164.502(a)(5)(i) Use and disclosure of genetic information for underwriting purposes: Notwithstanding any other provision of this subpart, a health plan, excluding an issuer of a long-term care policy falling within paragraph (1)(viii) of the definition of health plan, shall not use or disclose protected health information that is genetic information for	Does the health plan use or disclose for underwriting purposes, "Genetic Information" as defined at § 160.103, including family history? Inquire of management. Obtain and review all underwriting policies and procedures (for example, published and unpublished underwriting guidelines currently	

4

Phase 2 HIPAA Audits

- In 2016, the OCR began building their information population of covered entities ("CEs") by requiring CEs to verify contact information, as well as complete a pre-screening questionnaire.
- 167 covered entities were selected for topic-focused audits in mid-2016. Audit of business associates to commence anytime.
- Comprehensive on-site audits scheduled 2017
- Audit selectees have 10 business days to respond to initial data requests.

5

Benefits of Preparing

- Facilities could still be selected for audits in 2017 and going forward as part of OCR's continuous audit monitoring program.
- Facilities proactively mitigate risk and remediate control gaps.
- Evidence collected early can be set aside to save in the event of an audit, which cutes down on the burden of pulling together evidence in a 10-day window.
- Re-educational value

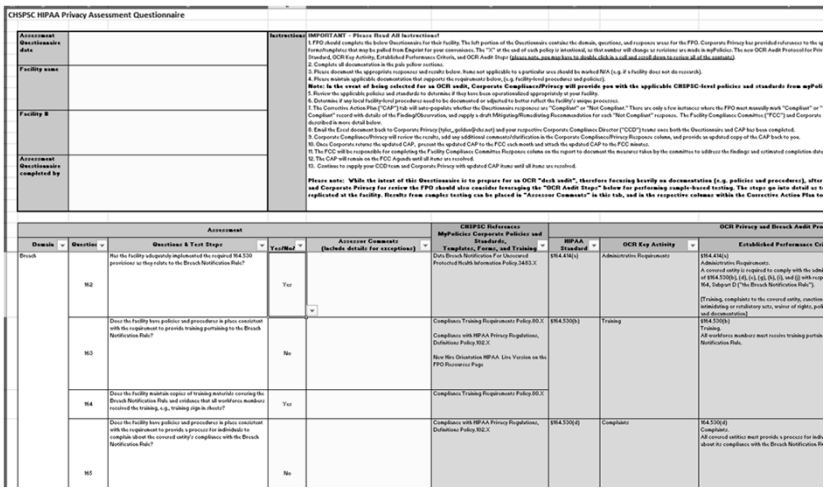
6

How Did We Prepare?

- Leveraged the latest OCR Protocol for the Privacy and Breach Notification Rules to create a Questionnaire tool
  - Security Rule was handled by Internal Audit and Corporate Security
- Based on responses, a Corrective Action Plan would automatically populate “Not Compliant” responses.
- Facilities worked with Corporate Compliance to address any “Not Compliant” areas

7

Questionnaire


CHSPSC HIPAA Privacy Assessment Questionnaire

Assessment Questionnaire date		Instructions	IMPORTANT – Please Read All Instructions!
Facility name			
Facility #			
Assessment Questionnaire completed by			

Assessment					CHSPSC References: MyPolicies Corporate Policies and Standards, Templates, Forms, and Training	OCR Privacy and Breach Audit Protocol		
Domain	Question #	Questions & Test Steps	Yes/No/#	Assessor Comments: (Include details for exceptions)		HIPAA Standard	OCR Exp Activity	Established Performance Cr
Breach	162	Has the Facility subsequently implemented the required §164.530 provisions as they relate to the Breach Notification Rule?	Yes		Data Breach Notification For Unsecured Protected Health Information Policy.3403.X	§164.414(a)	Administrative Requirements	§164.414(a) Administrative Requirements. A covered entity is required to comply with the subs of §164.530(b), (d), (e), (g), (h), (i), and (j) with respe 164, Subpart D ("the Breach Notification Rule"). (Training, complaints to the covered entity, sanction intimidating or retaliatory acts, waiver of rights, poli and documentation)
	163	Does the Facility have policies and procedures in place consistent with the requirement to provide training pertaining to the Breach Notification Rule?	No		Compliance Training Requirements Policy.80.X Compliance with HIPAA Privacy Regulations, Definitions Policy 502.X New Hire Orientation HIPAA Live Version on the FPO Resources Page	§164.530(b)	Training	§164.530(b) Training. All workforce members must receive training pertain Notification Rule.
	164	Does the Facility maintain copies of training materials covering the Breach Notification Rule, and evidence that all workforce members received the training, e.g., training sign-in sheets?	Yes		Compliance Training Requirements Policy.80.X			
	165	Does the Facility have policies and procedures in place consistent with the requirement to provide a process for individuals to complain about the covered entity's compliance with the Breach Notification Rule?	No		Compliance with HIPAA Privacy Regulations, Definitions Policy 502.X	§164.530(d)	Complaints	§164.530(d) Complaints. All covered entities must provide a process for indi about its compliance with the Breach Notification R

8

Corrective Action Plan

CHSPSC HIPAA Privacy Corrective Action Plan

Assessment Questionnaire date		Instructions	1. The Corrective Action Pla There are only a few instar FPO should populate any " Recommendation for each add additional clarifying a 2. Email the Excel documer teams once both the Quest 3. Corporate Compliance/Pr Response column, and pro 4. Once Corporate returns t 5. The FCC will be responsi measures taken by the cor 6. The CAP will remain on t 7. Continue to supply your
Facility name			
Facility #			
Assessment Questionnaire completed by			

Domain	OCR Key Activity	Question #	Compliant / Not Compliant	Findings/Observations	Mitigating/Remediating Recommendations	Corporate Compliance/Pr
Breach	Administrative Requirements	162	Compliant			
Breach	Training	163	Not Compliant			
Breach	Training	164	Compliant			
Breach	Complaints	165	Not Compliant			

9

Questions?

10